Safe DC SDC-PoE8

Switch with 8 PoE/PoE+/HiPoE or SFP ports integrated Micro-UPS

BACnet IP / HTTPS / SNMP

EN Advanced User's Manual

7. Configuration 57

1. General information

1.1 Purpose of the document

The Advanced user manual provides the information necessary for the configuration and the operation of the switch SDC-PoE8.

This manual complements the Operating Instructions of the product SDC-PoE8.

Theses instructions are also available in PDF format at www.slat.com .

1.2 Related documentation

The following documents are associated with this manual:

- Operating instructions
- Installation manual
- Commercial brochure
- Datasheet

This documentation is available at www.slat.com.

2. Commissioning

Before starting to commission the switch, check that the LED "Status" on the front is green. This means the product is powered properly and ready to function.

The switch parameters can be configured via the HTTPS website. It also makes it possible to configure the energy saving mode (ECO) and the stealth mode.

Using the onboard website, the system parameters can be defined, the switch and all its ports managed and controlled as well as the network conditions monitored. The administrator can set up the managed switch by selecting the functions listed in the main menu. To be able to communicate with the product, the port, to which the supervisor is connected to, has to be part of the **VLAN 1**.

In order to manage and to communicate with the product, it must be configured according to the following chapters. The computer's network configuration, to which the product will be connected to, has to be compatible with the product's network parameters.

2.1 Communication protocols

The product supports the following communication protocols.

Application layer protocols

- HTTPS
- BACnet IP
- SNMP v1, v2c + v3
- DHCP

Network layer protocols

- IPv4
- ICMP

2.2 Assigning an IP address

The DHCP (dynamic IP address allocation) automatically assigns an IP address to a product in order to communicate with it. This feature is enabled by default in the factory configuration.

Two different operating modes exist according to the availability or lack of a DHCP server on the network:

A. DHCP server available
If a DHCP server is available, it automatically allocates an IP address to the product. If several products are connected to the network, it assigns a different IP address to each one.
To determine the new address, browse the network

B. DHCP server not available
If no DHCP server is available on the network, the product uses the IP settings below. When the switch is first connected to the network, it remains in DHCP for 1 minute before switching to the predefined IP address.

- **IP address** **192.168.1.1**
- **Network mask** **255.255.255.0**
- **No gateway**

In this case, if several products need to be connected to a single network, they must be isolated and the IP address of each product must be modified using their HTTPS, to avoid any address conflicts web interface. Indeed, they possess the same IP parameters before being connected to the network. The same procedure applies if the same IP address exists several times on a given network. See the Advanced user's manual for instructions on changing the IP address.

2.3 Login page – Logging onto the product

Using the allocated or predefined IP address, it is possible to log onto the product using a web browser over HTTPS.

When connecting to the product for the first time with an IP address, the user will have a warning about the website's security certificate. Ignore this warning and proceed to access the website. Each time the product's IP address changes, the user will redo the same operation.

IMPORTANT REMARK!

The default login and password are:

Login: admin

There is no password. Click directly on "OK".

For the security of your installation, it is imperative to set a password

Figure 2.1: Login page

2.4 Web-based user interface – Description

After entering the login and the password in the login page and once connection with the product has been established, the "System Information" page of the section "System State" is displayed (see chapter 3.1).

The user interface, as shown in Figure 2.2, is divided in three areas: headline, main menu and main screen.

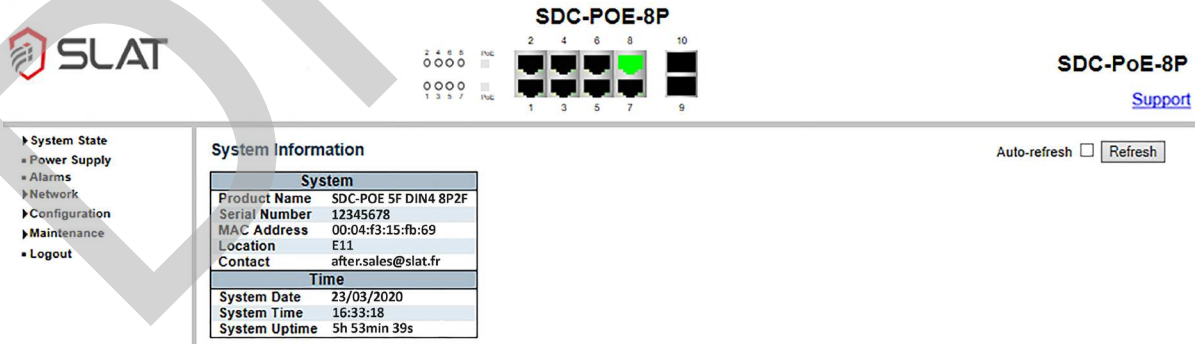


Figure 2.2: User interface

2.4.1 Headline

The headline is the area on top of each page. The headline is the same for each page of the menu. In the center, it contains the product's name defined in the "System Settings Configuration" page (chapter 6.1) as well as the port indicators and the PoE LEDs. The featured port numbers in the headline correspond to the numbers on the switch. The colors of the port indicators inform about the link working status.

- link 10/100 Mbps (yellow)
- link 1000 Mbps (green)
- no link (black)

The PoE LEDs located on the left hand side of the stacked modular jack drawing show when the Peripheral Device is Powered over Ethernet.

- Blue – powered over PoE
- Red – fault on PoE

The user can use the "Support" link, located on the left side of the headline, to send an email to SLAT's after-sales service.

2.4.2 Main menu

The main menu is situated on the left side of the interface. It gives an overview of the different sections and allows access to all the pages of this site. The pages are organized in the following sections:

- System State
- Power Supply
- Alarms
- Network
- Configuration
- Maintenance

2.4.3 Main screen

The main screen, occupying most of the screen space, contains all the relevant information of one page. Depending on the page, information can here be visualized or parameters configured.

3. System State

The ‘System State’ section gives an overview of all the data relevant for the running of the switch. The results of the settings defined in the other sections are visualized on the corresponding pages in the ‘System State’ section. The information displayed in these pages can only be configured by going to the respective configuration page.

3.1 System Information

Once connection with the product has been established, the "System Information" page is opened. The general information regarding the ‘System’ and the ‘Time’ is displayed here.

- **Product Name**
  The designation of this switch. This is a product specific information which can’t be modified.
- **Serial Number**
  The serial number of this switch. This is a product specific information which can’t be modified.
- **MAC Address**
  The MAC address of this switch. This is a product specific information which can’t be modified.
- **Location**
  The location defines the place where the product is installed (physical location). This information can be changed in the "System Settings Configuration" page (see chapter 6.1).
- **Contact**
  The after-sales contact information. This is information can’t be modified.
- **System Date**
  The current (GMT) system date. The system date is obtained through the Timing server on the network.
- **System Time**
  The current (GMT) system time. The system time is obtained through the Timing server on the network.
- **System Uptime**
  The time span that has passed since the switch was last turned on.

Check the ‘Auto-refresh’ box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the ‘Refresh’ button.

3.2 System Log

This page provides the switch’s ‘System Log’ information.

It can be chosen which type of information is shown by checking the corresponding box under the list. The table contains information regarding:

- Power
- Network
- Configuration
- Miscellaneous

The table features:

- the time and date of the system log entry,
- the message of the system log entry
- the concerned port number.

Time stamp

If the date and time are available via the NTP, then the events are time stamped in the following format:

hours : minutes : seconds **day/month/year**

Example ➲

```
6:10:50 13/12/2018 - System Start
6:10:53 13/12/2018 - P2: 100Mbps
0:48:58 14/12/2018 - Mains Fault
0:48:58 14/12/2018 - Backup Mode
0:55:26 14/12/2018 - Mains OK
```

Otherwise, the elapsed time since the last start is used pending the availability of NTP data. In this case, the events are in the following format:

hours : minutes : seconds **the number of the days D**

Example ➲

```
00:00:00    0D - System Start
00:00:00    0D - Reset Configuration
00:00:01    0D - Mains Fault
00:00:01    0D - Backup Mode
00:00:03    0D - P1: 100Mbps
```

3.3 Power Supply State

The "Power Supply State" page displays the operating status and all the physical values of the power supply measured by the product.

Information outside the frame

- **Product description**
  On top of the frame the following product information is displayed:
  - Product reference and version
  - Actual capacity in Watt-hours
  - Product serial number
- **Mains input**
  The mains power is indicated by the value and the pictogram on the left of the frame. If no mains power is present, a red cross is displayed over the pictogram. The value displayed indicates mains consumption in Watts.
- **Output**
  On the right of the frame information regarding the output is shown. When the breaker is closed, the PoE applications are powered by the product. If the breaker is open, the backup is reaching the end of its autonomy: disconnection and interruption of the power supply are imminent. The value indicates the total PoE power supplied to the devices in Watts.

Information inside the frame

- **Operating mode**
  The product operating mode is indicated by the frame color:
  - Operating on mains gray frame
  - Operating on backup orange frame
  - Eco or Stealth Mode green frame
- **Product operating status**
  The text (title) inside the frame indicates whether the product operation is ok, or whether there is a product fault.
- **Operation-related data**
  The information on the left inside the frame describe the data related to the operating of the power supply.
  - Output voltage and current
  - Battery voltage and current (If the displayed battery current is negative, the battery is discharging.)

- The product's internal temperature
- Total Watt-hours drained from the Safe DC since product factory inspection and commissioning
- Total number of power cuts since product factory inspection and commissioning

- **Charge gauge**
  The gauge on the right shows the backup pack's charge status. The backup pack must be fully charged once before the gauge will display an accurate reading.

The page is refreshed automatically every 3 seconds. To manually refresh the data, click on the "Refresh" button.

3.4 MAC Table

The entries in the "MAC Address Table" are shown on this page. The MAC Table contains up to 8192 entries. It is sorted first by VLAN ID and then by MAC address.

MAC Table Columns

- **Type**
  Indicates whether the entry is a static or a dynamic entry.
- **VLAN**
  The VLAN ID of the entry.
- **MAC address**
  The MAC address of the entry.
- **Port Members**
  The ports that are members of the entry.

Navigating the MAC Table

Each page shows up to 999 entries from the MAC table, default being 20. They can be selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed entry will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The "Start from VLAN" and "MAC address" input fields allow the user to select the starting point in the MAC Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next MAC Table match. In addition, the two input fields will - upon a "Refresh" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> button will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over. The table is updated, starting from the first entry in the MAC Table.

Check the "Auto-refresh" box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the table manually click on the "Refresh" button. The displayed table will start from the "Start from VLAN" and "MAC address" input fields. By clicking the "Clear" button, all the dynamic entries are cleared.

3.5 VLANs

3.5.1 Membership

The "VLAN Membership Status for Combined users" page provides an overview of the membership status of the VLAN users. Different tables can be displayed depending on the selected type of VLAN user.

Types of VLAN users

Various internal software modules may use VLAN services to configure VLAN memberships on the fly (MEP or NAS). The drop-down list on the top right allows for selecting to show VLAN memberships as configured by:

- ‘Admin’: the administrator
- ‘MEP’ or ‘NAS’: one of the internal software modules
- ‘Combined’: a combination of the administrator and the internal software modules configuration. It basically reflects the actual configuration of the product.

Navigating the VLAN Membership Status Table

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input field allows the user to select the starting point in the VLAN Table. Clicking the button ‘Refresh’ will update the displayed table starting from that or the closest next VLAN Table match.

The >> button will use the last entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached, the text " No data exists for the selected user " is shown in the displayed table. Use the |<< button to start over.

VLAN Membership Status Table Columns

- **VLAN ID**
  The VLAN ID for which the Port members are displayed.
- **Port Members**
  A row of check boxes for each port is displayed for each VLAN ID.
  - The port in not configured on a VLAN
  - The port is included in a VLAN.
  - The port is in the forbidden port list.
  - The port is in the forbidden port list and at the same time attempts to be included in the VLAN (conflict port). The port will not be a member of the VLAN in this case.

Check the ‘Auto-refresh’ box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the ‘Refresh’ button.

3.5.2 Ports

This page provides information regarding the VLAN Port Status. Different tables can be displayed depending on the selected type of VLAN user.

Types of VLAN users

Various internal software modules may use VLAN services to configure VLAN ports on the fly (NAS, MSTP or ERPS). The drop-down list on the top right allows for selecting to show VLAN ports as configured by:

- ‘Admin’: the administrator
- ‘NAS’, ‘MSTP’ or ‘ERPS’: one of the internal software modules
- ‘Combined’: a combination of the administrator and the internal software modules configuration. It basically reflects the actual configuration of the product.

If a given software module hasn't overridden any of the port settings, the text "No data exists for the selected user" is shown in the table.

VLAN Port Status Table Columns

- **Port**
  The logical port for the settings contained in the same row.
- **Port Type**
  Shows the port type (Unaware, C-Port, S-Port, S-Custom-Port.) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.
- **Ingress Filtering**
  Shows whether a given user wants ingress filtering enabled or not. The field is empty if not overridden by the selected user.
- **Frame Type**
  Shows the acceptable frame types (All, Taged, Untagged) that a given user wants to configure on the port. The field is empty if not overridden by the user.
- **Port VLAN ID**
  Shows the Port VLAN ID (PVID) that a given user wants the port to have. The field is empty if not overridden by the selected user.
- **Tx Tag**
  Shows the Tx Tag requirements (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID) that a given user has on a port. The field is empty if not overridden by the selected user.
- **Untagged VLAN ID**
  If the Tx Tag is overridden by the selected user and set to ⍰Tag⍰ or ⍰Untag UVID⍰, then this field will show the VLAN ID the user wants to tag or untag on egress. The field is empty if not overridden by the selected user.
- **Conflicts**
  Two users may have conflicting requirements to a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress. Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized way. The Administrator has the least priority. Other software modules are prioritized according to their position in the drop-down list (in the top right): The higher their position in the list, the higher their priority. If conflicts exist, they will be displayed as "Yes" for the "Combined" user and the offending software module. The "Combined" user basically reflects the actual configuration of the product.

Check the ⍰Auto-refresh⍰ box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the ⍰Refresh⍰ button.

3.6 Ports Status

3.6.1 Traffic Overview

This page provides an overview of general traffic statistics for all switch ports (⍰Port Statistics Overview⍰).

The displayed counters are:

- **Port**
  The logical port for the settings contained in the same row.
  Click on the port number to see the detailed statistics for this particular port. By clicking on a port number, the user is redirected to the corresponding ⍰Detailed Port Statistics⍰ page (see chapter 3.6.2).
- **Packets**
  The number of received and transmitted packets per port.

- **Bytes**
  The number of received and transmitted bytes per port.
- **Errors**
  The number of frames received in error and the number of incomplete transmissions per port.
- **Drops**
  The number of frames discarded due to ingress or egress congestion.
- **Filtered**
  The number of received frames filtered by the forwarding process.

Check the "Auto-refresh" box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the "Refresh" button.

By clicking the "Clear" button, the counters for all ports are cleared.

3.6.2 Detailed Statistics

The "Detailed Port Statistics" page provides detailed traffic statistics for a specific switch port. The drop-down menu in the top right corner of the page can be used to select which switch port details to display.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit and the error counters for receive and transmit.

Receive Total and Transmit Total

- **Rx and Tx Packets**
  The number of received and transmitted (good and bad) packets.
- **Rx and Tx Octets**
  The number of received and transmitted (good and bad) bytes. Includes FCS but excludes framing bits.
- **Rx and Tx Unicast**
  The number of received and transmitted (good and bad) unicast packets.
- **Rx and Tx Multicast**
  The number of received and transmitted (good and bad) multicast packets.
- **Rx and Tx Broadcast**
  The number of received and transmitted (good and bad) broadcast packets.
- **Rx and Tx Pause**
  A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters

The number of received and transmitted packets per input and output queue.

Receive Error Counters

- **Rx Drops**
  The number of frames dropped due to lack of receive buffers or egress congestion.

- **Rx CRC/Alignment**
  The number of frames received with CRC or alignment errors.
- **Rx Undersize**
  The number of short[1] frames received with valid CRC.
- **Rx Oversize**
  The number of long[2] frames received with valid CRC.
- **Rx Fragments**
  The number of short[1] frames received with invalid CRC.
- **Rx Jabber**
  The number of long[2] frames received with invalid CRC.
- **Rx Filtered**
  The number of received frames filtered by the forwarding process.

[1] Short frames are frames that are smaller than 64 bytes.
[2] Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

- **Tx Drops**
  The number of frames dropped due to output buffer congestion.
- **Tx Late/Exc. Coll.**
  The number of frames dropped due to excessive or late collisions.

Check the ‘Auto-refresh’ box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the ‘Refresh’ button.

By clicking the ‘Clear’ button, the counters for all ports are cleared.

3.6.3 Aggregation

3.6.3.1 System Status

This page provides a status overview for all LACP instances (LACP System Status).

- **Aggr ID**
  The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'.
- **Partner System ID**
  The system ID (MAC address) of the aggregation partner.
- **Partner Key**
  The Key that the partner has assigned to this aggregation ID.
- **Last Changed**
  The time since this aggregation changed.
- **Local Ports**
  Shows which ports are a part of this aggregation for this switch. The format is: "Switch ID:Port".

Check the ‘Auto-refresh’ box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the ‘Refresh’ button.

3.6.3.2 Port Status

This page provides a status overview for the LACP Status for all ports.

- **Port**
  The switch port number.
- **LACP**
  - "Yes" means that LACP is enabled and the port link is up.
  - "No" means that LACP is not enabled or that the port link is down.
  - "Backup" means that the port could not join the aggregation group but will join if another port leaves. Meanwhile it's LACP status is disabled.
- **Key**
  The key assigned to this port. Only ports with the same key can aggregate together.
- **Aggr ID**
  The Aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs while IDs 3-14 are LLAGs.
- **Partner System ID**
  The partner's System ID (MAC address).
- **Partner Port**
  The partner's port number connected to this port.
- **Partner Prio**
  The partner's port priority.

Check the "Auto-refresh" box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the "Refresh" button.

3.6.3.3 Port Statistics

This page provides an overview for LACP statistics for all ports.

- **Port**
  The switch port number.
- **LACP Received**
  Shows how many LACP frames have been received at each port.
- **LACP Transmitted**
  Shows how many LACP frames have been sent from each port.
- **Discarded**
  Shows how many unknown or illegal LACP frames have been discarded at each port.

Check the "Auto-refresh" box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the "Refresh" button.

By clicking the "Clear" button, the counters for all ports are cleared.

3.6.4 Thermal Protection

This page allows the user to inspect the status information related to thermal protection.

Thermal Protection Port Status

- **Port**
  The switch port number.
- **Temperature**
  Shows the current chip temperature in degrees Celsius.
- **Port Status**
  Shows if the port is thermally protected (link is down) or if the port is operating normally.

Check the "Auto-refresh" box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the "Refresh" button.

3.6.5 Green Ethernet

The Green Ethernet Status page provides the current Port Power Savings Status for the Energy Efficient Ethernet (EEE).

- **Port**
  This is the logical port number for this row.
- **Link**
  The current link state is displayed graphically. The color indicates if a link has been created to the respective port:
  - Red link down (no link)
  - Green link up (link established)
- **EEE Cap**
  Shows if the port is EEE capable.
- **EEE Ena**
  Shows if the EEE is enabled for the port. This information reflects the settings defined in the Port Power Savings configuration page (chapter 5.1.5 Green Ethernet).
- **LP EEE cap**
  Shows if the link partner is EEE capable.
- **EEE In power save**
  Shows if the system is currently saving power due to EEE. When EEE is enabled, the system will power down if no frame has been received or transmitted in 5 µs.
- **ActiPhy Savings**
  Shows if the system is currently saving power due to ActiPhy.
- **PerfectReach Savings**
  Shows if the system is currently saving power due to PerfectReach.

Check the "Auto-refresh" box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the "Refresh" button.

3.6.6 PoE Status

The Power Over Ethernet Status page allows the user to inspect the current status for all PoE ports.

- **Local Port**
  This is the logical port number for this row.
- **Description**
  This case can be used to describe where the port is connected.
  Shows the description which the user can add during the configuration of the PoE Port settings (chapter 5.2.1).
- **PD Class**
  Each PD is classified according to a class that defines the maximum power the PD will use. The ‘PD Class’ shows the class the PD is classified to.
  Eight classes are defined:
  - Class 0: Max. power 15.4 W
  - Class 1: Max. power 4.0 W
  - Class 2: Max. power 7.0 W
  - Class 3: Max. power 15.4 W
  - Class 4: Max. power 30.0 W
  - Class 5 : Max power 45W (*)
  - Class 6 : Max power 60W (*)
  - Class 7 : Max power 75W (*)
  - Class 8 : Max power 90W (*)

  Note: Only available on High PoE ports [1-4]
- **Power Requested**
  The Power Requested shows the requested amount of power the PD wants to be reserved.
- **Power Allocated**
  The Power Allocated shows the amount of power the switch has allocated to the PD.
- **Power Used**
  The Power Used shows how much power the PD is currently using.
- **Current Used**
  The Power Used shows how much current the PD is currently using.
- **Priority**
  The Priority shows the port's priority configured by the user.
- **Port Status**
  The Port Status shows the actual status of the port. The status can be one of the following values:
  - ‘PoE turned ON’: The PD is powered over PoE.
  - ‘PoE not available - No PoE chip found’: PoE not supported for the port.
  - ‘PoE turned OFF - PoE disabled’: PoE is disabled by user.
  - ‘PoE turned OFF - Power budget exceeded’: The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver. In consequence, the port(s) with the lowest priority is/are powered down.
  - ‘No PD detected’: No PD was detected for the port.
  - ‘PoE turned OFF - PD overload’: The PD has requested or used more power than the port can deliver. In consequence, the port is powered down.
  - ‘PoE turned OFF’: The PD is off.
  - ‘Invalid PD’: The PD is detected but is not working correctly.

Check the ‘Auto-refresh’ box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the ‘Refresh’ button.

3.7 LLDP

3.7.1 Neighbors

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The columns hold the following information.

LLDP Neighbor Information ▯ LLDP Remote Device Summary

- **Local Port**
  The port on which the LLDP frame was received.
- **Chassis ID**
  The Chassis ID is the identification of the neighbor's LLDP frames.
- **Port ID**
  The Port ID is the identification of the neighbor port.
- **Port Description**
  The Port Description is the description of the port advertised by the neighbor unit.
- **System Name**
  The System Name is the name advertised by the neighbor unit.
- **System Capabilities**
  The System Capabilities describes the neighbor unit's capabilities. The possible capabilities are:
  1. Other
  2. Repeater
  3. Bridge
  4. WLAN Access Point
  5. Router
  6. Telephone
  7. DOCSIS cable device
  8. Station only
  9. Reserved

  When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).
- **Management Address**
  The Management Address is the neighbor unit's address that is used for higher layer entities to assist the discovery by the network management. This could for instance hold the neighbor's IP address.

Check the ▯Auto-refresh▯ box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the ▯Refresh▯ button.

3.7.2 PoE

This page provides a status overview for all LLDP PoE neighbors. The displayed table contains a row for each port on which an LLDP PoE neighbor is detected. The columns hold the following information.

LLDP Neighbor Power Over Ethernet Information

- **Local Port**
  The port of the switch on which the LLDP frame was received.
- **Power Type**
  The Power Type represents whether the device is a Power Sourcing Entity (PSE) or Power Device (PD). If the Power Type is unknown it is represented as "Reserved".

- **Power Source**
  The Power Source represents the power source being utilized by a PSE or PD device.
  - PSE device
    If the device is a PSE device, it can either run on its Primary Power Source or its Backup Power Source. If it is unknown whether the PSE device is using its Primary Power Source or its Backup Power Source, it is indicated as "Unknown".
  - PD device
    If the device is a PD device, it can either run on its local power supply or it can use the PSE as power source. It can also use both its local power supply and the PSE.
  - Reserved
    If it is unknown what power supply the PD device is using it is indicated as "Unknown".

- **Power Priority**
  The Power Priority represents the priority of the PD device or the power priority associated with the PSE type device's port that is sourcing the power. There are three levels of power priority. The three levels are: Critical, High and Low. If the power priority is unknown it is indicated as "Unknown".

- **Maximum Power**
  The Maximum Power Value contains a numerical value that indicates the maximum power in watts required by a PD device from a PSE device or the minimum power a PSE device is capable of sourcing over a maximum length cable based on its current configuration.
  The maximum allowed value is 102.3 W. If the device indicates a value higher than 102.3 W, it is represented as "reserved".

Check the ☐Auto-refresh☐ box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the ☐Refresh☐ button.

3.7.3 Port Statistics

This page provides an overview of all LLDP traffic. Two types of counters are shown. Global counters are counters that refer to the whole switch, while local counters refer to per port counters for the switch.

LLDP Global Counters

- **Neighbor entries were last changed**
  Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

- **Total Neighbors Entries Added**
  Shows the number of new entries added since switch reboot.

- **Total Neighbors Entries Deleted**
  Shows the number of new entries deleted since switch reboot.

- **Total Neighbors Entries Dropped**
  Shows the number of LLDP frames dropped due to the entry table being full.

- **Total Neighbors Entries Aged Out**
  Shows the number of entries deleted due to Time-To-Live expiring.

LLDP Statistics Local Counters

The displayed table contains a row for each port. The columns hold the following information:

- **Local Port**
  The port on which LLDP frames are received or transmitted.

- **Tx Frames**
  The number of LLDP frames transmitted on the port.

- **Rx Frames**
  The number of LLDP frames received on the port.
- **Rx Errors**
  The number of received LLDP frames containing some kind of error.
- **Frames Discarded**
  If a LLDP frame is received on a port and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received or when the entry ages out.
- **TLVs Discarded**
  Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
- **TLVs Unrecognized**
  The number of well-formed TLVs, but with an unknown type value.
- **Org. Discarded**
  If a LLDP frame is received with an organizationally TLV, but the TLV is not supported the TLV is discarded and counted.
- **Age-Outs**
  Each LLDP frame contains information about how much time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed and the Age-Out counter is incremented.

Check the ‘Auto-refresh’ box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the ‘Refresh’ button.

By clicking the ‘Clear’ button, the local counters are cleared. To clear all counters (including the global counters) a reboot of the switch has to be done.

3.8 Loop Protection

This page displays the Loop Protection Status of the ports of this switch.

Loop Protection Status

- **Port**
  The switch port number of the logical port.
- **Action**
  The currently configured port action.
- **Transmit**
  The currently configured port transmit mode.
- **Loops**
  The number of loops detected on this port.
- **Status**
  The current loop protection status of the port.
- **Loop**
  Whether a loop is currently detected on the port.

- **Time of Last Loop**
  The time of the last detected loop event.

Check the ?Auto-refresh? box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the ?Refresh? button.

3.9 Spanning Tree

3.9.1 Bridge Status

The STP Detailed Bridge Status page provides detailed information on a single STP bridge instance, along with the port state for all associated active ports.

The page contains two tables with the following information.

STP Bridge Status

- **Bridge Instance**
  The Bridge instance: CIST, MSTI, ...
- **Bridge ID**
  The Bridge ID of this Bridge instance.
- **Root ID**
  The Bridge ID of the currently elected root bridge.
- **Root Cost**
  The Root Path Cost for the Root Bridge is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
- **Root Port**
  The switch port currently assigned the root port role.
- **Regional Root**
  The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge (For the CIST instance only).
- **Internal Root Cost**
  The Regional Root Path Cost for the Regional Root Bridge is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge (For the CIST instance only).
- **Topology Flag**
  The current state of the Topology Change Flag of this Bridge instance.
- **Topology Change Count**
  The number of times where the topology change flag has been set (during a one-second interval).
- **Topology Change Last**
  The time passed since the Topology Flag was last set.

CIST Ports & Aggregations State

- **Port**
  The switch port number of the logical STP port.
- **Port ID**
  The Port ID as used by the STP protocol. This is the priority part and the logical port index of the bridge port.

- **Role**
  The current STP port role. The port role can be one of the following values:
  AlternatePort BackupPort RootPort DesignatedPort
- **State**
  The current STP port state. The port state can be one of the following values:
  Discarding Learning Forwarding
- **Path Cost**
  The current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value.
- **Edge**
  The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.
- **Point-to-Point**
  The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state.
- **Uptime**
  The time since the bridge port was last initialized.

Check the Auto-refresh box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the Refresh button.

3.9.2 Port Status

This page displays the STP CIST Port Status for physical ports of the currently selected switch.

STP Port Status

- **Port**
  The switch port number of the logical STP port.
- **CIST Role**
  The current STP port role of the CIST port. The port role can be one of the following values:
  AlternatePort BackupPort RootPort DesignatedPort Disabled
- **CIST State**
  The current STP port state of the CIST port. The port state can be one of the following values:
  Discarding Learning Forwarding
- **Uptime**
  The time since the bridge port was last initialized.

Check the Auto-refresh box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the Refresh button.

3.9.3 Port Statistics

This page displays the STP Port Statistics counters of bridge ports in the currently selected switch.

STP Statistics

The STP port statistics counters are:

- **Port**
  The switch port number of the logical STP port.
- **MSTP**
  The number of MSTP BPDU's received/transmitted on the port.
- **RSTP**
  The number of RSTP BPDU's received/transmitted on the port.
- **STP**
  The number of legacy STP Configuration BPDU's received/transmitted on the port.
- **TCN**
  The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.
- **Discarded Unknown**
  The number of unknown Spanning Tree BPDU's received (and discarded) on the port.
- **Discarded Illegal**
  The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

Check the ⍰Auto-refresh⍰ box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the ⍰Refresh⍰ button.

By clicking the ⍰Clear⍰ button, the counters are cleared and reset.

3.10 IGMP Snooping

3.10.1 Status

This page provides the IGMP Snooping Status.

Statistics

- **VLAN ID**
  The VLAN ID of the entry.
- **Querier Version**
  Currently working Querier Version.
- **Host Version**
  Currently working Host Version.
- **Querier Status**
  The Querier status can be "ACTIVE" or "IDLE". "DISABLE" denotes that the specific interface is administratively disabled.
- **Queries Transmitted**
  The number of Transmitted Queries.
- **Queries Received**
  The number of Received Queries.

- **V1 Reports Received**
  The number of Received V1 Reports.
- **V2 Reports Received**
  The number of Received V2 Reports.
- **V3 Reports Received**
  The number of Received V3 Reports.
- **V2 Leaves Received**
  The number of Received V2 Leaves.

Router Port

This section displays which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

- **Port**
  Switch port number.
- **Status**
  Indicates whether the specific port is a router port or not:
  - ?Static?: The specific port is configured to be a router port.
  - ?Dynamic?: The specific port has learnt to be a router port.
  - ?Both?: The specific port is configured or has learnt to be a router port.

Check the ?Auto-refresh? box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the ?Refresh? button.

By clicking the ?Clear? button, all the Statics counters are cleared and reset.

3.10.2 Group Information

This page shows the entries in the IGMP Snooping Group Table. The IGMP Group Table is sorted first by VLAN ID then by group.

Navigating the IGMP Group Table

Each page shows up to 99 entries from the IGMP Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table.

The "Start from VLAN", and "group address" input fields allow the user to select the starting point in the IGMP Group Table. Clicking the ?Refresh? button will update the displayed table starting from that or the closest next IGMP Group Table match. In addition, the two input fields will - upon a ?Refresh? button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

IGMP Group Table Columns

- **VLAN ID**
  VLAN ID of the group.
- **Groups**
  Group address of the displayed group.
- **Port Members**
  Ports under this group.

Check the "Auto-refresh" box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the "Refresh" button.

3.11 DHCP

3.11.1 Snooping Table

This page displays the dynamic IP assigned information after the DHCP Snooping mode is disabled. All DHCP clients that obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.

Navigating the DHCP snooping Table

Each page shows up to 99 entries from the Dynamic DHCP snooping table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic DHCP snooping Table.

The "MAC address" and "VLAN" input fields allows the user to select the starting point in the Dynamic DHCP snooping table. Clicking the button "Refresh" will update the displayed table starting from that or the closest next Dynamic DHCP snooping table match. In addition, the two input fields will - upon a "Refresh" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

DHCP Snooping Table Columns

- **MAC Address**
  User MAC address of the entry.
- **VLAN ID**
  VLAN-ID in which the DHCP traffic is permitted.
- **Source Port**
  Switch Port Number for which the entries are displayed.
- **IP Address**
  User IP address of the entry.
- **IP Subnet Mask**
  User IP subnet mask of the entry.
- **DHCP Server**
  DHCP Server address of the entry.

To enable to refresh the page automatically check the box next to "Auto-refresh". Automatic refresh occurs every 3 seconds.
To flush all dynamic entries, click the "Clear" button.
|<< Updates the table starting from the first entry in the Dynamic DHCP snooping table.
>> Updates the table, starting with the entry after the last entry currently displayed.

3.11.2 Detailed Statistics

This page provides detailed statistics for the DHCP Snooping. Notice that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by a L3 forwarding mechanism. Also clearing the statistics on specific port may not take effect on global statistics since it gathers the different layer overview.

On the top right, two drop-down menus allow to determine which statistics should be displayed.

This first one is the DHCP user select box. It helps to determine which user is affected. It can either be only "Normal Forward", "Client" or "Snooping". By choosing "Combined", all DHCP users are displayed.

With the second one (Port select box), the port for which the packets statistics should be presented can be chosen.

Receive and Transmit Packets

- **Rx and Tx Discover**
  The number of discover (option 53 with value 1) packets received and transmitted.
- **Rx and Tx Offer**
  The number of offer (option 53 with value 2) packets received and transmitted.
- **Rx and Tx Request**
  The number of request (option 53 with value 3) packets received and transmitted.
- **Rx and Tx Decline**
  The number of decline (option 53 with value 4) packets received and transmitted.
- **Rx and Tx ACK**
  The number of ACK (option 53 with value 5) packets received and transmitted.
- **Rx and Tx NAK**
  The number of NAK (option 53 with value 6) packets received and transmitted.
- **Rx and Tx Release**
  The number of release (option 53 with value 7) packets received and transmitted.
- **Rx and Tx Inform**
  The number of inform (option 53 with value 8) packets received and transmitted.
- **Rx and Tx Lease Query**
  The number of lease query (option 53 with value 10) packets received and transmitted.
- **Rx and Tx Lease Unassigned**
  The number of lease unassigned (option 53 with value 11) packets received and transmitted.
- **Rx and Tx Lease Unknown**
  The number of lease unknown (option 53 with value 12) packets received and transmitted.
- **Rx and Tx Lease Active**
  The number of lease active (option 53 with value 13) packets received and transmitted.
- **Rx Discarded checksum error**
  The number of discarded packets that the IP/TCP/UDP checksum is error.
- **Rx Discarded from Untrusted**
  The number of discarded packets that are coming from untrusted ports.

Check the "Auto-refresh" box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the "Refresh" button.

By clicking the "Clear" button, all the counters for the selected port are cleared and reset.

3.12 Security

3.12.1 Port Security

The Port Security is a module with no direct configuration. The configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

3.12.1.1 Switch

The Port Security Switch Status page shows the Port Security status. This page is divided into two sections - one with a legend of user modules and one with the actual port status.

User Module Legend

The legend shows all user modules that may request Port Security services.

- **User Module Name**
  The full name of a module that may request Port Security services.
- **Abbr**
  A one-letter abbreviation of the user module. This is used in the Users column in the port status table below.

Port Status

The table has one row for each port on the switch and a number of columns, which are:

- **Port**
  The port number for which the status applies. Click on the port number to see the status for this particular port. The user is redirected to the Port Security Port Status page (see chapter 3.12.1.2).
- **Users**
  Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.
- **State**
  Shows the current state of the port. It can take one of four values:
  - Disabled: No user modules are currently using the Port Security service.
  - Ready: The Port Security service is in use by at least one user module and is awaiting frames from unknown MAC addresses to arrive.
  - Limit Reached: The Port Security service is enabled by at least the Limit Control user module. That module has indicated that the limit is reached and no more MAC addresses should be taken in.
  - Shutdown: The Port Security service is enabled by at least the Limit Control user module and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Port Security Limit Control Configuration web-page (chapter 6.3.1).

- **MAC Count (Current, Limit)**
  The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.
  If no user modules are enabled on the port, the Current column will show a dash (-).
  If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

Check the "Auto-refresh" box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the "Refresh" button.

3.12.1.2 Port

The Port Security Port Status page shows the MAC addresses secured by the Port Security module.

- **MAC Address & VLAN ID**
  The MAC address and the VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "*No MAC addresses attached*" is displayed.
- **State**
  Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.
- **Time of Addition**
  Shows the date and time when this MAC address was first seen on the port.
- **Age/Hold**
  If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin.
  If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Use the drop-down menu to select for which port the status should be shown.

Check the "Auto-refresh" box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the "Refresh" button.

3.12.2 802.1X – Network Access Server

3.12.2.1 Switch

The Network Access Server Switch Status page provides an overview of the current NAS port states for the selected switch.

- **Port**
  The switch port number. Click on a number to navigate to the detailed NAS statistics for this port (chapter 3.12.2.2).
- **Admin State**
  The port's current administrative state. Refer to NAS "Admin State" (chapter 6.3.2) for a description of possible values.
- **Port State**
  The current state of the port. Refer to NAS "Port State" (chapter 6.3.2) for a description of the individual states.

- **Last Source**
  The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication and the most recently received frame from a new client for MAC-based authentication.
- **Last ID**
  The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication and the source MAC address from the most recently received frame from a new client for MAC-based authentication.
- **QoS Class**
  QoS Class assigned to the port by the RADIUS server if enabled.
- **Port VLAN ID**
  The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.
  If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID.
  If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

Check the ‘Auto-refresh’ box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the ‘Refresh’ button.

3.12.2.2 Port

This page provides detailed NAS statistics for a specific switch port, running an EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it only shows selected backend server (RADIUS Authentication Server) statistics.

By using the port select box, it can be selected which port details are to be displayed.

Port State

- **Admin State**
  The port's current administrative state. Refer to NAS ‘Admin State’ (chapter 6.3.2) for a description of possible values.
- **Port State**
  The current state of the port. Refer to NAS ‘Port State’ (chapter 6.3.2) for a description of the individual states.
- **QoS Class**
  The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.
- **Port VLAN ID**
  The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.
  If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID.
  If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

Port Counters

- **EAPOL Counters**
  These supplicant frame counters are available for the following administrative states:
  - Force Authorized
  - Force Unauthorized
  - Port-based 802.1X
  - Single 802.1X
  - Multi 802.1X

EAPOL Counters			
Direction	**Name**	**IEEE Name**	**Description**
Rx	Total	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
Rx	Response ID	dot1xAuthEapolRespIdFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.
Rx	Responses	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.
Rx	Start	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
Rx	Logoff	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that have been received by the switch.
Rx	Invalid Type	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
Rx	Invalid Length	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
Tx	Total	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
Tx	Request ID	dot1xAuthEapolReqIdFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.
Tx	Requests	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.

Tableau 3.1: EAPOL Counters

- **Backend Server Counters**

  These backend (RADIUS) frame counters are available for the following administrative states:
  - Port-based 802.1X
  - Single 802.1X
  - Multi 802.1X
  - MAC-based Auth.

Backend Server Counters			
Direction	**Name**	**IEEE Name**	**Description**
Rx	Access Challenges	dot1xAuthBackendAccessChallenges	**802.1X-based:** Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch. **MAC-based:** Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).
Rx	Other Requests	dot1xAuthBackendOtherRequests ToSupplicant	**802.1X-based:** Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method. **MAC-based:** Not applicable.
Rx	Auth. Successes	dot1xAuthBackendAuthSuccesses	**802.1X- and MAC-based:** Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.
Rx	Auth. Failures	dot1xAuthBackendAuthFails	**802.1X- and MAC-based:** Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.
Tx	Responses	dot1xAuthBackendResponses	**802.1X-based:** Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted. **MAC-based:** Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.

Tableau 3.2: Backend Server Counters

- **Last Supplicant/Client Info**
  This gives information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:
  - Port-based 802.1X
  - Single 802.1X
  - Multi 802.1X
  - MAC-based Auth.

Last Supplicant/Client Info		
Name	**IEEE Name**	**Description**
MAC Address	dot1xAuthLastEapolFrameSource	The MAC address of the last supplicant/client.
VLAN ID		The VLAN ID on which the last frame from the last supplicant/client was received.
Version	dot1xAuthLastEapolFrameVersion	**802.1X-based:** The protocol version number carried in the most recently received EAPOL frame. **MAC-based:** Not applicable.
Identity		**802.1X-based:** The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. **MAC-based:** Not applicable.

Tableau 3.3: Last Supplicant/Client Info

Selected Counters

The Selected Counters table is visible when the port is in one of the following administrative states:

- **Multi 802.1X**
- **MAC-based Auth.**

The table is identical to and placed next to the Port Counters table. It will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.

Attached MAC Addresses

- **Identity**
  Shows the identity of the supplicant, as received in the Response Identity EAPOL frame.
  Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows No supplicants attached.
  This column is not available for MAC-based Auth.

- **MAC Address**
  For Multi 802.1X, this column holds the MAC address of the attached supplicant.
  For MAC-based Auth., this column holds the MAC address of the attached client.
  Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table.
  If no clients are attached, it shows No clients attached.

- **VLAN ID**
  This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.

- **State**
  The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for "Hold Time" (chapter 6.3.2) seconds.

- **Last Authentication**
  Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

Check the "Auto-refresh" box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the "Refresh" button.

Click the "Clear" button to clear the counters for the selected port. This button is available in the following modes: Force Authorized, Force Unauthorized, Port-based 802.1X and Single 802.1X.

To clear both the port counters and all the attached client's counters, click the "Clear All" button. However, the "Last Client" will not be cleared. This button is available in the following modes: Multi 802.1X and MAC-based Auth.X.

To only clear the currently selected client's counters, click "Clear This" This button is available in the following modes: Multi 802.1X and MAC-based Auth.X.

3.12.3 ACL Status

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined by the switch. It is a conflict, if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs on this switch is 128.

On the top right, a drop-down menu allows to determine which ACL users should be displayed. By choosing "combined", all ACL users are displayed.

The ACL status list gives information about:

- **User**
  Indicates the ACL user.

- **ACE**
  Indicates the ACE ID on the local switch.

- **Frame Type**
  Indicates the frame type of the ACE. Possible values are:
  - Any: The ACE will match any frame type.
  - EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.
  - ARP: The ACE will match ARP/RARP frames.
  - IPv4: The ACE will match all IPv4 frames.
  - IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.
  - IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.
  - IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.
  - IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.
  - IPv6: The ACE will match all IPv6 standard frames.

- **Action**
  Indicates the forwarding action of the ACE.
  - Permit: Frames matching the ACE may be forwarded and learned.
  - Deny: Frames matching the ACE are dropped.
  - Filter: Frames matching the ACE are filtered.

- **Rate Limiter**
  Indicates the rate limiter number of the ACE. The allowed range is 1 to 15. When "Disabled" is displayed, the rate limiter operation is disabled.
- **Mirror**
  Specifies the mirror operation of this port. It defines if frames received on the port are mirrored.
- **CPU**
  Forwards the packets that matched the specific ACE to CPU.
- **Counter**
  The counter indicates the number of times the ACE was hit by a frame.
- **Conflict**
  Indicates the hardware status of the specific ACE.

Check the "Auto-refresh" box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the "Refresh" button.

3.12.4 AAA

3.12.4.1 Radius Overview

The RADIUS Server Status Overview page provides an overview of the status of the RADIUS servers configurable on the RADIUS Server Configuration page (see chapter 6.3.7).

- **#**
  The RADIUS server number. Click on the number to navigate to the detailed statistics for this server.
- **IP Address**
  The IP address of this server.
- **Authentication Port**
  UDP port number for authentication.
- **Authentication Status**
  Describes the current status of the server. This field takes one of the following values:
  - Disabled: The server is disabled.
  - Not Ready: The server is enabled, but the IP communication is not yet up and running.
  - Ready: The server is enabled, the IP communication is up and running and the RADIUS module is ready to accept access attempts.
  - Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
- **Accounting Port**
  UDP port number for accounting.
- **Accounting Status**
  Describes the current status of the server. This field takes one of the following values:
  - Disabled: The server is disabled.
  - Not Ready: The server is enabled, but the IP communication is not yet up and running.
  - Ready: The server is enabled, the IP communication is up and running and the RADIUS module is ready to accept access attempts.
  - Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Check the ‘Auto-refresh’ box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the ‘Refresh’ button.

3.12.4.2 Radius Details

The RADIUS Details page provides detailed authentication and accounting statistics for a particular RADIUS server.

By using the drop-down menu, a user can switch between the backend servers and select so a server to show the details for.

RADIUS Authentication Statistics

- **Packet Counters**
  The RADIUS authentication server packet counter is divided into ‘Receive Packets’ and ‘Transmit Packets’. There are seven receive (Rx) and four transmit (Tx) counters.

Packet Counters			
Direction	**Name**	**RFC4668 Name**	**Description**
Rx	Access Accepts	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	Access Rejects	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	Access Challenges	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	Malformed Access Responses	radiusAuthClientExtMalformed AccessResponses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
Rx	Bad Authenticators	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx	Unknown Types	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.
Rx	Packets Dropped	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Tx	Access Requests	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Tx	Access Retransmissions	radiusAuthClientExtAccess Retransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Tx	Pending Requests	radiusAuthClientExtPendingRequests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept,

Packet Counters			
Direction	**Name**	**RFC4668 Name**	**Description**
			Access-Reject, Access-Challenge, timeout or retransmission.
Tx	Timeouts	radiusAuthClientExtTimeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

Tableau 3.4: RADIUS Authentication Statistics – Packet Counters

- **Other Info**
  This section contains information about the state of the server and the latest round-trip time.

Other Info		
Name	**RFC4668 Name**	**Description**
IP Address	–	IP address and UDP port for the authentication server in question.
State	–	Shows the state of the server. It takes one of the following values: "Disabled": The selected server is disabled. "Not Ready": The server is enabled, but the IP communication is not yet up and running. "Ready": The server is enabled, the IP communication is up and running, and the RADIUS module is ready to accept access attempts. "Dead (X seconds left)": Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAuthClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

Tableau 3.5: RADIUS Authentication Statistics – Other Info

RADIUS Accounting Statistics

- **Packet Counters**
  The RADIUS Accounting server packet counter is divided into ‘Receive Packets’ and ‘Transmit Packets’. There are five receive (Rx) and four transmit (Tx) counters.

Packet Counters			
Direction	**Name**	**RFC4670 Name**	**Description**
Rx	Responses	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	Malformed Responses	radiusAccClientExtMalformedResponses	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.
Rx	Bad Authenticators	radiusAcctClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	Unknown Types	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	Packets Dropped	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx	Requests	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx	Retransmissions	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx	Pending Requests	radiusAccClientExtPendingRequests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.
Tx	Timeouts	radiusAccClientExtTimeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

Table 3.6: RADIUS Accounting Statistics – Packet Counters

- **Other Info**
  This section contains information about the state of the server and the latest round-trip time.

Other Info		
Name	**RFC4670 Name**	**Description**
IP Address		IP address and UDP port for the accounting server in question.
State		Shows the state of the server. It takes one of the following values: Disabled: The selected server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAccClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

Tableau 3.7: RADIUS Accounting Statistics Other Info

Check the Auto-refresh box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the Refresh button.

To clear the counters for the selected server, click the Clear button. The "Pending Requests" counters will not be cleared by this operation.

3.13 QoS

3.13.1 QoS Statistics

The QoS Statistics page provides statistics (Queuing Counters) for the different queues for all switch ports.

The displayed counters are:

- **Port**
  The logical port for the settings contained in the same row.
- **Qn**
  There are 8 QoS queues per port. Q0 is the lowest priority queue.
- **Rx/Tx**
  The number of received (Rx) and transmitted (Tx) packets per queue.

Check the Auto-refresh box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the Refresh button.

To clear the counters for all ports, click the Clear button.

3.13.2 QCL Status

This page shows the QoS Control List (QCL) Status by different QCL users. Each row describes the QCE that is defined. It is a conflict, if a specific QCE is not applied to the hardware due to hardware limitations.

The user can select what selection of QCEs will be shown. By clicking on the drop down menu on the top right, The QCL status can be chosen, to show only the "Static" entries, only the "Conflict" entries or all entries "Combined".

- **User**
  Indicates the QCL user.
- **QCE**
  Indicates the QCE ID.
- **Port**
  Indicates the list of ports configured with the QCE.
- **Frame Type**
  Indicates the type of frame. Possible values are:
  - Any: Match any frame type.
  - Ethernet: Match EtherType frames.
  - LLC: Match LLC frames.
  - SNAP: Match SNAP frames.
  - IPv4: Match IPv4 frames.
  - IPv6: Match IPv6 frames.
- **Action**
  Indicates the classification action taken on the ingress frame, if the configured parameters are matched with the frame's content. Possible actions are:
  - CoS: Classify Class of Service.
  - DPL: Classify Drop Precedence Level.
  - DSCP: Classify DSCP value.
- **Conflict**
  Displays the Conflict status of the QCL entries, as hardware resources are shared by multiple applications. It may happen, that resources, required to add a QCE, may not be available. In that case conflict status is shown as 'Yes', otherwise it is always 'No'.
  Please note that a conflict can be resolved by pressing "Resolve Conflict" button. The H/W resources required to add a QCL entry will be released in case the conflict status for any QCL entry is 'yes'.

Check the "Auto-refresh" box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the page manually click on the "Refresh" button.

4. Power Supply

The "POWER SUPPLY" page contains information relating to the battery and its use.

- **Battery**
  The capacity displayed is the battery's minimum capacity. The value is given for information purposes and cannot be changed. It differs from the capacity's typical value given on the product label

- **Stealth Mode**
  The Stealth Mode allows supervision to disconnect the product to relieve network load. The product automatically reconnects once the remaining autonomy has reached the guaranteed autonomy percentage selected by the administrator during configuration.
  To enable the Stealth Mode, the threshold (percentage of the guaranteed autonomy when Stealth Mode is used) must be defined: 25% / 50% / 75% / Disabled. Click on "OK" to the right to save the new threshold.

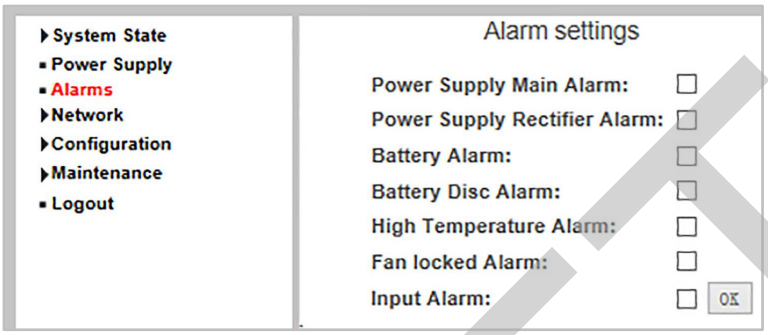
- **Eco Mode**
  When enabled, the Eco Mode improves power efficiency at low charge (<20% of I_{max}), while guaranteeing a defined percentage of autonomy. In the factory settings, the Eco Mode is disabled by default.
  To enable the Eco Mode, the threshold (percentage of the autonomy that must remain available to the user) must be defined: 50% / 60% / 70% / 80% / Disabled. Click on "OK" to the right to save the new threshold.

The page is refreshed automatically every 3 seconds. To manually refresh the data, click on the "Refresh" button.

5. Alarms

The "ALARMS" page contains the alarm settings available which can be reported thanks to a dry contact.

Select one or more alarms and click OK to save the alarms that will be reported.



The page is refreshed automatically every 3 seconds. To manually refresh the data, click on the "Refresh" button.

6. Network

6.1 Port Configuration

6.1.1 Ports

The page allows the configuration of the switch's port specifications. In the pictured table, current characteristics for each port are displayed and can also be configured.

- **Port**
  The featured numbers correspond to the logical port number for this row.
- **Link**
  The current link state is displayed graphically. The color indicates if a link has been created to the respective port:
  - Red link down (no link)
  - Green link up (link established)
- **Current Link Speed**
  The indicated value provides the current link speed of the port. The word "Down" indicates, that no link has been established (link down).
- **Configured Link Speed**
  For a given switch port one of the available link speeds can be selected. Only speeds supported by the specific port are shown. Possible speeds are:
  - "Disabled": The port is disabled.
  - "Auto": This setting allows the port to automatically negotiate the speed with the link partner. It determines the highest speed that is compatible with the connected device and applies it.
  - "10Mbps HDX": Forces the Cu port (Ethernet port) to work in 10 Mbps half duplex mode.
  - "10Mbps FDX": Forces the Cu port (Ethernet port) to work in 10 Mbps full duplex mode.
  - "100Mbps HDX": Forces the Cu port (Ethernet port) to work in 100 Mbps half duplex mode.
  - "100Mbps FDX": Forces the Cu port (Ethernet port) to work in 100 Mbps full duplex mode.
  - "1Gbps FDX": Forces the Cu port (Ethernet port) to work in 1 Gbps full duplex mode.
  - "100Mbps FDX": Forces the SFP port to work in 100 Mbps full duplex mode.
  - "1Gbps FDX": Forces the SFP port to work in 1 Gbps full duplex mode
- **Flow Control**
  This is a flow control mechanism for a variety of port configurations. Full-duplex ports (FDX) use 802.3x flow control. Half-duplex ports (HDX) use backpressure flow control.
  When "Auto" Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner.
  When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation.
  The flow control is disabled by default. Check the "Configured" column to use flow control. This setting is related to the setting for Configured Link Speed.
  NOTICE: The 100FX standard doesn't support Auto-Negotioation, so when in 100FX mode the flow control capabilities will always be shown as "disabled".
- **Maximum Frame Size**
  The maximum frame size allowed for the switch port can be set here. The default setting is 9600, which

is to support Jumbo frames.

- **Excessive Collision Mode**
  To configure the port's transmit collision behavior, use the drop-down menu.
  - "Discard": Discards frame after 16 collisions (default).
  - "Restart": Restarts backoff algorithm after 16 collisions for automatic restart of the port.

After the configuration is set, click "Save" to save and activate the settings. To undo any changes made locally and revert to previously saved values, click "Reset". By clicking on the "Refresh" button on the top right, the page is refreshed, undoing any changes made locally without saving.

6.1.2 Aggregation

The user can set up multiple links among multiple switches. The Link Aggregation is a method to tie several physical ports together as one logic port to enlarge the bandwidth.

IMPORTANT REMARK!

If any port in a link aggregation group is disconnected, the other connected ports in this aggregation group will share the load of the data packet, which should normally be sent to the disconnected port.

6.1.2.1 Static Aggregation

This page is used to configure the aggregation hash mode and the static aggregation group.

Aggregation Mode Configuration

To configure the Aggregation Mode, the Hash Code Contributors have to be defined and enabled. By default, all the contributors are activated (box checked).

- **Source MAC Address**
  The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, the Source MAC Address is enabled.
- **Destination MAC Address**
  The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, the Destination MAC Address is disabled.
- **IP Address**
  The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, the IP Address is enabled.
- **TCP/UDP Port Number**
  The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, the TCP/UDP Port Number is enabled.

Aggregation Group Configuration

The configuration of the Aggregation Group is done by assigning the ports to one group or letting them in their normal mode without any aggregation. Note that this switch only allows a maximum of 8 ports to be aggregated as 1 static trunk group at the same time.

- **Group ID**
  The Group ID is the identifier of one aggregation group and is defined by the settings contained in the same row. The Group ID "Normal" indicates there is no aggregation. This switch supports up to 5 groups with 2 to 8 ports tied as one group. Only one group ID is valid per port.

- **Port Member**
  Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the "Normal" radio button to remove the port from the aggregation. Each port can only be assigned to one aggregation group. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

After the configuration is set, click "Save" to save and activate the settings. To undo any changes made locally and revert to previously saved values, click "Reset".

6.1.2.2 LACP

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between partner systems that require high-speed redundant links. The link aggregation allows to group up to eight consecutive ports into a single dedicated connection. This feature can expand the bandwidth to a device on the network. The LACP operation requires a full-duplex mode. For more detailed information, refer to the IEEE 802.3ad standard.

LACP Port Configuration

The user can create the dynamic aggregation group by configuring the LACP Port settings.

- **Port**
  The switch port number

- **LACP Enabled**
  Controls whether the LACP is enabled on this switch port. The LACP will form an aggregation when 2 or more ports are connected to the same partner. Up to 5 aggregations are supported. The checking or unchecking of the box enables or disables the LACP function of the corresponding port.

- **Key**
  The key value incurred by the port ranges between 1 and 65535.
  The "Auto" setting will set the key as appropriate by the physical link speed:
  10Mb = 1, 100Mb = 2, 1Gb = 3.
  Using the "Specific" setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group while ports with different keys cannot.

- **Role**
  The Role shows the LACP activity status. The "Active" will transmit the LACP packets each second, while "Passive" will wait for a LACP packet from a partner (speak if spoken to).

- **Timeout**
  The Timeout controls the period between BPDU transmissions. "Fast" will transmit the LACP packets each second, while "Slow" will wait for 30 seconds before sending a LACP packet.

- **Prio**
  The Prio controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device, this parameter will control which ports will be active and which ports will be in a backup role. A lower number means a greater priority.

After the configuration is set, click "Save" to save and activate the settings. To undo any changes made locally and revert to previously saved values, click "Reset".

6.1.3 Mirroring

The Mirroring function provides the monitoring of the network traffic. To debug network problems, selected traffic can be copied, or mirrored, on a **mirror port** where a frame analyzer can be attached to analyze the frame flow. It forwards a copy of each incoming or outgoing packet from one port of a network switch to another port, where the packet can be studied. It enables the manager to keep close track of the switch performance and alter it if necessary.

The traffic to be copied on the mirror port is selected as follows:

- All frames received on a given port (also known as ingress or source mirroring).
- All frames transmitted on a given port (also known as egress or destination mirroring).

Mirror Configuration - Port to mirror to

The ‘Port to mirror’ is also known as the mirror port. Frames from ports, that have either source (rx) or destination (tx) mirroring enabled, are mirrored on this port. ‘Disabled’ disables the mirroring.

Mirror Port Configuration

The following information is used for Rx and Tx enabling.

- **Port**
  The logical port for the settings contained in the same row.
- **Mode**
  To configure the Mirror Port, the source port mirror mode has to be selected:
  - Rx only: Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.
  - Tx only: Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.
  - Disabled: Neither frames transmitted nor frames received are mirrored.
  - Enabled: Frames received and frames transmitted are mirrored on the mirror port.

  Note:
  - For a given port, a frame is only transmitted once. It is therefore not possible to mirror the Tx frames of a mirror port. Because of this, the mode for the, in the mirror configuration, selected mirror port is limited to ‘Disabled’ or ‘Rx only’.

IMPORTANT REMARK!

A fast speed port can’t be set to mirror a low speed port. For example, there is problem when trying to mirror a 100 Mbps port to a 10 Mbps port. This means, the destination port should have equal or higher speed comparing to the source port. Further, the source port and the destination port should not be the same one.

After the configuration is set, click ‘Save’ to save and activate the settings. To undo any changes made locally and revert to previously saved values, click ‘Reset’.

6.1.4 Thermal Protection

The thermal protection is a tool to detect and to protect the working switch from overheat. When the switch detects, that a port temperature is higher than the defined temperature, the system will disable this port to protect the switch itself.

When the temperature exceeds the configured thermal protection temperature, ports will be turned off in order to decrease the power consumption. It is possible to arrange the ports with different priorities. Each priority can be given a temperature at which the corresponding ports shall be turned off.

Thermal Protection Configuration

- **Temperature settings for priority groups**
  The switch supports 4 thermal protection priority groups. The user can define a specific temperature at which the ports with the corresponding priority will be turned off. Temperatures between 0 and 255°C are supported.
- **Port priorities**
  For each port the priority group, the port belongs to, has to be defined. Four priorities are supported.

IMPORTANT REMARK!

By default, all ports of the switch belong to the priority group 0, with a protection temperature of 255°C.

After the configuration is set, click ‘Save’ to save and activate the settings. To undo any changes made locally and revert to previously saved values, click ‘Reset’.

6.1.5 Green Ethernet

The Green Ethernet allows the user to configure the Port Power Savings features and to optimize so the power consumption of the switch.

What is EEE

EEE is a power saving option that reduces the power usage when there is low or no traffic utilization.

The EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 µs for 1Gbit links and 30 µs for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup time information using the LLDP protocol.

EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode.

When a port is powered down for saving power, outgoing traffic is stored in a buffer until the port is powered up again. Because there is some overhead in turning the port down and up, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic.

Port Power Savings Configuration - Optimize EEE for

The switch can be set to optimize EEE for either:

- ‘Power’: best power saving or
- ‘Latency’: least traffic latency.

Port Configuration

- **Port**
  The switch port number of the logical port.
- **ActiPHY**
  By checking the box, the "link down power savings" are enabled for this switch port.
  ActiPHY works by lowering the power for a port when there is no link. The port is powered up for a short moment in order to determine if a cable is inserted.
- **PerfectReach**
  By checking the box, the "cable length power savings" are enabled for this switch port.
  The PerfectReach works by determining the cable length and lowering the power for ports with short cables.
- **EEE**
  By checking the box, the EEE is enabled for this switch port.
  For maximizing power savings, the circuit isn't started once transmit data is ready for a port. Instead the data is queued until a burst of data is ready to be transmitted. This will give some traffic latency.
  If desired, it is possible to minimize the latency for specific frames by mapping the frames to a specific queue (done with QOS) and then mark the queue as an "urgent queue". When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.
- **EEE Urgent Queues**
  Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted.

After the configuration is set, click "Save" to save and activate the settings. To undo any changes made locally and revert to previously saved values, click "Reset".

6.2 PoE

6.2.1 PoE Setting

This page allows the user to inspect and configure the current PoE port settings.

Power Over Ethernet Configuration

- **Reserved Power determined by**
  There are two modes for configuring how the ports may reserve power.
  - "Auto": The Switch automatically assigns the maximum amount of power that each port may reserve according to the detected PD class. For more information regarding the PD Class, please refer to the IEEE 802.3af / 802.3at / 802.3bt definition.
  - "Manual": The maximum amount of power that a port will reserve can be customized by the user in the table below.

  For all modes: If a port uses more power than the reserved power for the port, the port is shut down.
- **Power Management Mode**
  There are two modes for configuring when to shut down the ports.
  - "Actual Consumption": In this mode, the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver (budget) or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down.

- "Reserved Power": In this mode, the ports are shut down when the total amount of reserved power exceeds the amount of power that the power supply can deliver. In this mode, the port power is not turned on if the PD requests more power than available from the power supply.

PoE Power Supply Configuration

For being able to determine the amount of power the PD may use, it must be defined what amount of power a power source can deliver.

Valid values are in the range 0 to 180 Watts.

PoE Port Configuration

- **Port**
  This is the logical port number for this row.
  Ports that are not PoE-capable are not displayed here and thus impossible to configure PoE for.
- **PoE Mode**
  The PoE Mode represents the PoE operating mode for the port.
  - Disabled: PoE is disabled for the port.
  - PoE: Enables PoE IEEE 802.3af (Class 4; PDs limited to 15.4 W)
  - PoE+: Enables PoE+ IEEE 802.3at (Class 4; PDs limited to 30 W)
  - PoE-BT (HiPoE): Enables 4PPoE IEEE 802.3bt (Class 8; PDs limited to 90 W)
- **Priority**
  The Priority represents the ports priority. There are three levels of power priority named Low, High and Critical.
  The priority is used in the case where the remote devices require more power than the power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.
- **Maximum Power**
  The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device.
  The maximum allowed value for PoE is 15.4 W
  The maximum allowed value for PoE+ is 30 W.
  The maximum allowed value for PoE-BT (HiPoE) is 90 W.
- **Description**
  In this field the user can enter additional information. This information will be displayed in the PoE status overview (chapter 3.6.6).

6.2.2 DAM Setting

In this page the function DAM (Device Activity Monitoring) can be configured. This function authorizes the surveillance of the applications, connected to the ports 1 to 8 (PoE).

Once the function is active, it remains on standby waiting for the connected application to start and to answer to the regularly sent inquiries. As soon as the application has started, it answers to the inquiries and thus activates the DAM supervision and protection of the application. In case the application does no longer answer, the DAM launches an automatic restart for the corresponding PoE port.

- **Port**
  This column contains the port identifier. It can be customized as required by entering a name of up to 11 characters in the right-hand box. If an IP address has been entered in the "IP Address" column, then the text "Port X" is a hypertext link to this same IP address.

- **IP Address**
  This field is used to enter an IP address. If this IP address is different from "0.0.0.0", it changes the "Port X" identifier to a hypertext link to this same IP address.
  For the DAM function being operable, the connected application's IP address has to be entered in the field "IP Address".
- **DAM**
  This field allows to control the DAM function. The administrator can activate ("On") or disable ("Off") this function. It is disabled by default.

To save changes made to a port, click on "OK" to the right of the same row.

6.3 IP Parameters

The product's IP parameters consist of its IP address, network mask and gateway IP address. These parameters can be automatically assigned by DHCP, or entered manually. DHCP is enabled by default. It is only possible to function in DHCP if a DHCP server is available on the network.

The following paragraph explains how to configure the product's IP parameters:

- **Automatic IP parameter assignment**
  For an automatic assignment, the DHCP must be enabled (box to the right of DHCP checked). Click on "OK" next to "Gateway IP Address". The DHCP server allocates a new IP address to the product. It is necessary to explore the network to know the new address.

- **Manually entering IP parameters**
  To enter the IP parameters manually, DHCP must be disabled (box to the right of DHCP unchecked). Enter the new parameters into the three fields below (product IP address, network mask and gateway IP address). If the gateway feature is to be disabled, enter the gateway IP address of "0.0.0.0". Click on "OK" next to "Gateway IP Address" to save the configuration. The user is automatically re-routed to the new address (login page).

6.4 Network Administration

6.4.1 NTP

NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. The NTP servers can be specified and the GMT time zone set. The NTP configuration screen will appear after clicking "Network">"NTP".

NTP Configuration

- **Mode**
  This field indicates the NTP mode operation. By clicking on the drop-down menu next to "Mode", it can be selected if the NTP is "Enabled" or "Disabled":
  - Enabled: Enables NTP client mode operation. When enabling NTP mode operation, the agent forwards and transfers SNTP messages between the clients and the server when they are not on the same subnet domain.
  - Disabled: Disables NTP client mode operation.

- **Server #**
  In the space next to "Server #" the IP address for a NTP Server can be entered. The product receives the NTP information from that server.
  Note: The IPv4 or IPv6 address of a NTP server can be entered here. The IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

After the configuration is set, click "Save" to save and update the setting. To undo any changes made locally and revert to previously saved values, click "Reset".

6.4.2 Timezone

The Timezone is related to the NTP (see chapter 5.2). Via this page the GMT (Greenwich Mean Time) Timezone Offset can be set.

System Information Configuration

- **System Timezone Offset**
  In the space can be entered the time (in minutes), that the system differs from the GMT.

After the configuration is set, click "Save" to save and update the setting. To undo any changes made locally and revert to previously saved values, click "Reset".

6.4.3 SNMP & BACnet

BACnet

The BACnet IP protocol can operate in one of the following modes:

- **Read/Write**
  The data can be viewed and modified via the BACnet IP protocol. Actions can be implemented.
- **Read Only**
  The data can only be viewed via the BACnet IP protocol.
- **Disabled**
  The BACnet IP protocol is disabled.

Click on "OK" next to "BACnet" to save the configuration.

SNMP

The SMNP (Simple Network Management Protocol) is an application layer protocol that facilitates the exchange of management information between network devices. SNMP enables network administrators to manage the network performance, find and solve network problems and plan for network growth.

This switch supports the versions SNMP v1, v2c and v3. Different versions of SNMP provide different security levels for management stations and network devices.

The SNMP protocol can operate in one of the following modes:

- **Read/Write**
  The data can be viewed and modified via the SNMP protocol. Actions can be implemented.
- **Read Only**
  The data can only be viewed via the SNMP protocol.

Version SNMP v1 and v2c: Click on "OK" next to "SNMP" to save the configuration.

Version SNMP V3:

- **User USM**
  Create a login.
- **Auth Algorithm**
  Choose the algorithm to hash the password corresponding to the login.
- **Auth Password**
  Enter a password of between 8 and 16 characters.
- **Privacy Algorithm**
  Choose the encryption algorithm.
- **Privacy Password**
  Enter an encryption code of between 8 and 16 characters.

By clicking on "OK" next to "Privacy Password ", the configuration is saved.

SNMP Server IP Address

Traps are used by the agent to asynchronously inform the Network Management System (NMS) of some event. These events may be very serious, such as a fault, or just general information, such as port status change. In these cases, the switch creates the trap information and sends it then to the receiver or the network administrator.

If the user wishes to receive SNMP traps, he/she must configure the IP address of the SNMP servers receiving them. To save the changes, click on "OK" to the right of the same row.

If the function is to be disabled, enter the IP address of "0.0.0.0".

Two SNMP servers can be entered.

MIB Download

The SNMP MIB (Management Information Base) can be downloaded here. In case the download doesn't start, verify that it isn't blocked by the internet browser.

A MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules. This switch uses a standard MIB-2 information management module and a specific MIB SLAT-SDC. So, the MIB object value can be read by any SNMP web-managed software.

5.4.4 Syslog

The product is able to send events via UDP / 514 to one or two Syslog servers (RFC 5424 and RFC 5426). Enter the level of severity of the events to be sent and the IP address(es) of the servers.

LEVEL		DESCRIPTION	EVENT SEVERITY			
			ALL	< 5	< 4	DESABLED
0	Emergency	System is unusable	✓	✓	✓	
1	Alert	Action must be taken immediately if necessary	✓	✓	✓	
2	Critical	Critical conditions for the system	✓	✓	✓	
3	Error	Operating error	✓	✓	✓	
4	Warning	Warning (an error can occur if no action is taken)	✓	✓		
5	Notice	Normal but significant conditions	✓			
6	Informational	Informational messages	✓			

The category code used for the priority of SysLog messages is 1.

List of events

TYPE OF EVENTS	LEVEL OF SEVRITY	COMMENT
End of backup	0	Backup at the end of autonomy. Imminent stop.
Short circuit	2	Short circuit output.
Charger fault	2	Charger malfunction: the product needs to be changed.
Converter Fault	2	Converter malfunction: the product must be changed.
Battery Fault	2	Battery malfunction: the product must be changed.
P * - PoE Fault	3	PoE fault on port P * (overload, short circuit).
Backup Mode	4	The product operates in Backup out of Green mode.
Overload	4	Output consumption> 100% of the nominal value (current limitation to limit the output power).
Mains Fault	4	No mains
Temperature Fault	4	Internal temperature too high.
High Consumption	5	Output consumption> 95% of the nominal value.
Regular Mode	6	Normal operation on mains.
Green Mode	6	Mains present, the product is in Erase Mode or Energy Saving Mode (ECO)
Consumption OK	6	Normal output consumption.
Stealth Request	6	Receiving an external setpoint to operate in Stealth request
Stop Stealth Request	6	Stop Stealth request.
Mains OK	6	The mains is present.
Temperature OK	6	Internal temperature OK.
Charger OK	6	Proper operation of the charger.
Converter OK	6	Correct operation of the output converter.
Battery OK	6	Battery OK.
P * - PoE Halted	6	PoE port P * is actually stopped.
P * - PoE Active	6	PoE is active: energy is supplied on port P *.
P * - PoE Standby	6	PoE port P * is ready to provide power.
P * - PoE On	6	P* port PoE operation command.
P * - PoE Restart	6	P* port PoE restart command (stop for 8 seconds).

P* ➔ Port 1 and 8

Table 5.1: Events related to the power converter

TYPE OF EVENTS	LEVEL OF SEVRITY	COMMENT
Link fault	**4**	Event enabled when disconnecting a port or losing an Ethernet link. The event is active until it is acknowledged.
Acknowledgment defect link	**6**	Acknowledgment of the event «Default link».
P* - No link	**6**	Port Ethernet link state P *
P* - 10 Mbps	**6**	
P* - 100 Mbps	**6**	

P* ➔ Port 1 and 8

Table 5.2: Events related to the network board

TYPE OF EVENTS	LEVEL OF SEVRITY	COMMENT
Reset configuration	**5**	Reset the factory configuration.
Configuration changed	**6**	Event generated 2 minutes after the last configuration change of the product.

Table 5.3: Events related to the configuration

TYPE OF EVENTS	LEVEL OF SEVRITY	COMMENT
Temp. Sensor Fault	**0**	The temperature sensor is in failure
Internal Swt Com Fault	**0**	The switch communication is in failure
Internal Pwr Com Fault	**0**	The power supply communication is in failure
Internal Bat Com Fault	**0**	The battery communication is in failure
Start system	**5**	Generated when starting or rebooting the system.
Temp. Sensor OK	**6**	The temperature sensor is OK
Internal Swt Com Ok	**6**	The switch communication is OK
Internal Pwr Com Ok	**6**	The power supply communication is OK
Internal Bat Com Ok	**6**	The battery communication is OK

Table 5.4: Events related to the system

7. Configuration

7.1 Settings Configuration

This page allows to perform the configuration of the basic settings. Confirm the operations by clicking on the button next to them ("OK").

- **Change password**
  The password can be changed by entering the current password as well as twice the new password.
- **Enter the system name**
  The system name with up to 16 characters can be entered. Over HTTPS, the name always possesses the prefix "SDC-". The name is displayed in the headline of the web interface (see chapter 2.4.1).
  This information is also available over SNMP and BACnet IP, but without the prefix.
- **Enter the product location**
  The location here defined is shown on the "System state > System Information" page (see chapter 3.1).
  This information is also available over SNMP and BACnet IP.

7.2 Advanced Configuration

7.2.1 MAC Address Table

The MAC Address Table is configured on this page.

Aging Configuration

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

- **Disable Automatic Aging**
  By checking the box, the automatic aging of dynamic entries can be disabled.
- **Aging Time**
  The aging time is the time after which a learned entry is discarded. To configure the aging time, a value in the range from 10 to 1000000 seconds has to be entered. The default value is 300.

MAC Table Learning

Each port can do learning based upon the following settings. This switch supports three types for MAC Table Learning. If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.

- **Auto**
  The learning is done automatically as soon as a frame with an unknown SMAC is received.
- **Disable**
  The port will NOT learn the MAC address.
- **Secure**
  Only the static MAC entries are learned. The port will only forward the data of the configured static MAC address, all other frames are dropped.

IMPORTANT REMARK!

It must be made sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain up to 64 entries. The MAC table is sorted first by VLAN ID and then by MAC address.

- **Add New Static Entry**
  Click the button to add a new entry to the static MAC table. Specify the VLAN ID, MAC address and port members for the new entry and click "Save" on the bottom of the page.
- **Delete**
  Check the box to delete the entry. It will be deleted during the next save.
- **VLAN ID**
  Add the VLAN ID of the entry.
- **MAC Address**
  Add the MAC address of the entry.
- **Port Members**
  Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

After the configuration is set, click "Save" to save and update the setting. To undo any changes made locally and revert to previously saved values, click "Reset".

7.2.2 VLANs

The VLAN (Virtual Local Area Network - 802.1Q) logically divides one LAN (Local Area Network) into a plurality of subsets. Each subset will form their own broadcast area network. This means, VLAN is a communication technology that logically divides one physical LAN into multiple broadcast area networks (multiple VLAN). The hosts within one VLAN can communicate directly, but VLAN groups can not directly communicate with each other. This will limit the broadcast packets within one VLAN, since it can not directly access between VLAN groups. Thus, the network security improves.

The VLAN Configuration page allows for controlling the VLAN configuration on the switch. The page is divided into a global section and a per-port configuration section.

Global VLAN Configuration

- **Allowed Access VLANs**
  This field shows the allowed Access VLANs, i.e. it only affects ports configured as Access ports (see below). Ports in other modes are members of all VLANs specified in the Allowed VLANs field (Port VLAN Configuration on the same site, see below). By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound.
  The following example will create the VLANs 1, 10, 11, 12, 13, 200, and 300 (spaces are allowed in between the delimiters): "**1, 10-13, 200, 300**"
- **Ethertype for Custom S-ports**
  This field specifies the Ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose port type (set in Port VLAN Configuration on the same page) is set to a S-Custom-port.

Port VLAN Configuration

- **Port**
  This is the logical port number of this row.

- **Mode**
  The port mode determines the fundamental behavior of the port in question. A port can be in one of three modes as described below. By default, the active mode is Access.
  Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question.
  Grayed out fields show the value that the port will get when the mode is applied.

  Access
  Access ports are normally used to connect to end stations. They have the following characteristics:
  - Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1.
  - Accepts untagged and C-tagged frames.
  - Discards all frames that are not classified to the Access VLAN.
  - On egress, all frames classified to the Access VLAN are transmitted untagged. Others are transmitted tagged.

  Trunk
  Trunk ports can carry traffic on multiple VLANs simultaneously and are normally used to connect to other switches. They have the following characteristics:
  - By default, a trunk port is a member of all VLANs (1-4095).
  - The VLANs, that a trunk port is member of, may be limited by the use of Allowed VLANs (see column on the right and its description below).
  - Frames classified to a VLAN, that the port is not a member of, are discarded.
  - By default, frames classified to the Port VLAN (a.k.a. Native VLAN) do not get C-tagged on egress. All the other frames get tagged on egress.
  - Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress.

  Hybrid
  Hybrid ports resemble trunk ports in many ways, but add additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:
  - The ports can be configured to be VLAN tag unaware, C-tag aware, S-tag aware or S-custom-tag aware.
  - Ingress filtering can be controlled.
  - Ingress acceptance of frames and configuration of egress tagging can be configured independently.

- **Port VLAN**
  This field determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4094, with default being 1.
  On ingress, frames get classified to the Port VLAN, if the port is configured as VLAN unaware, the frame is untagged or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0).
  On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN.
  The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.
  To be able to communicate with the product, the port to which the supervisor is connected to, has to be part of the **VLAN 1**.

- **Port Type**
  Ports in hybrid mode allow to change the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.

  Unaware
  On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN and possible tags are not removed on egress.

  C-Port
  On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag.

  S-Port
  On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.

  S-Custom-Port
  On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.

- **Ingress Filtering**
  Hybrid ports allow for changing the ingress filtering. Access and Trunk ports always have ingress filtering enabled.
  If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN, that the port is not a member of, get discarded.
  If ingress filtering is disabled (checkbox is unchecked), frames classified to a VLAN, that the port is not a member of, are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.

- **Ingress Acceptance**
  Hybrid ports allow for changing the type of frames that are accepted on ingress.

  Tagged and Untagged
  Both tagged and untagged frames are accepted.

  Tagged Only
  Only tagged frames are accepted on ingress. Untagged frames are discarded.

  Untagged Only
  Only untagged frames are accepted on ingress. Tagged frames are discarded.

- **Egress Tagging**
  Ports in Trunk and Hybrid mode may control the tagging of frames on egress.

  Untag Port VLAN
  Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.

  Tag All
  All frames, whether classified to the Port VLAN or not, are transmitted with a tag.

  Untag All
  All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.

- **Allowed VLANs**
  Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be members of one VLAN, the Access VLAN.
  The field's syntax is identical to the syntax used in the Allowed Access VLANs field (see above). By default, a Trunk or Hybrid port will become member of all VLANs and is therefore set to 1-4094.
  The field may be left empty, which means that the port will not become member of any VLANs.

- **Forbidden VLANs**
  A port may be configured to never be a member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs.
  The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Allowed Access VLANs field.
  By default, this field is left blank, which means that the port may become a member of all possible VLANs.

After the configuration is set, click ?Save? to save and update the setting. To undo any changes made locally and revert to previously saved values, click ?Reset?.

7.2.3 Port Isolation

Port isolation is used to limit the data flow between ports. It is similar to VLAN, but stricter.

This page is used for enabling or disabling port isolation on ports in a Private VLAN. Also, a port member of a VLAN can be isolated to other isolated ports on the same VLAN and on a Private VLAN.

A port can be isolated to prevent it to forward the data flow. To define a port as isolated, check the box of the corresponding port.

Port Isolation Configuration

A check box is provided for each port of a private VLAN.

- When checked, port isolation is enabled on that port.
- When unchecked, port isolation is disabled on that port.
- By default, port isolation is disabled on all ports.

After the configuration is set, click ?Save? to save and update the setting. To undo any changes made locally and revert to previously saved values, click ?Reset?.

7.2.4 Loop Protection

The Loop protection is used to avoid broadcast loops.

General Settings Configuration ? Global Configuration

- **Enable Loop Protection**
  This controls whether the loop protection is enabled (as a whole). Click on the drop-down menu to disable or enable the Loop Protection.

- **Transmission Time**
  The transmission time is the interval between each loop protection PDU sent on each port. Valid values are from 1 to 10 seconds. Enter a number to set the Loop Protection Interval Time.

- **Shutdown Time**
  The shutdown time is the period (in seconds) for which a port will be kept disabled in the event that a loop is detected (and the port action (defined below) shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart). Enter a number to set the port Shutdown Time.

Port Configuration

- **Port**
  The switch port number of the port.
- **Enable**
  Check the box to enable the loop protection on the corresponding port.
- **Action**
  When a loop is detected on the port, a predefined action is performed. There are 3 types of action for users to select
  - Shutdown port
  - Shutdown port and Log
  - Log Only
- **Tx Mode**
  The Tx Mode controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's. It can be enabled or disabled by clicking on the drop-down menu.

After the configuration is set, click "Save" to save and activate the setting. To undo any changes made locally and revert to previously saved values, click "Reset".

7.2.5 Spanning Tree

The Spanning Tree Protocol (STP) can be used to detect and disable network loops. It also serves to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices in the network to ensure that only one route exists between any two stations on the network as well as to provide backup links which automatically take over when a primary link goes down

7.2.5.1 Bridge Settings

The STP Bridge Configuration page allows the configuration of the STP system settings. The settings are used by all STP Bridge instances in the switch. To define the STP settings the following parameters have to be specified.

Basic Settings

- **Protocol Version**
  Click on the drop-down menu to select the protocol version:
  - STP - Spanning Tree Protocol (IEEE802.1D)
  - RSTP - Rapid Spanning Tree Protocol (IEEE802.1w)
- **Bridge Priority**
  This field controls the bridge priority. It can be selected using the drop-down menu. Lower numeric values have a higher priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch, form a *Bridge Identifier*.
- **Forward Delay**
  The Forward Delay is the delay used by STP Bridges to transit Root and Designated Ports to forward information (used in STP compatible mode). The setting range is from 4 to 30 seconds. The default value is 15 seconds.
- **Max Age**
  This value indicates the maximum age of the information transmitted by the bridge when it is the Root Bridge. Valid values are in the range from 6 to 40 seconds *and* the MaxAge must be <= (ForwardDelay-1)*2. The default value is 20 seconds.

- **Maximum Hop Count**
  This count defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines to how many bridges a root bridge can distribute its BPDU information. Valid values are in the range from 6 to 40 hops. The default value is 20 hops.
- **Transmit Hold Count**
  The value indicates the number of BPDUs a bridge port can send per second. When the number is exceeded, the transmission of the next BPDU will be delayed. Valid values are in the range from 1 to 10 BPDUs per second. The default value is 6 BPDUs.

Advanced Settings

- **Edge Port BPDU Filtering**
  With this setting, the user controls whether a port, explicitly configured as Edge, will transmit and receive BPDUs.
- **Edge Port BPDU Guard**
  With this setting, the user controls whether a port, explicitly configured as Edge, will disable itself upon the reception of a BPDU. In this case the port will enter the error-disabled state and will be removed from the active topology.
- **Port Error Recovery**
  Using the Port Error Recovery, it can be controlled whether a port in the error-disabled state automatically will be enabled after a certain time. (This ⍰timeout⍰ can be defined in the field below.) If recovery is not enabled, ports have to be disabled and re-enabled for a normal STP operation. The condition is also cleared by a system reboot.
- **Port Error Recovery Timeout**
  It indicates the time that has to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours). This is only used when the Port Error Recovery is enabled.

After the configuration is set, click ⍰Save⍰ to save and activate the setting. To undo any changes made locally and revert to previously saved values, click ⍰Reset⍰.

7.2.5.2 Bridge Ports

This page allows the user to inspect the current STP CIST port configurations and possibly change them as well. It contains settings for physical and aggregated ports.

CIST Aggregated Port Configuration & CIST Normal Port Configuration

- **Port**
  The switch port number of the logical STP port.
- **STP Enabled**
  The STP function can be enabled by checking the box.

- **Path Cost**
  With this field the path cost incurred by the port can be controlled.
  - ⍰Auto⍰
    The Auto setting will set the path cost as appropriate by the physical link speed, using the IEEE 802.1D recommended values. The value is set to 0.
  - ⍰Specific⍰
    Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range from 1 to 200000000.

- **Priority**
  This category controls the port priority. This can be used to control the priority of ports having identical port costs. (See above)

- **Admin Edge**
  With this field the edge state on the bridge port can be defined.
  - ⍰Edge⍰
    Edge ports are ports of a bridge that do not transmit BPDU packets.
  - ⍰Non-Edge⍰
    Non-Edge ports are ports of a bridge that transmit BPDU packets.

- **Auto Edge**
  Controls whether the bridge should enable automatic edge detection on the bridge port. To set the corresponding port in Auto Edge check the box.

- **Restricted Role**
  If the port is a Restricted Role, it defines the port as a root port. To set the corresponding port as Restricted Role check the box.

- **Restricted TCN**
  If the port is a Restricted TCN, it is defined as a port that sends the changes of the STP state. To set the corresponding port as Restricted TCN check the box.

- **BPDU Guard**
  To enable the BPDU Guard check the box. So, when a port receives a BPDU reception, it will be disabled (Shut Down).

- **Point-to-point**
  This function controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined or forced either true or false. The transition to the forwarding state is faster for point-to-point LANs than for shared media. (This applies to physical ports only. Aggregations are always forced Point2Point.)

After the configuration is set, click ⍰Save⍰ to save and activate the setting. To undo any changes made locally and revert to previously saved values, click ⍰Reset⍰.

7.2.6 IGMP Snooping

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

7.2.6.1 Basic IGMP Snooping Configuration

On this page the IGMP Snooping Configuration can be performed.

Global Configuration

- **Snooping Enabled**
  The Global IGMP Snooping can be enabled by checking or disabled by unchecking the box. The default value is "Disabled".
- **Unregistered IPMCv4 Flooding Enabled**
  The unregistered IPMCv4 Flooding can be enabled by checking the box.
  The flooding control takes effect only when IGMP Snooping is enabled. When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.

Port Related Configuration

- **Port**
  The switch port number of the port.
- **Router Port**
  By checking the box, it can be specified which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or the IGMP querier.
  If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
- **Fast Leave**
  By checking the box, the Fast Leave can be enabled.
  The Fast Leave performs the deleting of the MAC forward entry, immediately upon receiving the message for the group de-registration.

After the configuration is set, click "Save" to save and activate the setting. To undo any changes made locally and revert to previously saved values, click "Reset".

7.2.6.2 IGMP Snooping VLAN Configuration

Navigating the IGMP Snooping VLAN Table

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input field allows the user to select the starting point in the VLAN Table. Clicking the "Refresh" button will update the displayed table starting from that or the next closest VLAN Table match.

The >> button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

Click the "Add a new IGMP VLAN" button to add a new IGMP VLAN to the list. The VLAN ID has to be specified and the details of the new entry configured. Click "Save" to safe the new entry. The specific IGMP VLAN starts working after the corresponding static VLAN is also created (chapter 6.2.2).

IGMP Snooping VLAN Table Columns

- **Delete**
  Click to delete the IGMP VLAN in the corresponding line. The designated entry will be deleted during the next save.

- **VLAN ID**
  The VLAN ID of the entry.
- **Snooping Enabled**
  The per-VLAN IGMP snooping can be enabled by checking or disabled by unchecking the box. Up to 32 VLANs can be selected for IGMP Snooping.
- **Querier Election**
  To join the IGMP Querier election in the VLAN, enable the Querier Election by checking the box. When disabled, the VLAN acts as an IGMP Non-Querier.
- **Querier Address**
  Define the IPv4 address as source address used in the IP header for the IGMP Querier election. When the Querier address is not set, the system uses the IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, the system uses the first available IPv4 management address. Otherwise, the system uses a pre-defined value. By default, this value will be 192.0.2.1.

After the configuration is set, click "Save" to save and activate the setting. To undo any changes made locally and revert to previously saved values, click "Reset".

7.2.7 LLDP

The Link Layer Discovery Protocol (LLDP) is used to discover the basic information about the neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. The advertised information is represented in the Type Length Value (TLV) format according to the IEEE 802.1ab standard and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

LLDP Parameters

The following characteristics allow the user to inspect and configure the current LLDP port settings:

- **Tx Interval (Transmission Interval Time)**
  The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the "Tx Interval" value. Valid values are restricted to 5 - 32768 seconds.
- **Tx Hold (Hold time Multiplier)**
  Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to "Tx Hold" multiplied by "Tx Interval" seconds. Valid values are restricted to 2 - 10 times.
- **Tx Delay (Transmit Delay Time)**
  If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted. But the time between the LLDP frames will always be at least the value of "Tx Delay" seconds. Tx Delay cannot be larger than 1/4 of the "Tx Interval" value. Valid values are restricted to 1 - 8192 seconds.
- **Tx Reinit (Transmit Remit Time)**
  When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the number of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

LLDP Port Configuration

- **Port**
  The switch port number of the logical LLDP port.
- **Mode**
  The LLDP messages transmit and receive modes for LLDP Protocol Data Units can be selected here. The options available are:
  - Rx only
    The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.
  - Tx only
    The switch will drop LLDP information received from neighbors but will send out LLDP information.
  - Enabled
    The switch will send out LLDP information and will analyze LLDP information received from neighbors.
  - Disabled
    The switch will not send out LLDP information and will drop LLDP information received from neighbors.
- **Optional TLVs**
  These fields are used to configure the information included in the TLV field of advertised messages. When one of the following options is checked, the corresponding information will be included in the transmitted LLDP information.
  - Port Descr
    When the box is checked, the "port description" is included in the transmitted LLDP information.
  - Sys Name
    When the box is checked, the "system name" is included in the transmitted LLDP information.
  - Sys Descr
    When the box is checked, the "system description" is included in the transmitted LLDP information.
  - Sys Capa
    When the box is checked, the "system capability" is included in the transmitted LLDP information.
  - Mgmt Addr
    When the box is checked, the "management address" is included in the transmitted LLDP information.

After the configuration is set, click "Save" to save and activate the setting. To undo any changes made locally and revert to previously saved values, click "Reset".

7.3 Security Configuration

7.3.1 Port Security Limit

The Port Security Limit Control Configuration page allows to configure the Port Security Limit Control system and port settings.

The Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If the Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four different actions as described below.

The Limit Control module utilizes a lower-layer module, the Port Security module, which manages the MAC addresses learnt on the port.

The Limit Control configuration consists of two sections, a system- and a port-wide.

System Configuration

- **Mode**
  Indicates if Limit Control is globally "Enabled" or "Disabled" on the switch. If it is globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

- **Aging Enabled**
  If checked, secured MAC addresses are subject to aging as discussed under "Aging Period".

- **Aging Period**
  If "Aging Enabled" is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shortest requested aging period of all modules that use the functionality.
  The Aging Period can be set to a number between 10 and 10,000,000 seconds.
  To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected and the corresponding resources are freed on the switch.

Port Configuration

The table has one row for each port on the selected switch and a number of columns, which are:

- **Port**
  The port number to which the configuration below applies.

- **Mode**
  Controls whether Limit Control is enabled or disabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.

- **Limit**
  The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.
  The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

- **Action**
  If the "Limit" is reached, the switch can take one of the following actions:
  - "None"
    Do not allow more than "Limit" MAC addresses on the port, but take no further action.
  - "Trap"
    If "Limit" + 1 MAC addresses are seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded.

- "Shutdown"
  If "Limit" + 1 MAC addresses are seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:
  1) Boot the switch,
  2) Disable and re-enable Limit Control on the port or the switch,
  3) Click the "Reopen" button.
- "Trap & Shutdown"
  If "Limit" + 1 MAC addresses are seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

- **State**
  This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values:
  - "Disabled": Limit Control is either globally disabled or disabled on the port.
  - "Ready": The limit is not yet reached. This can be shown for all actions.
  - "Limit Reached": Indicates that the limit is reached on this port. This state can only be shown if "Action" is set to "None" or "Trap".
  - "Shutdown": Indicates that the port is shut down by the Limit Control module. This state can only be shown if "Action" is set to "Shutdown" or "Trap & Shutdown".

- **Re-open Button**
  If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to "Shutdown" in the "Action" section.
  Note that clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost.

After the configuration is set, click "Save" to save the changes and activate the setting. To undo any changes made locally and revert to previously saved values, click "Reset".

To refresh the page, click on the "Refresh" button. Note that unsaved changes will be lost.

802.1X – Network Access Server

The Network Access Server (NAS) configuration page allows the user to configure the IEEE 802.1X and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "Configuration → Security Configuration → AAA-RADIUS" page. Until the client is authenticated, 802.1X access control allows only EAPOL traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

MAC-based authentication allows for authentication of more than one user on the same port and doesn't require the user to have special 802.1X supplicant software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.

The NAS configuration consists of two sections, a system- and a port-wide.

System Configuration

- **Mode**
  The Network Access Server can be globally enabled or disabled by using the drop-down menu. If it is globally disabled, all ports are allowed to forward frames.

- **Reauthentication Enabled**
  The reauthentication is enabled by checking the box. If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached. For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client and therefore doesn't imply that a client is still present on a port (see Aging Period below).

- **Reauthentication Period**
  The Reauthentication period determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range from 1 to 3600 seconds.

- **EAPOL Timeout**
  The EAPOL Timeout determines the time for retransmission of Request Identity EAPOL frames.
  Valid values are in the range from 1 to 65535 seconds. This has no effect for MAC-based ports.

- **Aging Period**
  This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:
    - Port-based 802.1X
    - MAC-Based Auth.

  When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.
  If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.
  For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

- **Hold Time**
  This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:
    - Port-based 802.1X
    - MAC-Based Auth.

  If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server requests time out (according to the timeout specified on the AAA RADIUS page; see chapter 6.3.7) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication.
  In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.
  The Hold Time can be set to a number between 10 and 1000000 seconds.

Port Configuration

The table has one row for each port on the selected switch.

- **Port**
  The port number for which the configuration below applies.
- **Admin State**
  If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:
  - Force Authorized
    In this mode, the switch will send one EAPOL Success frame when the port link comes up and any client on the port will be allowed network access without authentication.
  - Force Unauthorized
    In this mode, the switch will send one EAPOL Failure frame when the port link comes up and any client on the port will be disallowed network access.
  - 802.1X (port based)
    This switch supports IEEE 802.1X port-based authentication. In the 802.1X-world, the user is called the supplicant, the switch is the authenticator and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP (Extensible Authentication Protocol) over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets.
    RADIUS packets also encapsulate EAP PDUs, together with other attributes like the switch's IP address, its name and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

    When the authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block the traffic on the switch port connected to the supplicant.
    Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page) and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.
  - Mac-based Auth.
    Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of "MAC-based authentication" over "port-based 802.1X authentication" is, that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication and that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

- **Port State**

  The Port State indicates the current state of the port. It can undertake one of the following values:

  - Globally Disabled
    NAS is globally disabled.
  - Link Down
    NAS is globally enabled, but there is no link on the port.
  - Authorized
    The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.
  - Unauthorized
    The port is in Force Unauthorized or in a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.
  - X Auth/Y Unauth
    The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

  The port state is connected to the enabling of the Network Access Server System Mode. If in the system configuration (see above) the mode is disabled, all the port states are "Globally Disabled".

- **Restart**

  Two buttons are available for each row " "Reauthenticate" and "Reinitialize". The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based (802.1X) or MAC-based mode.

  Clicking these buttons will not cause settings changed on the page to take effect.

  - Reauthenticate
    It schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately.
    The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.
  - Reinitialize
    It forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

After the configuration is set, click "Save" to save and activate the setting. To undo any changes made locally and revert to previously saved values, click "Reset".

To refresh the page, click on the "Refresh" button. Note that unsaved changes will be lost.

7.3.3 ACL

ACL is an acronym for Access Control List. It is a table made up of the ACEs (Access Control Entry) defined on this switch. They contain access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for various situations. In networking, the ACL refers to a list of service ports or network services that are available on a host or a server. Each one of them has a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic and, in this context, they are similar to firewalls.

7.3.3.1 ACL Ports Configuration

Via this page the ACL parameters (ACE) of each switch port can be configured. These parameters will affect frames received on a port unless the frame matches a specific ACE.

- **Port**
  The logical port for the settings contained in the same row.
- **Policy ID**
  Select the policy to apply to this port. The allowed values are 0 through 255. The default value is 0.
- **Action**
  Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".
- **Rate Limiter ID**
  Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is "Disabled". (For more details go to section 6.3.3.2. ACL Rate Limiter Configuration.)
- **Port Redirect**
  Select which port frames are redirected on. The allowed values are Disabled or a specific port number. A port number can't be set when action is permitted. The default value is "Disabled".
- **Mirror**
  Specify the mirror operation of this port. The allowed values are:
  - Enabled: Frames received on the port are mirrored.
  - Disabled: Frames received on the port are not mirrored.

  The default value is "Disabled".
- **Logging**
  Specify the logging operation of this port. Notice that the logging message doesn't include the 4 bytes CRC. The allowed values are:
  - Enabled: Frames received on the port are stored in the System Log.
  - Disabled: Frames received on the port are not logged.

  The default value is "Disabled".
  Note: The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.
- **Shutdown**
  Specify the port shut down operation of this port. The allowed values are:
  - Enabled: If a frame is received on the port, the port will be disabled.
  - Disabled: Port shut down is disabled.

  The default value is "Disabled".
  Note: The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).

- **State**
  Specify the state of this port. The allowed values are:
  - "Enabled": To reopen ports by changing the volatile port configuration of the ACL user module.
  - "Disabled": To close ports by changing the volatile port configuration of the ACL user module.

  The default value is "Enabled".
- **Counter**
  Counts the number of frames that match this ACE.

After the configuration is set, click "Save" to save and activate the setting. To undo any changes made locally and revert to previously saved values, click "Reset".

To refresh the page, click on the "Refresh" button. Note that unsaved changes will be lost.

By clicking the "Clear" button, the counters for all ports are cleared.

7.3.3.2 ACL Rate Limiter Configuration

On this page the ACL Rate Limiters can be configured.

- **Rate Limiter ID**
  The rate limiter ID is the identifier for the settings contained in the same row.
- **Rate**
  The rate range is located between 0 and 128k in pps.
  The valid rate is 0 - 99, 100, ..., 3276700 in pps or 0, 100, 2*100, 3*100, ..., 1000000 in kbps.
- **Unit**
  By using the drop-down menu, the rate unit has to be specified. The allowed values are:
  - "pps": packets per second
  - "kbps": kbits per second

After the configuration is set, click "Save" to save and activate the setting. To undo any changes made locally and revert to previously saved values, click "Reset".

7.3.3.3 Access Control List Configuration

This page shows the Access Control List (ACL), which is made up of the Access Control Entries (ACE) defined on this switch. Each row describes one defined ACE. The maximum number of ACEs on this switch is 128.

Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted. The order sequence cannot be changed and the priority is set beginning with the highest.

- **ACE**
  Indicates the ACE ID.
- **Ingress Port**
  Indicates the ingress port of the ACE. Possible values are:
  - "All": The ACE will match all ingress ports.
  - Port "X": The ACE will match a specific ingress port X, with X being the number of the switch port.
- **Policy / Bitmask**
  Indicates the policy number and bitmask of the ACE.

- **Frame Type**
  Indicates the frame type of the ACE. Possible values are:
  - ?Any?: The ACE will match any frame type.
  - ?EType?: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.
  - ?ARP?: The ACE will match ARP/RARP frames.
  - ?IPv4?: The ACE will match all IPv4 frames.
  - ?IPv4/ICMP?: The ACE will match IPv4 frames with ICMP protocol.
  - ?IPv4/UDP?: The ACE will match IPv4 frames with UDP protocol.
  - ?IPv4/TCP?: The ACE will match IPv4 frames with TCP protocol.
  - ?IPv4/Other?: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.
  - ?IPv6?: The ACE will match all IPv6 standard frames.
  - ?IPv6 - NH:ICMPv6?: The ACE will match IPv6 frames with ICMP protocol.
  - ?IPv6 - NH:UDP?: The ACE will match IPv6 frames with UDP protocol.
  - ?IPv6 - NH:TCP?: The ACE will match IPv6 frames with TCP protocol.
  - ?IPv6- NH:*Value Other*?: The ACE will match IPv6 frames, which are not ICMP/UDP/TCP.
- **Action**
  Indicates the forwarding action of the ACE.
  - ?Permit?: Frames matching the ACE may be forwarded and learned.
  - ?Deny?: Frames matching the ACE are dropped.
  - ?Filter?: Frames matching the ACE are filtered.
- **Rate Limiter**
  Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.
- **Port Redirect**
  Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.
- **Mirror**
  Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:
  - ?Enabled?: Frames received on the port are mirrored.
  - ?Disabled?: Frames received on the port are not mirrored.

  The default value is "Disabled".
- **Counter**
  The counter indicates the number of times the ACE was hit by a frame.
- **Modification Buttons**
  You can modify each ACE (Access Control Entry) in the table using the following buttons:

   Insert a new ACE before this current ACE row.

   Edit this ACE row.

   Move this ACE up the list.

   Move this ACE down the list.

   Delete this ACE.

   The lowest plus sign adds a new entry at the bottom of the ACE listings

Check the ?Auto-refresh? box to refresh the page automatically. The automatic refresh occurs every 3 seconds.
To refresh the page manually click on the ?Refresh? button.
By clicking the ?Clear? button, the counters for all ports are cleared.
The ?Remove All? button removes all the ACEs on the Access Control List.

A. ACE Configuration

An ACE (Access Control Entry) consists of several parameters. These parameters vary according to the frame type. First the ingress port for the ACE and then the frame type has to be selected. Different parameter options are displayed depending on the selected frame type.

A frame that matches this ACE configuration is defined as follows.

- **Ingress Port**
  Select the ingress port for which this ACE applies
  - 'All': The ACE applies to all port.
  - 'Port X': The ACE applies to this port number, with X being the number of the switch port.
- **Policy Filter**
  Specify the policy number filter for this ACE.
  - 'Any:' No policy filter is specified (policy filter status is "don't-care").
  - 'Specific': If you want to filter a specific policy with this ACE, choose this option. Two field for entering a 'policy value' and 'bitmask' appear.
- **Policy Value**
  When "Specific" is selected for the policy filter, a specific policy value can be entered. The allowed range is from 0 to 255.
- **Policy Bitmask**
  When "Specific" is selected for the policy filter, a specific policy bitmask can be entered. The allowed range is 0x0 to 0xFF. Notice in the usage of bitmasks, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [policy_value & policy_bitmask].
  For example, if the policy value is 3 and the policy bitmask is 0x10 (bit 0 is "don't-care" bit), then policy 2 and 3 are applied to this rule.
- **Frame Type**
  Select the frame type for this ACE. These frame types are mutually exclusive.
  - 'Any': Any frame can match this ACE.
  - 'Ethernet Type': Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0x0600 hexadecimal).
  - 'ARP': Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type.
  - 'IPv4': Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.
  - 'IPv6': Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.
- **Action**
  Specify the action to take with a frame that hits this ACE.
  - 'Permit': The frame that hits this ACE is granted permission for the ACE operation.
  - 'Deny': The frame that hits this ACE is dropped.
  - 'Filter': Frames matching the ACE are filtered.
- **Filter port**
  Specify the filter port of the ACE. The allowed values are 'All' or a specific port number. The filter port can only be set when the action is 'Filter'.
- **Rate Limiter**
  Specify the rate limiter in number of base units. The allowed range is 1 to 16. Disabled indicates that the rate limiter operation is disabled.

- **Port Redirect**
  Specify the port redirect of the ACE. Frames matching the ACE are redirected to the port number specified here. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled. A port redirect number can only be set when the action is "Deny".

- **Mirror**
  Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the mirror port. The allowed values are:
  - "Enabled": Frames received on the port are mirrored.
  - "Disabled": Frames received on the port are not mirrored.

  The default value is "Disabled".

- **Logging**
  Specify the logging operation of the ACE. Notice that the logging message doesn't include the 4 bytes CRC information. The allowed values are:
  - "Enabled": Frames matching the ACE are stored in the System Log.
  - "Disabled": Frames matching the ACE are not logged.

  Note: The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.

- **Shutdown**
  Specify the port shut down operation of the ACE. The allowed values are:
  - "Enabled": If a frame matches the ACE, the ingress port will be disabled.
  - "Disabled": Port shut down is disabled for the ACE.

  Note: The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).

- **Counter**
  The counter indicates the number of times the ACE was hit by a frame.

MAC Parameters

The MAC Parameters are only displayed when the frame type is Ethernet Type or ARP.

- **SMAC Filter**
  Specify the source MAC filter for this ACE. This field is only displayed when the frame type is Ethernet Type or ARP.
  - "Any": No SMAC filter is specified. (SMAC filter status is "don't-care".)
  - "Specific": If you want to filter a specific source MAC address with this ACE, choose this option. A field for entering a SMAC value appears.

- **SMAC Value**
  When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value.

- **DMAC Filter**
  Specify the destination MAC filter for this ACE.
  - "Any": No DMAC filter is specified (DMAC filter status is "don't-care").
  - "MC": Frame must be multicast.
  - "BC": Frame must be broadcast.
  - "UC": Frame must be unicast.
  - "Specific": If you want to filter a specific destination MAC address with this ACE, choose this option. A field for entering a DMAC value appears.

- **DMAC Value**
  When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.

VLAN Parameters

The VLAN Parameters can be defined for all sorts of Frame Types.

- **802.1Q Tagged**
  Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are:
  - 'Any': Any value is allowed ("don't-care"). The default value is "Any".
  - 'Enabled': Tagged frame only.
  - 'Disabled': Untagged frame only.
- **VLAN ID Filter**
  Specify the VLAN ID filter for this ACE.
  - 'Any': No VLAN ID filter is specified (VLAN ID filter status is "don't-care").
  - 'Specific': If you want to filter a specific VLAN ID with this ACE, choose this option. A field for entering a VLAN ID number appears.
- **VLAN ID**
  When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is from 1 to 4095. A frame that hits this ACE matches this VLAN ID value.
- **Tag Priority**
  Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is from 0 to 7 or range 0-1, 2-3, 4-5, 6-7, 0-3 and 4-7. The value 'Any' means that no tag priority is specified (tag priority is "don't-care").

Ethernet Type Parameters

The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected.

- **EtherType Filter**
  Specify the Ethernet type filter for this ACE.
  - 'Any': No EtherType filter is specified (EtherType filter status is "don't-care").
  - 'Specific': If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering an EtherType value appears.
- **Ethernet Type Value**
  When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is from 0x600 to 0xFFFF but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.

ARP Parameters

The ARP parameters can be configured when Frame Type "ARP" is selected.

- **ARP/RARP**
  Specify the available ARP/RARP opcode (OP) flag for this ACE.
  - 'Any': No ARP/RARP OP flag is specified (OP is "don't-care").
  - 'ARP': Frame must have ARP opcode set to ARP.
  - 'RARP': Frame must have RARP opcode set to RARP.
  - 'Other': Frame has unknown ARP/RARP Opcode flag.

- **Request/Reply**
  Specify the available Request/Reply opcode (OP) flag for this ACE.
  - ?Any?: No Request/Reply OP flag is specified (OP is "don't-care").
  - ?Request?: Frame must have ARP Request or RARP Request OP flag set.
  - ?Reply?: Frame must have ARP Reply or RARP Reply OP flag.

- **Sender IP Filter**
  Specify the sender IP filter for this ACE.
  - ?Any?: No sender IP filter is specified (Sender IP filter is "don't-care").
  - ?Host?: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears.
  - ?Network?: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.

- **Sender IP Address**
  When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation. Notice that the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly add a deny action.

- **Sender IP Mask**
  When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.

- **Target IP Filter**
  Specify the target IP filter for this specific ACE.
  - ?Any?: No target IP filter is specified (Target IP filter is "don't-care").
  - ?Host?: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears.
  - ?Network?: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.

- **Target IP Address**
  When "Host" or "Network" is selected for the Target IP Filter, you can enter a specific target IP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly add a deny action.

- **Target IP Mask**
  When "Network" is selected for the Target IP Filter, you can enter a specific target IP mask in dotted decimal notation.

- **ARP Sender MAC Match**
  Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.
  - ?0?: ARP frames where SHA is not equal to the SMAC address.
  - ?1?: ARP frames where SHA is equal to the SMAC address.
  - ?Any?: Any value is allowed ("don't-care").

- **RARP Target MAC Match**
  Specify whether frames can hit the action according to their target hardware address field (THA) settings.
  - ?0?: RARP frames where THA is not equal to the target MAC address.
  - ?1?: RARP frames where THA is equal to the target MAC address.
  - ?Any?: Any value is allowed ("don't-care").

- **IP/Ethernet Length**
  Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.
  - 0: ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the PLN is not equal to IPv4 (0x04).
  - 1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the PLN is equal to IPv4 (0x04).
  - Any: Any value is allowed ("don't-care").

- **IP**
  Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.
  - 0: ARP/RARP frames where the HRD is not equal to Ethernet (1).
  - 1: ARP/RARP frames where the HRD is equal to Ethernet (1).
  - Any: Any value is allowed ("don't-care").

- **Ethernet**
  Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.
  - 0: ARP/RARP frames where the PRO is not equal to IP (0x800).
  - 1: ARP/RARP frames where the PRO is equal to IP (0x800).
  - Any: Any value is allowed ("don't-care").

IP Parameters

The IP parameters can be configured when Frame Type "IPv4" is selected.

- **IP Protocol Filter**
  Specify the IP protocol filter for this ACE.
  - Any: No IP protocol filter is specified ("don't-care").
  - ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained below (ICMP Parameters).
  - UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained blow (UDP Parameters).
  - TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained below (TCP Parameters).
  - Other: If you want to filter another, specific IP protocol filter with this ACE, choose this option. A field for entering an IP protocol value appears.

- **IP Protocol Value**
  When "Other" is selected for the IP protocol value, you can enter a specific value. The allowed range is from 0 to 255. A frame that hits this ACE matches this IP protocol value.

- **IP TTL**
  Specify the Time-to-Live settings for this ACE.
  - Zero: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.
  - Non-zero: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.
  - Any: Any value is allowed ("don't-care").

- **IP Fragment**
  Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.
  - No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.

- "Yes": IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.
- "Any": Any value is allowed ("don't-care").

- **IP Option**
  Specify the options flag setting for this ACE.
  - "No": IPv4 frames where the options flag is set must not be able to match this entry.
  - "Yes": IPv4 frames where the options flag is set must be able to match this entry.
  - "Any": Any value is allowed ("don't-care").

- **SIP Filter**
  Specify the Source IP (SIP) Filter for this ACE.
  - "Any": No source IP filter is specified (Source IP filter is "don't-care").
  - "Host": Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.
  - "Network": Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.

- **SIP Address**
  When "Host" or "Network" is selected for the Source IP Filter, you can enter a specific SIP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly add a deny action.

- **SIP Mask**
  When "Network" is selected for the Source IP Filter, you can enter a specific SIP mask in dotted decimal notation.

- **DIP Filter**
  Specify the destination IP filter for this ACE.
  - "Any": No destination IP filter is specified (Destination IP filter is "don't-care").
  - "Host": Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.
  - "Network": Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.

- **DIP Address**
  When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly add a deny action.

- **DIP Mask**
  When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

IPv6 Parameters

The IPv6 parameters can be configured when Frame Type "IPv6" is selected.

- **Next Header Filter**
  Specify the IPv6 next header filter for this ACE.
  - "Any": No IPv6 next header filter is specified ("don't-care").
  - "Other": If you want to filter a specific IPv6 next header filter with this ACE, choose this option. A field for entering an IPv6 next header value appears.
  - "ICMP": Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained below (ICMP Parameters).
  - "UDP": Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained below (UDP Parameters).

- ⍰TCP⍰: Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained below (TCP Parameters).

- **Next Header Value**
  When "Other" is selected for the IPv6 next header value, you can enter a specific value. The allowed range is from 0 to 255. A frame that hits this ACE matches this IPv6 protocol value.

- **SIP Filter**
  Specify the source IPv6 filter for this ACE.
  - ⍰Any⍰: No source IPv6 filter is specified (Source IPv6 filter is "don't-care").
  - ⍰Specific⍰: Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address and the SIP Bitmask fields that appear.

- **SIP Address**
  When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 address. The field only supports the last 32 bits for the IPv6 address.

- **SIP Bitmask**
  When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supports the last 32 bits for the IPv6 address. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [sipv6_address & sipv6_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFFE (bit 0 is "don't-care" bit), then the SIPv6 address 2001::2 and 2001::3 are applied to this rule.

- **Hop Limit**
  Specify the hop limit settings for this ACE.
  - ⍰0⍰: IPv6 frames with a hop limit field greater than zero must not be able to match this entry.
  - ⍰1⍰: IPv6 frames with a hop limit field greater than zero must be able to match this entry.
  - ⍰Any⍰: Any value is allowed ("don't-care").

ICMP Parameters

The ICMP Parameters described here are valid for the IPv4 as well as for the IPv6 Frame Type.

- **ICMP Type Filter**
  Specify the ICMP filter for this ACE.
  - ⍰Any⍰: No ICMP filter is specified (ICMP filter status is "don't-care").
  - ⍰Specific⍰: If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.

- **ICMP Type Value**
  When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is from 0 to 255. A frame that hits this ACE matches this ICMP value.

- **ICMP Code Filter**
  Specify the ICMP code filter for this ACE.
  - ⍰Any⍰: No ICMP code filter is specified (ICMP code filter status is "don't-care").
  - ⍰Specific⍰: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.

- **ICMP Code Value**
  When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is from 0 to 255. A frame that hits this ACE matches this ICMP code value.

TCP/UDP Parameters

The TCP and the UDP Parameters described here are valid for the IPv4 as well as for the IPv6 Frame Type.

- **TCP/UDP Source Port Filter**
  Specify the TCP/UDP source port filter for this ACE.

- ‘Any’: No TCP/UDP source port filter is specified (TCP/UDP source port filter status is "don't-care").
- ‘Specific’: If you want to filter a specific TCP/UDP source port filter with this ACE, you can enter a specific TCP/UDP source port number. A field for entering a TCP/UDP source port number appears.
- ‘Range’: If you want to filter a specific range TCP/UDP source port filter with this ACE, you can enter a specific TCP/UDP source port range. A field for entering a TCP/UDP source port range value appears.

- **TCP/UDP Source Port No.**
  When "Specific" is selected for the TCP/UDP source port filter, you can enter a specific TCP/UDP source number. The allowed range is from 0 to 65535. A frame that hits this ACE matches this TCP/UDP source number.
- **TCP/UDP Source Port Range**
  When "Range" is selected for the TCP/UDP source port filter, you can enter a specific TCP/UDP source port range value. The allowed range is from 0 to 65535. A frame that hits this ACE matches this TCP/UDP source port value.
- **TCP/UDP Destination Port Filter**
  Specify the TCP/UDP destination port filter for this ACE.
  - ‘Any’: No TCP/UDP destination port filter is specified (TCP/UDP destination port filter status is "don't-care").
  - ‘Specific’: If you want to filter a specific TCP/UDP destination port filter with this ACE, you can enter a specific TCP/UDP destination port number. A field for entering a TCP/UDP destination port number appears.
  - ‘Range’: If you want to filter a specific range TCP/UDP destination port filter with this ACE, you can enter a specific TCP/UDP destination port range. A field for entering a TCP/UDP destination value appears.
- **TCP/UDP Destination Port Number**
  When "Specific" is selected for the TCP/UDP destination port filter, you can enter a specific TCP/UDP destination port number. The allowed range is from 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.
- **TCP/UDP Destination Port Range**
  When "Range" is selected for the TCP/UDP destination port filter, you can enter a specific TCP/UDP destination range value. The allowed range is from 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination port value.
- **TCP FIN**
  Specify the TCP "No more data from sender" (FIN) value for this ACE.
  - ‘0’: TCP frames where the FIN field is set must not be able to match this entry.
  - ‘1’: TCP frames where the FIN field is set must be able to match this entry.
  - ‘Any’: Any value is allowed ("don't-care").
- **TCP SYN**
  Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE.
  - ‘0’: TCP frames where the SYN field is set must not be able to match this entry.
  - ‘1’: TCP frames where the SYN field is set must be able to match this entry.
  - ‘Any’: Any value is allowed ("don't-care").
- **TCP RST**
  Specify the TCP "Reset the connection" (RST) value for this ACE.
  - ‘0’: TCP frames where the RST field is set must not be able to match this entry.
  - ‘1’: TCP frames where the RST field is set must be able to match this entry.
  - ‘Any’: Any value is allowed ("don't-care").

- **TCP PSH**
  Specify the TCP "Push Function" (PSH) value for this ACE.
  - ‘0’: TCP frames where the PSH field is set must not be able to match this entry.
  - ‘1’: TCP frames where the PSH field is set must be able to match this entry.
  - ‘Any’: Any value is allowed ("don't-care").
- **TCP ACK**
  Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.
  - ‘0’: TCP frames where the ACK field is set must not be able to match this entry.
  - ‘1’: TCP frames where the ACK field is set must be able to match this entry.
  - ‘Any’: Any value is allowed ("don't-care").
- **TCP URG**
  Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.
  - ‘0’: TCP frames where the URG field is set must not be able to match this entry.
  - ‘1’: TCP frames where the URG field is set must be able to match this entry.
  - ‘Any’: Any value is allowed ("don't-care").

After the configuration is set, click ‘Save’ to save and activate the setting. To undo any changes made locally and revert to previously saved values, click ‘Reset’. To return to the previous page click ‘Cancel’.

By clicking on the buttons ‘Save’ or ‘Cancel’ the user returns to the Access Control List Configuration page.

7.3.4 DHCP

The DHCP (Dynamic Host Configuration Protocol) protocol is widely used to dynamically allocate reusable network resources, such as an IP address.

7.3.4.1 DHCP Snooping Setting

The addresses assigned to DHCP clients on insecure ports can be carefully controlled using the dynamic bindings registered with the DHCP Snooping. The DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port.

Command Usage:

- Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on a non-secure interface from outside the network or firewall. When the DHCP snooping is enabled globally and enabled on a VLAN interface, DHCP messages received on an untrusted interface from a device not listed in the DHCP snooping table will be dropped.
- Table entries are only learned for trusted interfaces. An entry is added or removed dynamically to the DHCP snooping table when a client receives or releases an IP address from a DHCP server. Each entry includes a MAC address, an IP address, a lease time, a VLAN identifier and port identifier.
- When DHCP snooping is enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.
- If a DHCP packet from a client passes the filtering criteria, it will only be forwarded to trusted ports in the same VLAN.
- If a DHCP packet from a server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.
- If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.

DHCP Snooping Configuration

The status indicates the DHCP snooping mode operation. It can be chosen via the drop-down menu. Possible modes are:

- ⍰Enabled⍰: Enables DHCP snooping mode operation. When the DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and will only allow reply packets from trusted ports.
- ⍰Disabled⍰: Disables DHCP snooping mode operation.

Port Mode Configuration

The status indicates the DHCP snooping port mode. Possible port modes are:

- ⍰Trusted⍰: Configures the port as trusted source of the DHCP messages.
- ⍰Untrusted⍰: Configures the port as untrusted source of the DHCP messages

After the configuration is set, click ⍰Save⍰ to save and activate the setting. To undo any changes made locally and revert to previously saved values, click ⍰Reset⍰.

7.3.4.2 Dynamic DHCP Snooping Table

This page displays the dynamic IP assigned information after the DHCP Snooping mode is disabled. All DHCP clients that obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.

Navigating the DHCP snooping Table

Each page shows up to 99 entries from the Dynamic DHCP snooping table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic DHCP snooping Table. The "MAC address" and "VLAN" input fields allows the user to select the starting point in the Dynamic DHCP snooping table. Clicking the button ⍰Refresh⍰ will update the displayed table starting from that or the closest next Dynamic DHCP snooping table match. In addition, the two input fields will - upon a ⍰Refresh⍰ button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

DHCP Snooping Table Columns

- **MAC Address**
  User MAC address of the entry.
- **VLAN ID**
  VLAN-ID in which the DHCP traffic is permitted.
- **Source Port**
  Switch Port Number for which the entries are displayed.
- **IP Address**
  User IP address of the entry.
- **IP Subnet Mask**
  User IP subnet mask of the entry.
- **DHCP Server**
  DHCP Server address of the entry.

To enable to refresh the page automatically check the box next to ⍰Auto-refresh⍰. Automatic refresh occurs every 3 seconds.
To flush all dynamic entries, click the ⍰Clear⍰ button.
|<< Updates the table starting from the first entry in the Dynamic DHCP snooping table.
>> Updates the table, starting with the entry after the last entry currently displayed.

7.3.5 IP&MAC Source Guard

The IP&MAC Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

7.3.5.1 Configuration

This page provides IP Source Guard related information.

IP Source Guard Configuration

By using the drop-down menu, the Global IP Source Guard Mode can be enabled or disabled. When the mode is enabled all the configured ACEs will be lost.

To translate all dynamic entries to static entries, click on the "Translate dynamic to static" button.

Port Mode Configuration

- **Port**
  The logical port for the settings contained in the same row.
- **Mode**
  By specifying the mode of a port, it will be defined if the IP Source Guard is enabled or disabled on the corresponding port. Only when both the Global Mode and the Port Mode on a given port are enabled, the IP Source Guard is enabled on this port.
- **Max Dynamic Clients**
  The maximum number of dynamic clients that can be learned on given port have to be specified. This value can be 0, 1, 2 or "Unlimited". If the port mode is "Enabled" and the value of max dynamic client is equal to 0, It is only allowed to forward the IP packets that are matched in the static entries on the specific port.

After the configuration is set, click "Save" to save and activate the setting. To undo any changes made locally and revert to previously saved values, click "Reset".

7.3.5.2 Static Table

In this page, the user can manually set the Static Table of the IP&MAC Guard to fulfill the controlling function of the port.

- **Delete**
  Click the button or check the box to delete the entry. It will be deleted during the next save.
- **Port**
  Click on the drop-down menu to select the logical port for the settings.
- **VLAN ID**
  Specify the VLAN ID for the settings.
- **IP Address**
  Allowed Source IP address.
- **MAC address**
  Allowed Source MAC address.

By clicking on the "Add New Entry" button, a new entry for the Static IP Source Guard table can be created.

After the configuration is set, click "Save" to save and activate the setting. To undo any changes made locally and revert to previously saved values, click "Reset".

7.3.6 ARP Inspection

The Dynamic ARP Inspection (DAI) is a security feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. A Dynamic ARP prevents the untrusted ARP packets to go through, based on the DHCP Snooping Database.

7.3.6.1 Port Configuration

This page provides ARP Inspection related configuration.

ARP Inspection Configuration

By using the drop-down menu, the Global ARP Inspection Mode can be enabled or disabled

To translate all dynamic entries to static entries, click on the "Translate dynamic to static" button.

Port Mode Configuration

- **Port**
  The logical port for the settings contained in the same row.
- **Mode**
  By using the port mode configuration table, it can be specified on which ports the ARP Inspection is enabled. Using the drop-down menu, allows to enable or disable the port-based ARP Inspection. Only when both Global Mode and Port Mode on a given port are enabled, the ARP Inspection is enabled on this given port. The possible modes are:
  - "Enabled": Enables the ARP Inspection operation.
  - "Disabled": Disables the ARP Inspection operation.
- **Check VLAN**
  Possible settings of "Check VLAN" are:
  - "Enabled": Enables the check VLAN operation.
  - "Disabled": Disables the check VLAN operation.

  If the user wants to inspect the VLAN configuration, he has to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of the ARP Inspection will refer to the port setting. When the setting of "Check VLAN" is enabled, the log type of the ARP Inspection will refer to the VLAN setting.
- **Log Type**
  Only when the Global Mode and Port Mode on a given port are enabled and the setting of "Check VLAN" is disabled, the log type of the ARP Inspection will refer to the port setting. There are four log types:
  - "None": Log nothing.
  - "Deny": Log denied entries.
  - "Permit": Log permitted entries.
  - "ALL": Log all entries.

After the configuration is set, click "Save" to save and activate the setting. To undo any changes made locally and revert to previously saved values, click "Reset".

7.3.6.2 VLAN Configuration

Each page shows up to 9999 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input field allows the user to select the starting point in the VLAN Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next VLAN Table match. The >> button will use

the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached, the warning message is shown in the displayed table. Use the |<< button to start over.

VLAN Mode Configuration

By using the VLAN mode configuration table, it can be specified on which VLANs the ARP Inspection is enabled. First, the port setting on the "Port mode configuration" web page has to be enabled. Only when both Global Mode and Port Mode on a given port are enabled, the ARP Inspection is enabled on this given port. Second, specify which VLAN will be inspected on the "VLAN mode configuration" web page:

- **Delete**
  Click the button or check the box to delete the entry.
- **VLAN ID**
  Indicates the ID of this particular VLAN.
- **Log Type**
  The log type also can be configured on a per VLAN setting. Possible types are:
  - "None": Log nothing.
  - "Deny": Log denied entries.
  - "Permit": Log permitted entries.
  - "All": Log all entries.

By clicking on the "Add New Entry" button, a new VLAN can be added to the ARP Inspection VLAN table.

After the configuration is set, click "Save" to save and activate the setting. To undo any changes made locally and revert to previously saved values, click "Reset".

7.3.6.3 Static Table

The user can configure manually the Static ARP Inspection Table to control a port.

- **Delete**
  Click the button or check the box to delete the entry. It will be deleted during the next save.
- **Port**
  Click on the drop-down menu to select the logical port for the settings.
- **VLAN ID**
  The VLAN ID for the settings.
- **MAC Address**
  Allowed Source MAC address in ARP request packets.
- **IP Address**
  Allowed Source IP address in ARP request packets.

By clicking on the "Add New Entry" button, a new entry can be created in the Static ARP Inspection table.

After the configuration is set, click "Save" to save and activate the setting. To undo any changes made locally and revert to previously saved values, click "Reset".

7.3.6.4 Dynamic Table

The entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries. These are sorted first by port, then by VLAN ID, then by MAC address and then by IP address.

Navigating the ARP Inspection Table

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "Start from Port", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the ?Refresh? button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the input fields will - upon a ?Refresh? button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

ARP Inspection Table Columns

- **Port**
  Switch Port Number for which the entries are displayed.
- **VLAN ID**
  VLAN-ID in which the ARP traffic is permitted.
- **MAC Address**
  User MAC address of the entry.
- **IP Address**
  User IP address of the entry.
- **Translate to static**
  Select the checkbox to translate the dynamic entry to a static entry.

After the configuration is set, click ?Save? to save and activate the setting. To undo any changes made locally and revert to previously saved values, click ?Reset?.

Check the ?Auto-refresh? box to refresh the page automatically. The automatic refresh occurs every 3 seconds. To refresh the table manually click on the ?Refresh? button. The displayed table will start from the input fields.

7.3.7 AAA ? RADIUS

This page allows the user to configure the RADIUS Servers.

Global Configuration

These setting are common for all the RADIUS servers.

- **Timeout**
  Timeout is the number of seconds, in the range from 1 to 1000 seconds, to wait for a reply from a RADIUS server before retransmitting the request.
- **Retransmit**
  Retransmit is the number of times, in the range from 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.
- **Deadtime**
  Deadtime, which can be set to a number between 1 and 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

- **Key**
  The secret key - up to 63 characters long is shared between the RADIUS server and the switch.
- **NAS-IP-Address (Attribute 4)**
  The IPv4 address is to be used as attribute 4 in the RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.
- **NAS-Identifier (Attribute 32)**
  The identifier - up to 253 characters long is to be used as attribute 32 in the RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

Server Configuration

The table has one row for each RADIUS server.

- **Delete**
  To delete a RADIUS server entry, check the box. The entry will be deleted during the next Save.
- **Hostname**
  The IP address or hostname of the RADIUS server.
- **Auth Port**
  The UDP port to use on the RADIUS server for authentication.
- **Acct Port**
  The UDP port to use on the RADIUS server for accounting.
- **Timeout**
  This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
- **Retransmit**
  This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.
- **Key**
  This optional setting overrides the global key. Leaving it blank will use the global key.

Click on the "Add New Server" button to add a new RADIUS server. An empty row is then added to the table and the RADIUS server can be configured as needed. Up to 5 servers are supported. The "Delete" button can be used to undo the addition of the new server.

After the configuration is set, click "Save" to save and activate the setting. To undo any changes made locally and revert to previously saved values, click "Reset".

7.4 QoS Configuration

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish a control over a network traffic. QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical and file-backup traffic. This function can not only reserve bandwidth, but also limit other traffic that is not so important.

7.4.1 Port Classification

This page allows you to configure the basic QoS Ingress Port Classification settings for all switch ports.

- **Port**
  The port number for which the configuration below applies.
- **CoS**

This field controls the default Class of Service (CoS), ranging from 0 (lowest) to 7 (highest).
All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority.
The classified CoS can be overruled by a QCL entry.
Note: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.

- **DPL**
  Controls the default drop precedence level (DPL). All the frames are classified to a drop precedence level.
  If the port is VLAN aware and the frame is tagged, then the frame is classified to a DPL that is equal to the DEI value in the tag. Otherwise the frame is classified to the default DPL.
  The classified DPL can be overruled by a QCL entry.

- **PCP**
  Controls the default PCP (Priority Code Point) value. All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.

- **DEI**
  Controls the default DEI (Drop Eligible Indicator) value. All frames are classified to a DEI value.
  If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.

- **Address Mode**
  The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are:
  - ?Source?: Enable SMAC/SIP matching
  - ?Destination?: Enable DMAC/DIP matching

After the configuration is set, click ?Save? to save and activate the setting. To undo any changes made locally and revert to previously saved values, click ?Reset?.

7.4.2 Port Policing

This page allows the user to configure the QoS Ingress Port Policer settings for all switch ports.

- **Port**
  The port number for which the following configuration applies.

- **Enabled**
  Controls whether the policer is enabled or not on this switch port. By checking the box, the Port Policing is enabled.

- **Rate**
  Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps" and it is restricted to 1-3300 when the "Unit" is "Mbps" or "kfps".

- **Unit**
  Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps. The default value is "kbps".

- **Flow Control**
  If the flow control is enabled and the port is in flow control mode, then the pause frames are sent instead of the discarding frames. By checking the box, the Flow Control is enabled.

After the configuration is set, click ?Save? to save and activate the setting. To undo any changes made locally and revert to previously saved values, click ?Reset?.

7.4.3 Port Scheduler

This page provides an overview of the QoS Egress Port Schedulers for all switch ports.

- **Port**
  The number indicates the logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers. By clicking on a port number, the corresponding page "QoS Egress Port Scheduler and Shapers" opens (see chapter 6.4.5).
- **Mode**
  The content shows the scheduling mode for this port.
- **Weight " Qn**
  The content shows the weight for this queue and port.

7.4.4 Port Shaping

This page provides an overview of QoS Egress Port Shapers for all switch ports.

- **Port**
  The number indicates the logical port for the settings contained in the same row. Click on the port number in order to configure the shapers. By clicking on a port number, the corresponding page "QoS Egress Port Scheduler and Shapers" opens (see chapter 6.4.5).
- **Shapers " Qn**
  The content shows "disabled" or the actual queue shaper rate - e.g. "800 Mbps".
- **Shapers " Port**
  The content shows "disabled" or the actual port shaper rate - e.g. "800 Mbps".

QoS Egress Port Scheduler and Shapers " Port X

By clicking on a port number in the pages "QoS Egress Port Schedulers" (chapter 6.4.3) and "QoS Egress Port Shapers" (chapter 6.4.4) this page opens. This page allows the user to configure the Scheduler and Shapers for a specific port. The port can be selected by the drop-down menu on the top right.

- **Scheduler Mode**
  Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.
- **Queue Shaper " Enable**
  Controls whether the queue shaper is enabled for this queue on this switch port.
- **Queue Shaper " Rate**
  Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" and it is restricted to 1-3300 when the "Unit" is "Mbps".
- **Queue Shaper " Unit**
  Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".
- **Queue Shaper " Excess**
  Controls whether the queue is allowed to use excess bandwidth.
- **Queue Scheduler " Weight**
  Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
- **Queue Scheduler " Percent**
  Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

- **Port Shaper Enable**
  Controls whether the port shaper is enabled for this switch port.
- **Port Shaper Rate**
  Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" and it is restricted to 1-3300 when the "Unit" is "Mbps".
- **Port Shaper Unit**
  Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

After the configuration is set, click Save to save and activate the setting. To undo any changes made locally and revert to previously saved values, click Reset. To stop the configuration and to go back to the previous page click on the Cancel button. Changes that haven't been saved will be lost.

7.4.5 QoS Control List

The QoS Control List Configuration page shows the QoS Control List (QCL), which is made up of the QCEs. Each row describes a defined QCE.

Click on the lowest plus sign to add a new QCE to the list.

- **QCE**
  Indicates the QCE ID.
- **Port**
  Indicates the list of ports configured with the QCE.
- **DMAC**
  Indicates the Destination MAC address (DMAC). Possible values are:
  - Any: Match any DMAC.
  - Unicast: Match unicast DMAC.
  - Multicast: Match multicast DMAC.
  - Broadcast: Match broadcast DMAC.

  The default value is 'Any'.
- **SMAC**
  Indicates the Source MAC address (SMAC). Possible values are:
  - Any: Match any SMAC.
  - Specific: Match a specific SMAC.

  If a port is configured to match on DMAC/DIP, this field indicates the DMAC.
- **Tag Type**
  Indicates the tag type. Possible values are:
  - Any: Match tagged and untagged frames.
  - Untagged: Match untagged frames.
  - Tagged: Match tagged frames.
  - C-Tagged: Match C-tagged frames.
  - S-Tagged: Match S-tagged frames.

  The default value is 'Any'.

- **VID**
  VLAN ID: Indicates either a specific VID or a range of VIDs. VID can be in the range 1-4095 or 'Any'.
- **PCP**
  Priority Code Point: Valid values of PCP are a specific (0, 1, 2, 3, 4, 5, 6, 7), a range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
- **DEI**
  Drop Eligible Indicator: Valid values of DEI are 0, 1 or 'Any'.
- **Frame Type**
  Indicates the type of frame. Possible values are:
  - Any: Match any frame type.
  - Ethernet: Match EtherType frames.
  - LLC: Match LLC frames.
  - SNAP: Match SNAP frames.
  - IPv4: Match IPv4 frames.
  - IPv6: Match IPv6 frames.
- **Action**
  Indicates the classification action taken on an ingress frame, if the configured parameters are matched with the frame's content. Possible actions are:
  - CoS: Classify Class of Service.
  - DPL: Classify Drop Precedence Level.
  - DSCP: Classify DSCP value.
- **Modification Buttons**
  You can modify each QCE (QoS Control Entry) in the table using the following buttons:

  Add: Inserts a new QCE before the current row.

  Edit: Edits this QCE.

  Up: Moves this QCE up the list.

  Down: Moves this QCE down the list.

  Delete: Deletes this QCE.

  Add: The lowest plus sign adds a new entry at the bottom of the QCE listings.

A. QCE Configuration

By clicking on the "Edit" button or on one of the « Add » buttons , the QCE Configuration page opens. This page allows to edit/insert a single QoS Control Entry at a time. A QCE consists of several parameters. These parameters vary according to the frame type that the user selects.

Port Members

Check the checkbox button to include the port in the QCL entry. By default, all ports are included.

Key Parameters

The key parameters can be configured as follows:

- **DMAC (Destination MAC address)**
  Possible values are 'Unicast', 'Multicast', 'Broadcast' or 'Any'.
- **SMAC (Source MAC address)**
  Possible values are 'Specific' (xx-xx-xx-xx-xx-xx) or 'Any'. If a port is configured to match on DMAC/DIP, this field is the Destination MAC address.

- **Tag**
  The value of the Tag field can be 'Untagged', 'Tagged' or 'Any'.
- **VID**
  A valid value of the VLAN ID (VID) can be any value in the range 1-4095 or 'Any'. The user can enter either a 'specific' value or a 'range' of VIDs.
- **PCP**
  Valid values of the Priority Code Point (PCP) are a specific one (0, 1, 2, 3, 4, 5, 6, 7), a range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
- **DEI**
  A valid value of the Drop Eligible Indicator (DEI) can be '0', '1' or 'Any'.
- **Frame Type**
  The Frame Type can have any of the following values. Except for ‘Any’, each frame type has specific parameters to define. They are explained below.
  - Any: Allows all types of frames.
  - EtherType
  - LLC
  - SNAP
  - IPv4
  - IPv6

Action Parameters

- **CoS (Class of Service)**
  Valid values of the CoS are a specific one (0, 1, 2, 3, 4, 5, 6, 7) or 'Default'.
- **DPL (Drop Precedence Level)**
  Valid values of the CoS are a specific one (0 or 1) or 'Default'.
- **DSCP**
  Valid values of the DSCP are a specific one (0-63, BE, CS1-CS7, EF, AF11- AF13, AF21-AF23, AF31-AF33 or AF 41-AF43) or 'Default'.

Note: 'Default' means that the default classified value is not modified by this QCE.

EtherType Parameters

This parameter has only to be defined, when for the Frame Type of the Key parameters above has been selected ‘EtherType’.

A valid value of the EtherType can be a specific one (0x600-0xFFFF excluding 0x800 (IPv4) and 0x86DD (IPv6)) or 'Any'.

LLC Parameters

These parameters have only to be defined, when for the Frame Type of the Key parameters above has been selected ‘LLC’.

- **SSAP Address**
  A valid value of the SSAP (Source Service Access Point) can be a 'Specific' that varies from 0x00 to 0xFF or be 'Any'.
- **DSAP Address**
  A valid value of the DSAP (Destination Service Access Point) can be a 'Specific' that varies from 0x00 to 0xFF or be 'Any'.
- **Control**
  A valid value of the Control field can be a 'Specific' that varies from 0x00 to 0xFF or be 'Any'.

SNAP Parameters

This parameter has only to be defined, when for the Frame Type of the Key parameters above has been selected „SNAP".

A valid value of the PID (a.k.a EtherType) can be a 'Specific' one that varies from 0x0000 to 0xFFFF or be 'Any'.

IPv4 Parameters

These parameters have only to be defined, when for the Frame Type of the Key parameters above has been selected „IPv4".

- **Protocol**
  A valid value of the IP protocol number can be 'TCP', 'UDP', 'Other' (a value in the range from 0 to 255) or 'Any'. For the definition of the UDP or TCP Parameters see below.
- **SIP**
  The Source IP address (SIP) can be a specific one (in value and mask format) or 'Any'.
  The IP Value and the Mask are in the format w.x.y.z, with w, x, y and z being decimal numbers between 0 and 255. When the Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero. If a port is configured to match on DMAC/DIP, this field is the Destination IP address.
- **IP Fragment**
  To fragment the packets, the possible options for an IPv4 frame fragment are: 'Yes', 'No' or 'Any'.
- **DSCP**
  The Differentiated Services (DiffServ) Code Point (DSCP) value can be a specific value, a range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF, AF11-AF13, AF21-23, AF31-AF33 and AF41-AF43.

IPv6 Parameters

These parameters have only to be defined, when for the Frame Type of the Key parameters above has been selected „IPv6".

- **Protocol**
  A valid value of the IP protocol number can be 'TCP', 'UDP', 'Other' (a value in the range from 0 to 255) or 'Any'. For the definition of the UDP or TCP Parameters see below.
- **SIP (32 LSB)**
  The 32 LSB (Least Significant Bits) of the IPv6 Source IP address (SIP) can be specific ones (in value and mask format) or 'Any'.
  If a port is configured to match on DMAC/DIP, this field is the Destination IP address.
- **DSCP**
  The Differentiated Services (DiffServ) Code Point (DSCP) value can be a specific value, a range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF, AF11-AF13, AF21-23, AF31-AF33 and AF41-AF43.

UDP/TCP Parameters

These parameters have only to be defined, when for the Protocol of the IPv4/IPv6 parameters above has been selected „UDP" or „TCP".

- **Sport**
  The Source port (Sport) value, applicable for the IP protocols UDP or TCP, can be a specific one, a range or 'Any'. The specific one as well as the range is limited to values between 0 and 65535.

- **Dport**
  The Destination port (Dport) value, applicable for the IP protocols UDP or TCP, can be a specific one, a range or 'Any'. The specific one as well as the range is limited to values between 0 and 65535.

After the configuration is set, click ‘Save’ to save and activate the setting as well as to return to the main QoS Control List Configuration page. To undo any changes made locally and revert to the previously saved values, click ‘Reset’. To return to the previous page without saving the configuration change click ‘Cancel’.

7.4.6 Storm Control

The Storm control for the switch is configured on this page. There is a unicast storm rate control, a multicast storm rate control and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch.

Strom Control Configuration

- **Frame Type**
  The switch supports 3 kinds of Frame Types: Unicast, Multicast and Broadcast. The settings in a particular row apply to the corresponding frame type.
- **Enable**
  By checking the box, the storm control status for the given frame type is enabled.
- **Rate (pps)**
  The frame rate’s unit is ‘packets per second (pps)’. The valid values are:
  1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K or 1024K.

After the configuration is set, click ‘Save’ to save and activate the setting. To undo any changes made locally and revert to the previously saved values, click ‘Reset’.

8. Maintenance

8.1 Diagnostics

8.1.1 CPU Load

This page displays the CPU load in percentage using an SVG graph.

The load is measured as the average over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed and the last numbers are displayed as text as well.

In order to display the SVG graph, the used browser must support the SVG format. It may be necessary to install a plugin to support SVG.

To refresh the page automatically, check the box next to „Auto-refresh“ on the top right of the page. The automatic refresh occurs every 3 seconds.

8.2 Maintenance

8.2.1 Reboot Device

This page is used to restart the switch. To perform a restart of this device, click on the button „Yes“. To return to the „System Information“ page (chapter 3.1) without restarting, click on the button „No“.

After the restart, the switch will boot normally.

It is also possible to restart the switch locally. For more information go to chapter „Reboot device“ in the operating instructions.

8.2.2 Factory Reset

This page is used to reset the switch to return to the factory settings. To perform a restart of this device, click on the button „Yes“. To return to the „*System Information*“ page (chapter 3.1) without restarting, click on the button „No“.

The reset will take 120 seconds to be finished. After the reset, the switch will be active immediately.

It is also possible to reset the switch locally. For more information go to chapter „Factory configuration reset“ in the operating instructions.

8.2.3 Firmware Upgrade

The device‘s firmware can be updated to install new functions. The current versions are displayed in the page „Firmware List“ (chapter 7.2.4). This page facilitates a Software Update of the firmware controlling the switch.

By clicking on the „Browse“ button, the user can select the firmware that needs to be upgraded by choosing the location of the software image. It will be uploaded by clicking on the „Upload“ button.

After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.

IMPORTANT REMARK!

While the firmware is being updated, the web access appears to be defunct. Do not restart or power off the device during this time or the switch may fail to function afterwards.

8.2.4 Firmware List

This page provides a list of the different software and their current versions installed on this device.

9. Switch off

To stop and switch-off the product, it is necessary to:

- Disconnect the network cables.
- Disconnect the mains.
- Wait one (1) minute until the product turns off.

SLAT

11, Rue Jean Elysée Dupuy BP66
69543 Champagne au Mont d'Or Cedex
FRANCE

Tel.: +33 478 66 63 60
Fax: +33 478 47 54 33

e-mail: comm@slat.fr

SLAT GmbH

Leitzstraße 45
70469 Stuttgart
DEUTSCHLAND

Tel.: +49 711 899 890 08
Fax: +49 711 899 890 90

E-mail: info@slat-gmbh.de

www.slat.com