

# AMS Series Gigabit Managed Switches



AMS-10T2SFP AMS-26T6SFP AMS-48T4SFP AMS-24T4S4SP AMS-48T4S4SP AMS-4T24S4SP

# User Manual

About this Guide	6
Compliances and Safety Statements	7
Introduction	11
Overview	11
1. Operation of the Web-based Management	12
1.1 System	14
1.1.1 System Information	14
1.1.1-1 Information	14
1.1.1-2 Configuration	16
1.1.1-3 CPU Load	17
1.1.2 Time	18
1.1.2-1 Manual	18
1.1.2-2 NTP	20
1.1.3 Account	21
1.1.3-1 Users	
1.1.3-2 Privilege Level	
1.1.4 IP	24
1.1.4-1 IPv4	
1.1.4-2 IPv6	26
1.1.5 Syslog	28
1.1.5-1 Configuration	28
1.1.5-2 Log	29
1.1.5-3 Detailed Log	30
1.1.6 SNMP	31
1.1.6-1 System	31
1.1.6-2 Configuration	32
1.1.6-3 Communities	33
1.1.6-4 Users	
1.1.6-5 Groups	
1.1.6-6 Views	
1.1.6-7 Access	
1.1.6-8 Trap	44
1.2 Configuration	47
1.2.1 Port	47
1.2.1-1 Configuration	
1.2.1-2 Port Description	
1.2.1-3 Traffic Overview	

1.2.1-4 Detailed Statistics	53
1.2.1-5 QoS Statistics	
1.2.1-6 SFP Information	
1.2.1-7 EEE	
1.2.2 ACL	60
1.2.2-1 Ports	
1.2.2-2 Rate Limiters	
1.2.2-3 Access Control List	
1.2.2-4 ACL Status	
1.2.3 Aggregation	77
1.2.3-1 Static Trunk	
1.2.3-2 LACP	
1.2.3-2-1 Configuration	
1.2.3-2-2 System Status	
1.2.3-2-3 Port Status	
1.2.3-2-4 Port Statistics	85
1.2.4 Spanning Tree	
1.2.4-1 Bridge Settings	
1.2.4-2 MSTI Mapping	91
1.2.4-4 CIST Ports	94
1.2.4-5 MSTI Ports	96
1.2.4-6 Bridge Status	98
1.2.4-7 Port Status	100
1.2.4-8 Port Statistics	102
1.2.5 IGMP Snooping	104
1.2.5-1 Basic Configuration	105
1.2.5-2 VLAN Configuration	
1.2.5-3 Port Group Filtering	109
1.2.5-4 Status	111
1.2.5-5 Groups Information	113
1.2.5-6 IPv4 SSM Information	115
1.2.6 MLD Snooping	117
1.2.6-1 Basic Configuration	117
1.2.6-2 VLAN Configuration	120
1.2.6-3 Port Group Filtering	
1.2.6-4 Status	
1.2.6-5 Groups Information	126
1.2.6-6 IPv6 SSM Information	128
1.2.7 MVR	130
1.2.7-1 Configuration	130
1.2.7-2 Groups Information	
1.2.7-3 Statistics	133
1.2.8 LLDP	135

1.2.8-1 LLDP Configuration	135
1.2.8-2 LLDP Neighbours	
1.2.8-3 LLDP-MED Configuration	
1.2.8-4 LLDP-MED Neighbours	
1.2.8-5 EEE	
1.2.8-6 Port Statistics	
1.2.9 Filtering Data Base	156
1.2.9-1 Configuration	156
1.2.9-2 Dynamic MAC Table	158
1.2.10 VLAN	159
1.2.10-1 VLAN Membership	159
1.2.10-2 Ports	161
1.2.10-3 Switch Status	164
1.2.10-4 Port Status	166
1.2.10-5 Private VLAN	168
1.2.10-5-1 Private VLAN Membership	168
1.2.10-5-2 Port Isolation	170
1.2.10-6 MAC-based VLAN	171
1.2.10-6-1 Configuration	171
1.2.10-6-2 Status	173
1.2.10-7 Protocol-based VLAN	174
1.2.10-7-1 Protocol to Group	174
1.2.10-7-2 Group to VLAN	177
1.2.11 Voice VLAN	
1.2.11-1 Configuration	179
1.2.11-2 OUI	182
1.2.12 GARP	184
1.2.12-1 Configuration	184
1.2.12-2 Statistics	187
1.2.13 GVRP	188
1.2.13-1 Configuration	
1.2.13-2 Statistics	
1.2.14 QoS	191
1.2.14-1 Port Classification	
1.2.14-2 Port Policing	
1.2.14-3 Port Scheduler	
1.2.14-4 Port Shaping	
1.2.14-5 Port Tag Remarking	
1.2.14-6 Port DSCP	
1.2.14-7 DSCP-based QoS	
1.2.14-8 DSCP Translation	
1.2.14-9 DSCP Classification	211
1.2.14-10 QoS Control List	

1.2.14-11 QCL Status	217
1.2.14-12 Storm Control	
1.2.15 s-Flow Agent	221
1.2.15-1 Collector	
1.2.15-2 Sampler	
1.2.16 Loop Protection	225
1.2.16-1 Configuration	225
1.2.16-2 Status	227
1.2.17 Single IP	228
1.2.17-1 Configuration	228
1.2.17-2 Information	230
1.2.18 Easy Port	232
1.2.19 Mirroring	235
1.2.20 Trap Event Severity	237
1.2.21 SMTP Configuration	239
1.2.22 UPnP	241
1.3 Security	243
1.3.1 IP Source Guard	243
1.3.1-1 Configuration	243
1.3.1-2 Static Table	245
1.3.1-3 Dynamic Table	247
1.3.2 ARP Inspection	249
1.3.2-1 Configuration	249
1.3.2-2 Static Table	251
1.3.2-3 Dynamic Table	253
1.3.3 DHCP Snooping	255
1.3.3-1 Configuration	255
1.3.3-2 Statistics	257
1.3.4 DHCP Replay	259
1.3.4-1 Configuration	259
1.3.4-2 Statistics	261
1.3.5 NAS	263
1.3.5-1 Configuration	
1.3.5-2 Switch Status	274
1.3.5-3 Port Status	276
1.3.6 AAA	277
1.3.6-1 Configuration	
1.3.6-2 RADIUS Overview	281

1.3.6-3 RADIUS Details	283
1.3.7 Port Security	289
1.3.7-1 Limit Control	289
1.3.7-2 Switch Status	
1.3.7-3 Port Status	
1.3.8 Access Management	296
1.3.8-1 Configuration	
1.3.8-2 Statistics	
1.3.9 SSH	300
1.3.10 HTTPS	301
1.3.11 Auth Method	303
1.4 Maintenance	305
1.4.1 Restart Device	305
1.4.2 Firmware	306
1.4.2-1 Firmware Upgrade	306
1.4.2-2 Firmware Selection	308
1.4.3 Save/Restore	310
1.4.3-1 Factory Defaults	310
1.4.3-2 Save Start	
1.4.3-3 Save User	
1.4.3-4 Restore User	313
1.4.4 Export/Import	314
1.4.4-1 Export Configuration	
1.4.4-2 Import Configuration	315
1.4.5 Diagnostics	316
1.4.5-1 Ping	316
1.4.5-2 Ping6	318
1.4.5-3 VeriPHY	319
2. Specifications	320

# About this Guide

# Purpose

this guide gives specific information on how to operate and use the management functions of the switch.

# Audience

The guide is intended for use by network administrators who are responsible for operating and maintaining network equipment; consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

# Warranty

The AMS series comes with a standard 3 year warranty. For full Alloy warranty terms and conditions please follow the link below:

http://www.alloy.com.au/Warranty

## Conventions

The following conventions are used throughout this guide to show information:



**NOTE:** Emphasizes important information or calls your attention to related features or instructions.



**WARNING:** Alerts you to a potential hazard that could cause personal injury.



**CAUTION:** Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

# **Compliances and Safety Statements**

#### Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

**FCC Caution:** Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

#### European Community (CE) Electromagnetic Compatibility Directive

This information technology equipment complies with the requirements of the Council Directive 89/336/EEC on the Approximation of the laws of the Member States relating to Electromagnetic Compatibility and 73/23/EEC for electrical equipment used within certain voltage limits and the Amendment Directive 93/68/EEC. For the evaluation of the compliance with these Directives, the following standards were applied:

RFI Emission: - Limit according to EN 55022:2010 AS/NZS CISPR 22:2009, Class A

- Limit for harmonic current emission according to EN 61000-3-2:2006+A1:2009+A2:2009
- Limitation of voltage fluctuation and flicker in low-voltage supply system according to EN 61000-3-3:2008
- Immunity: Product family standard according to EN 55024:2010
  - Electrostatic Discharge according to IEC 61000-4-2:2008

- Radio-frequency electromagnetic field according to IEC 61000-4-3:2006+A1:2007+A2:2010
- Electrical fast transient/burst according to IEC 61000-4-4:2010
- Surge immunity test according to IEC 61000-4-5:2005
- Immunity to conducted disturbances, Induced by radio-frequency

Fields: IEC 61000-4-6:2008

- Power frequency magnetic field immunity test according to IEC

61000-4-8:2009

- Voltage dips, short interruptions and voltage variations immunity test

According to IEC 61000-4-11:2004

LVD: - EN60950-1:2006+A11:2009+A1:2010EMC:

#### Australian C-Tick Compliance.

This equipment is compliant with the required Australian C-Tick standards

# PLEASE READ THE FOLLOWING SAFETY INFORMATION CAREFULLY BEFORE INSTALLING THE SWITCH:

**WARNING:** Installation and removal of the unit must be carried out by qualified personnel only.

- This guide is intended for use by network administrators who are responsible for setting up and installing network equipment; consequently it assumes a basic working knowledge of LANs (Local Area Networks).
- The unit must be connected to an earthed (grounded) outlet to comply with international safety standards.
- Do not connect unit to an A.C outlet (power supply) without an earth (ground) connection.
- The appliance coupler (the connector to the unit and not the wall plug) must have a configuration for mating with an EN 60320/IEC 320 appliance inlet.
- The socket outlet must be near to the unit and easily accessible. You can only remove power from the unit by disconnecting the power cord from the outlet.
- This unit operates under SELV (Safety Extra Low Voltage) conditions according to IEC 60950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.

#### SAFETY PRECAUTIONS

Read the following information carefully before operating the device. Please follow the following precaution items to protect the device from risks and damage caused by fire and electric power:

- Use the power adapter that is included with the device package.
- Pay attention to the power load of the outlet or prolonged lines. An overburdened power outlet or damaged cords and plugs may cause electric shock or fire. Check the power cords regularly, if you find any damage, replace it at once.
- Proper space for heat dissipation is necessary to avoid any damage caused by device overheating. The ventilation holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these ventilation holes.
- Do not put this device close to a place where a heat source exits or high temperature occurs. Avoid placing the device in direct sunshine.
- Do not put this device close to a place which is damp or wet. Do not spill any fluid on this device.
- Please follow the instructions in the user manual/quick install guide carefully to connect the device to your PC or other electronic product. Any invalid connection may cause a power or fire risk.

Do not place this device on an unstable surface or support.



**CAUTION:** Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge.

To protect your device, always:

- Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.
- Pick up the device by holding it on the left and right edges only.
- If you are connecting a device mounted outdoors to this switch please ensure you have installed an additional lightning arrestor between this device and the outdoor equipment.



Fig. Additional arrester installed between outdoor device and this switch

**NOTE:** The switch is indoor device; if it will be used in outdoor environment or connects with some outdoor device, then it must use a lightning arrester to protect the switch



#### WARNING:

- Self-demolition of Product is strictly prohibited. Damage caused by self-demolition will result in voiding the switches warranty.
- Do not place product in outdoor locations.
- Before installation, please make sure input power supply and product specifications are compatible to each other.
- To reduce the risk of electric shock. Disconnect all AC or DC power cords and RPS cables to completely remove power from the unit.
- Before importing / exporting configuration please make sure the firmware version is always the same.

# Introduction

# **Overview**

In this user's manual, we will explain how to configure and monitor the AMS Series switches through the Web Management Interface.

The AMS Series, the next generation Web managed switches from Alloy, are a portfolio of affordable managed switches that provides a reliable infrastructure for your business network. These switches deliver more intelligent features you need to improve the availability of your critical business applications, protect your sensitive information, and optimize your network bandwidth to deliver information and applications more effectively. It provides the ideal combination of affordability and capabilities for entry level networking includes small business or enterprise application and helps you create a more efficient, better-connected workforce.

The major features of the AMS series Switches are outlined below:

- Wirespeed performance up to 130.94mpps switching architecture, 136Gbps forwarding rate
- High density port configurations up to 52 ports
- Dual speed SFP+ slots supporting Gigabit or 10Gigabit mini-GBICs modules
- Dual speed SFP slots for Fast Ethernet or Gigabit mini-GBIC modules
- Layer 2 Plus features provide enhanced manageability, security, QoS and Performance
- Easy to use Web Based Management
- Comprehensive VLAN, GVRP, DHCP Relay, IGMP and MLD Snooping functions
- Advanced QoS features including hardware Priority Queues, SR and WRR Scheduling, all major Classification regimes, Rate limiting and IPv6 Applications
- IPv6 and s-Flow support
- IEEE 802.3az Energy Efficient Ethernet standard
- Robust security features including SSH, SSL, HTTPS, 802.1x, Layer 2 Isolation, IP Source Guard, RADIUS/TACACS+, and ACLs
- Carrier Grade Ethernet: IEEE 802.3ah OAM 802.1ag Ethernet CFM, ITU-T Y.1731 Performance Monitoring ITU-T G.8032 (future release) and IEEE 588v2 PTP support (AMS-4T24S4SFP)

# **1. Operation of the Web-based Management**

This chapter instructs you on how to configure and manage the AMS Series switches through the web user interface. With this facility, you can easily access and monitor the switch through any of the Ethernet ports and view the status of the switch, including MIBs status, each port activity, Spanning tree status, port aggregation status, multicast traffic, VLAN and priority status, even illegal access record and so on.

The default values of the AMS Series switches are listed in the table below:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Username	admin
Password	

To access the web management of an AMS Series switch enter the default IP Address in web browser and hit enter. E.g. <u>http://192.168.1.1</u>

Once you have entered the IP Address into the web browser you will be prompted to enter a Username and Password in order to access the web management interface. Enter the default values as shown in the table above.

The AMS Series switches support a simple user management function allowing only one administrator to configure the system at the same time. If there are two or more users using the administrator's identity, it will allow only the first user who logs in to configure the system. The rest of the users, even with administrator's identity, can only monitor the system. For those who do not have administrator access they will only be able to monitor the system. Only a maximum of three users are able to login simultaneously.



#### NOTE:

The AMS Series switches support management interface on both IPv4 and IPv6 IP Addresses.

To optimize the display, we recommend you use Microsoft IE 6.0 and above, Netscape V7.1 and above or FireFox V1.00 and above and a screen resolution of 1024x768.

The server 19 password.	2.168.1.1 at AMS-24T6SFP requires a usernam	e and
	Password	
	Remember my credentials	

Fig. 1 The login page

# 1.1 System

This chapter describes the basic configuration tasks required to configure the system information on the AMS Series switches. The System Information page is the default page and will be the first page you see when you log into the switches web interface.

# 1.1.1 System Information

The System Information page shows you the following: Model Name, System Description, Location, Contact, Device Name, System Date, System Uptime, BIOS Version, Firmware Version, Hardware-Mechanical Version, Series Number, Host IP Address, Subnet Mask, Gateway IP Address, Host MAC Address, Console Baudrate, RAM Size, Flash Size, Bridge FDB Size, Transmit Queue and Maximum Frame Size. All relevant fields will be explained in more detail in the chapter.

# 1.1.1-1 Information

The switches system information is provided here.

# Web Interface

To view the System Information via the Web Interface:

 Click System, System Information and Information. The current configuration will be displayed, this is read only, and nothing can be configured here.

MS-24T6SFP		And a state state of the state of	Auto-Logout Logout
System	System Information		Auto-refresh 🥅 Refream
System Information Information			Harvest In Reveal
Configuration	Model Name	AMS-2416SFF	
CPU Load	System Description	20-Port 10/100/1000Base-T + 4 TP/(100/1G) SFP Comte + 2 (100/1G) SFP L2 Plus Managed Switch	
► Time	Location		
Account	Contact		
P Account	Device Name	AMS-2416SFP	
	System Date	2011-01-04 01:49:42	
Syslog	System Uptime	36 01 49 42	
► SNMP	BIOS Version	V1.00	
Configuration	Firmware Version	v1 42 2012-08-24	
Security	Hardware-Mechanical Version		
Maintenance	Series Number	03390500004	
	Host IP Address	192 168 1 1	
	Subnet Mask	255 256 255 0	
	Gateway IP Address	192.108.1.254	
	Host MAC Address	00-00-8c-00-00.4Z	
	Console Baudrate	115200	
	RAM Size	644/8	
	Flash Size	19AB	
	Bridge FDB Size	8192 MAC Addresses	
	Transmit Queue	8 queues per pot	
	Maximum Frame Size	9600	
	ī		

Fig. 2 System Information

Model Name:	The model name of this device.
System Description:	A brief description of this device.
Location:	A user-defined value describing the location of the switch.
Contact:	A user-defined value, normally the system/network administrator details will be entered here.
Device Name:	A user-defined value, give the switch a descriptive name for easy identification.
System Date:	Shows the system time and date of the switch. These details can be configured in the Time section. Format is YYYY-MM-DD HH:MM:SS.
System Uptime:	The time accumulated since the switch was powered on. Format is Day, Hour, Minute, Second.
BIOS Version:	The current BIOS version running in the switch.
Firmware Version:	The current firmware version running in the switch.
Hardware-Mechanical:	The current hardware and mechanical version numbers. The figure before the hyphen is the hardware version, the figure after the hyphen is the mechanical version.
Series Number:	The chipset serial number. Please note this is not the serial number of the actual switch.
Host IP Address:	The IP Address of the switch.
Subnet Mask:	The subnet mask of the switch.
Default Gateway:	The default gateway of the switch.
Host MAC Address:	The MAC Address of the management interface of the switch.
Console Baudrate:	The currently configured Baudrate of the switch.
RAM Size:	The size of the RAM in the switch.
Flash Size:	The size of the flash memory in the switch.
Bridge FDB size:	Displays the current Bridge FDB size.
Transmit Queue:	Displays the switches transmit hardware priority queue information.

Maximum Frame Size: Displays the switches maximum supported frame size.

# 1.1.1-2 Configuration

The Contact Information, name and the location of switch and can all be configured here.

#### Web Interface

To configure the contact information via the web interface:

- 1 Click System, System Information and Configuration.
- 2 Enter the required Contact, Device Name and Location details in the fields provided.
- 3 Click Save to apply your changes.



Fig. 3 System Information Configuration

Parameter Description	
System Contact:	The system/network administrator details will be entered here, as well as a contact phone number. The allowed string length is 0 to 255 characters.
System Name:	An administratively assigned name for the switch. By convention, this is the switches fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.

System Location: The physical location of the switch (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

# 1.1.1-3 CPU Load

This page displays the CPU load, using an SVG graph. The load is measured as averaged 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, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG.

# Web Interface

To view the CPU Load via the web interface:

- 1 Click System, System Information and CPU Load.
- 2 The CPU Load will be displayed on the screen.
- 3 If you wish to enable the Auto-Refresh function, tick the check box in the top right hand corner of the screen.

MS-24T6SFP		
System	Atto Logot 10#	Logout Hel
System Information Information Configuration CPU Load     Time Manual	CPU Load         100ms 0%         1 sec 10%         10sec 10%         (all numbers running average)	Auto-refresh 🕧 🏠
NTP + Account + IP + Syslog + SMMP - Sonfiguration Security Valotenance		75%
		50%
		25%
		2370

# Parameter Description

Fig. 4 CPU Load

Auto-Refresh: To enable Auto-Refresh, tick the check box in the top right hand corner of the screen.

# 1.1.2 Time

The page is used to configure the time setting on the switch. Time can be set manually or via a NTP server. By default NTP is used and is set to au.pool.ntp.org.

# 1.1.2-1 Manual

The time for the switch can set manually or via a NTP Server. When setting manually simply enter the date and time into the paces provided.

## Web Interface

To configure the time settings via the Web Interface:

- 1. Click System, Time and Manual.
- 2. Select use Local Settings.
- 3. Enter the time and date into the Local Time field.
- 4. Enter the Time Zone Offset.
- 5. If you would like to enable Daylight Savings, un-tick the box and enter the required Time Offset and the dates for when Daylights Savings begins and ends.
- 6. Click Save to apply your changes.

192.168.1.1			
LOY	AND Statement		
SFP			Auto-Logoul
ISFF			OFF .
	- COS - 1 - 1		
Information	Time Configuration	n	
	Clock Source:	Use Lotal Settings	
	Local Time:	Use NTP Server 2012-19-01 13 01-29 VYYY-MILLED HH MM/ SS	
1	Time Zone Offset:	2012-000 130129 1111-Waldou miniwa 35	
	Daylight Savings:	Disabled	
	Time Set Offset:	00 min (Range 1 - 1440, Default 60)	
tion	Daylight Savings Type:	By dates	
sce.	From:	* Recurrence YYYY-MIAOD HH MM	
	To:	YYYY-MMADD HHIMM	
	From:	Day Sun - Week First - Marille Oct - Time (2.00 Het MM	
	To:	Day Sun + Week First + Month Apr + Time 02.00 Hridald	
	Time & Date 2012-10-01 13:01:29		

Fig. 5 Manual Time Settings

Clock Source:	Select what clock source the switch will use for its time configuration. Use Local Settings allows you to manually set the time, or use NTP Server to allow the switch to sync it's time with an external NTP time server.
Local Time:	Displays the current time when using NTP Server, or is used to set the time when using Local Settings.
Time Zone Offset:	Provide the time zone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes. E.g. +10 will be 600 minutes.
Daylight Savings:	Daylight saving is adopted in some countries. If set, it will adjust the time by adding or removing time in unit of hours, according to the starting date and the ending date. For example, if you set the day light saving to be 1 hour. When the time passes over the starting time, the system time will be increased by one hour. When the time passes over the ending time, the system time will be decreased by one hour.
	If the Time Set Offset value is set to 0, no changes to the time will be made, nor will you have to set a start and end date. If you do add a valid value then you will need to configure your start and end dates for daylights savings in your particular area.
Time Set Offset:	Enter the Daylight Savings time offset for your region. The offset is given in minutes east of standard GMT. The valid range is 1 to 1440 minutes. Default is 60 minutes.
Daylight Savings Type:	Here you can select whether you want to set your daylight saving "By Dates" or by "Recurring". If you set "By Dates" this will need to be changed each year, if you select "Recurring" then this will only need to be setup once.
From:	Used to configure the Daylight Savings start date and time. Format is YYYY- MM-DD HH:MM.
То:	Used to configure the Daylight Savings end date and time. Format is YYYY- MM-DD HH:MM.

# 1.1.2-2 NTP

NTP (Network Time Protocol) is a protocol used to sync devices on the network with a time server.

## Web Interface

To configure the NTP Settings via the Web Interface:

- 1. Click System, Time and NTP.
- 2. Enter the required Server addresses in to the fields provided. Up to 5 NTP servers can be configured.
- 3. Click Save to apply your changes.

Aniedorce.com - Enterpro-	MAS-24T65FP 🐘 🙀 Australian Diskignt Sounces 🚺 👘	
⊢ → C 🗋 192.168.1.1		
ALLOY		
ALLOY		
AMS-24T6SFP		Auto-Logout
AMO-24 TOOFF		OFF .
System     System Information	NTP Configuration	
<ul> <li>Time</li> </ul>		
Manual	Server 1 au pool rep.org	
NTP	Server 2	
► Account	Server 3	
+ IP	Server 4	
Syslog SNMP	Server 5	
+ Contiguration	Server 0	
► Security	Apply Reset	
► Maintenance		

Fig. 6 NTP Time Settings

#### **Parameter Description**

Server 1 to 5: Enter a valid NTP Server IPv4 or IPv6 address, or enter the FQDN of a valid NTP Server.

# 1.1.3 Account

The Accounts function is used by the administrator to create, modify and delete users. The administrator can modify any guest user's settings including the privilege level and the guest user password. The guest user only has rights to modify their own password. Only one administrator account can be configured and up to four Guest accounts can be created.

# 1.1.3-1 Users

This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser

## Web Interface

To configure the User settings via the Web Interface:

- 1. Click System, Account and Users.
- 2. Click Add new User, you will now be prompted with a new interface.
- 3. Enter the required Username, Password and Privilege level.
- 4. Click Apply to save your settings.

Men: 18-50046,05-347.	KS-24T65FP 🔹 👘 Austine Persitivent Genoup Ber 👘 📋 Persitivet on Austre Services 🔹 📓 Wild Interpretient Enternal. 👘 👘	5.5 5
C 192.168.1.1		\$
Do you want Google Chrome to	to save your password? Save password Never for this site	
De pou sent Geogre Chome te Calascattospe Aussattospe System System System System Portoge Leve System Portoge Leve System S	Do tame your planse of Same planse of Users Configuration User Tame Privilege Level Materianse	And Logari Ter

Fig. 7 User Configuration

## **Parameter Description**

Add New User: Click the Add New User button to create a new user.

be you wint doope (home to law your plane) if see assumed there for the site	Alees 78-50046 (5-397		
	Do you want Google Chr	hrome to save your password? Save password Never for this site	
Perform     Add user       None     Add user       None     Perform       Stadger     Perform	AMS-24T6SFP		Auto Logost Cogost Heats
<ul> <li>Statuart</li> <li>Sta</li></ul>	* System	Addition	17.1 68
Uran     Uran taam       Propop Level     Pascord (spin)       > Bidly     Pholepa Level       > Bidly     Pholepa Level       Amoremance     Amoremance			
Project     Passendi       • Stadia     Passendi (spin)       • Stadia     • Passendi (spin)	* Account		
• stridg • s			
• BAA <sup>®</sup> Privilega Lacet         I         •           Security         Accept         Image         Image		Password (again)	
Acord Acord Concel	+ SNMP	Privilege Level 1	
	Configuration	Arris Bass Caural	
	* Maintenance	Carry (Carry) (Carry)	

Fig. 8 Adding a New User

User Name:	The name identifying the user, enter the username that you want to create.
Password:	Enter the required password. The password length can be between 0 and 255 characters.
Password (again):	Re-enter the password from the password field.
Privilege Level:	Used to assign the privilege level of the user being created. The allowed privilege range is from 1 through to 15. Level 15 is the highest level and will give you read/write access to the entire system. Each group can have a privilege level assigned. For a user to have access to that the group their privilege level must be equal or greater than the group value. By default every group is set to level 10 except the maintenance group which is set to 15. When creating users, guest users would be set to privilege level 5, standard users to 10 and administrators to 15. Guests will then have read only access to the system, standard users can do everything except maintenance tasks and the administrator will have full control of the switch.

# 1.1.3-2 Privilege Level

This page provides the administrator a way to give users access to the management interface of the switch. Privilege levels can be set for a variety of different switch functions. Each function is assigned to a group and a privilege level from 1 through to 15 can be assigned to each group.

#### Web Interface

To configure the Privilege Level settings via the Web Interface:

- 1. Click System, Account and Privilege Level.
- 2. Specify the privilege level for each of the groups.
- 3. Click Apply to save your changes.

C ] 1921681.1			
Do you want Google Chrome	to save your password?	e password Never for this site	
AMS-24T6SFP	Rife Thir Mart		Auto-Logout Essavol **01
System	-		
System Information	Privilege Leve	States - as the control of the	
<ul> <li>Time</li> <li>Account</li> </ul>	Group Name P		
Users	Account	10	
Privilege Lavel	Aggregation	10 -	
F IP F Syslog	Diagnostics	10 .	
+ SNMP	EEE	10 -	
Configuration	Easypot	10	
Security     Maintenance	GARP	10 -	
Asimienance	GVRP	10 -	
	p	10 -	
	IPMC Snooping	10 -	
	LACP	10 -	
	LLDP	10	
	LLOP MED	10 =	
	Loop Protect	10 -	
	MAC Table	10 -	
	MVR	10 -	
	Maintenance	15 -	
	Minorins	10 -	
	Pons	10 -	
	Printe VLANs	10 -	
		10 -	
	QoS		
	SFIDW	10 -	
	SMTP	10 -	
	SNMP	10 -	
	Security	10 .	
	Single IP	10	
	Spanning Tree	10	
	System	10 -	

Fig. 9 Setting the Privilege Levels

*Group Name:* The group name in which a privilege level can be assigned to.

Privilege Levels:The privilege levels can be set from 1 through to 15. Level 15 is the highest<br/>level and will give you read/write access to the entire system. Each group<br/>can have a privilege level assigned. For a user to have access to that the<br/>group their privilege level must be equal or greater than the group value. By<br/>default every group is set to level 10 except the maintenance group which is<br/>set to 15. When creating users, guest users would be set to privilege level 5,<br/>standard users to 10 and administrators to 15. Guests will then have read<br/>only access to the system, standard users can do everything except<br/>maintenance tasks and the administrator will have full control of the switch.

# 1.1.4 IP

IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network.

IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

# 1.1.4-1 IPv4

The AMS Series switches support both dynamically assigned and statically configured IP Addresses. If you are running a DHCP server on your network the switch can obtain an IP Address from the DHCP if DHCP Client is enabled. If not the switches IP settings must be configured manually. Please change the IP Address of the switch to suit your networks requirements.

#### Web Interface

To configure the IPv4 settings via the Web Interface:

- 1. Click System, IP and IPv4.
- 2. Select DHCP Client if you wish to obtain an IP Address automatically from a DHCP Server. Alternatively enter your required IP Settings for your network.
- 3. Click Save to apply your changes, or Reset to change values back to your previous settings.

C 192.168.1.1		
Do you want Google Chrome	to save your password? Save password Never for this site	
ALLOY AMS-24T6SFP	and the second second second second	Auto-Lopout
* System		
System Information	IP Configuration	
<ul> <li>Time</li> <li>Account</li> </ul>	Configured Current	
TIP	DHCP Client Ramm	
iPv4	IP Address 192.168.1.1 192.168.1.1	
IPv6	IP Mask 255 255 255 0 255 285 0	
Syslog SNMP	IP Gateway 192 160 1 254 192 166 1 254	
+ Configuration	VLANID 1 1	
<ul> <li>Security</li> </ul>	DNS Server 0000 0000	
<ul> <li>Maintenance</li> </ul>		
	IP DNS Proxy Configuration	
	DNS Proxy	
	and a second second	
	Apply Reset	

Fig. 10 IPv4 Address Configuration

DHCP Client:	Enable the DHCP Client by checking the tick box. When selected, the switch will obtain an IP Address from your DHCP Server. If the switch does not receive an IP Address the Default IP Address will be used.
Renew:	Click the Renew button to renew the DHCP lease from the DHCP Server.
IP Address:	Enter the required static IP Address in dotted decimal notation.
IP Mask:	Enter the required Subnet Mask in dotted decimal notation.
IP Router:	Enter the required Default Gateway in dotted decimal notation.
VLAN ID:	Provide the VLAN ID of the management interface. Valid range is from 1 to 4095.
DNS Proxy:	When DNS proxy is enabled, the switch will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network.

# 1.1.4-2 IPv6

The AMS Series switches support both dynamically assigned and statically configured IP Addresses. If you are running a DHCP server on your network the switch can obtain an IP Address from the DHCP if DHCP Client is enabled. If not the switches IP settings must be configured manually. Please change the IP Address of the switch to suit your networks requirements.

## Web Interface

To configure the IPv6 settings via the Web Interface:

- 1. Click System, IP and IPv6.
- 2. Select Auto Configuration if you wish to obtain an IP Address automatically from a DHCP Server. Alternatively enter your required IP Settings for your network.
- 3. Click Save to apply your changes, or Reset to change values back to your previous settings.

Hees FR-530340,075-347	WD-1416316 - Ver Au	Dis Products Unity 2n Production Au	alto Senters - 📲 Alla Integration: Emoré 🔊 👘	utital to
Do you want Google Chrome	e to save your password? San	ve password Never for this site		
AMS-24TESFP	Rest Rest		Hann daris inne	Auto-Logout Logout H4
System     System Information	IPv6 Configurat	tion		
+ Time	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Configured	Current	
+ Account	Auto Configuration		Renner	
T IP			1200000 C608 0101	
IPv4 IPv6	Address	c0a8.0101	LinkLocal Address (e30002 0200 8cf (e00 0012	
► Syslog	Prefix	96	96	
+ SNMP	Gateway			
Configuration				
<ul> <li>Security</li> </ul>	Apply Reset			
<ul> <li>Maintenance</li> </ul>				
- mannethance				

Fig. 11 IPv6 Address Configuration

#### Parameter Description

Auto Configuration: Enable the Auto Configuration by checking the tick box. When selected, the switch will obtain an IP Address from your DHCP Server. If the switch does not receive an IP Address the Default IP Address will be used.

Address:Enter the required static IPv6 address. An IPv6 address is a 128-bit record<br/>represented as eight fields of up to four hexadecimal digits with a colon<br/>separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol<br/>'::' is a special syntax that can be used as a shorthand way of representing<br/>multiple 16-bit groups of contiguous zeros; but it can only appear once. It<br/>can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

*Prefix:* Enter the IPv6 Prefix of this switch. The allowed range is 1 to 128.

*Gateway:* Enter the required IPv6 Gateway Address.

# 1.1.5 Syslog

The AMS Series Switches support offloading system messages to a Syslog Server. A Syslog is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It is supported by a wide variety of devices and receivers across multiple platforms.

# 1.1.5-1 Configuration

This section is used to configure the parameters of the Syslog server the switch will use to offload its system messages.

## Web Interface

To configure the Syslog settings via the Web Interface:

- 1. Click System, Syslog and Configuration.
- 2. Enter the Syslog parameters into the spaces provides and select the logging level.
- 3. Click Apply to save your changes.

Notes FR-SIDING JRS-247.	MS-24165FP 💦 🙀 Audeo Products Group Bri 👘 Production Audo Services 📲 Kill Integration, Extra A		$= 3_{1}$ $_{B}$
C 🖸 192.168.1.1			
AMS-24T6SFP		AttoLogout	Logout Help
System System Information	System Log Configuration		
Time Account	Server Mode Disabled -		
+ IP	Server Address 1		
* Syslog Configuration	Server Address 2 Syslag Level Into *		
Log Detailed Log	Apply Resol		
► SNMP Configuration			
Security			
Maintenance			
	1		

Fig. 12 Syslog Configuration

Server Mode:	Select enable from the dropdown box to enable the Syslog function.
Server Address 1:	Enter the IP Address of the Syslog Server.
Server Address 2:	Enter the IP Address of a second Syslog Server if required.

*Syslog Level:* Indicates what messages will be sent to the Syslog server.

# 1.1.5-2 Log

This section display's the system logging locally on the switch.

#### Web Interface

To view the System Logs via the Web Interface:

1. Click System, Syslog and Logs.

11.01		<u>\$</u>
TTOA		
4T6SFP		Auto-Logout Lapout Hele
n		
tem Information	System Log Information	Auto-refresh 🖾 Ratesh Clear 🦗 🦇 🤐
ount	Level All +	
og	The total number of entries is 11 for the given level.	
Mguration	Start from ID 1 with 20 entries per page	
	ID Level Time Message	
alled Log	1 Warming 2012-09-28 08 28:05 Switch just made a warm boot	
uration	2 Wiaming 2012-09-28 08 28 09 Link up on port 1 3 Info 2012-09-28 08 28 11 Login passed for user 'admin'	
ity enance	4 Info 2012-09-28 08 32 47 User admini logout	
	5 Info 2012-09-28 08 32-48 Login passed for user admin 5 Info 2012-09-28 08 43.05 User admin' logitit	
	7 Info 2012-09-20 16:10:10 Login passed for user admin 8 Info 2012-09-20 16:20:18 User admin' logout	
	9 Info 2012-10-01 08/21.17 Login passed for user admin	
	10 Info 2012-10-01 10:15-44 Login passed for user admin 11 Info 2012-10-01 10:15-44 Login passed for user admin	

Fig. 13 System Logs

Auto-refresh:	Select the Auto-refresh check box to enable the auto-refresh function. This enables the screen to refresh automatically.
Level:	Select the level of logging to be displayed on the screen. Options are All, Emergency, Alert, Critical, Error, Warning, Notice, Info and Debug.
ID:	Click on the ID to view additional information on the event.
Time:	Displays the time the event was logged by the system.
Message:	Displays detailed message of the event that has occurred.
Refresh:	Used to manually refresh the page.
Clear:	Used to clear the log.
Page Arrows:	Used to navigate between pages.

# 1.1.5-3 Detailed Log

This section is used to display events ID's in more detail.

## Web Interface

To view the Detailed System Logs via the Web Interface:

- 1. Click System, Syslog and Detailed Logs.
- 2. Enter the Event ID into the ID filed to display the event in more detail.

eter: FR-S1024G, GS-24T.	AM5-24T65FP 💿 m Audio Producty Group Rev. 👔 Perduction Audio Services 🖉 RGR Integration. Services 5	
C 192.168.1.1		÷
ALLOY		
		in the second
S-24T6SFP		Auto-Logout Logout He
em	Detailed System Log Information	Retesh jcc cc >> >>
tem information		(MARRIN) [ACC] [ACC] [AND]
ount	ID 1	
slog	Message	
9		
tailed Log	Level Wlammeg Time 2012/07/82800.28.05 Mossage Surston juster mode a wazm booc	
guration	Mazzale garzon Togo wang a karm proce	
enance		

Fig. 13 Detailed System logs

ID:	Enter the Event ID of the log event you want to view in detail.
Message:	Displays the detailed message of the log event.
Refresh:	Used to manually refresh the page.
Page Arrows:	Used to navigate between pages.

# 1.1.6 SNMP

The AMS Series Switches support SNMP and can be managed by any Network Management System (NMS). SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. A SNMP agent is running on the switch and if enabled will respond to the requests issued by a SNMP manager.

# 1.1.6-1 System

This section is used to enable or disable the SNMP Agent in the switch.

#### Web Interface

To enable or disable SNMP via the Web Interface:

- 1. Click System, SNMP and System.
- 2. Select to enable or disable the SNMP function by selecting the relevant radio button.
- 3. Enter a valid engine ID. This is used for SNMPv3 and should not need to be changed.
- 4. Click the Apply button to save your changes.

Aussing Palmin Diversity	MAS-3478999 💿 🧑 Austic Produces Group Ba- 👘 Sections Austic Devices 🚽 🎆 BCB Integration, Enternál 👘 💆 Desider - Colonidore Fred Fr. 🔪		- 31 - V
← C D 192,168,1.1			(1)
AMS-24T5SFP		Auto-Logout	Logaut Hela
		1001 181	
System     System Information	SNMP System Configuration		
+ Time	SMMP State 9 Enable Cleable		
Account	Engine ID Scott 45 contactor 78 aloco		
► IP ► Syslog			
Y SNATP	(5450)		
System			
Configuration			
Users			
Groups			
Views Access			
Trap			
<ul> <li>Configuration</li> </ul>			
<ul> <li>Security</li> <li>Maintenance</li> </ul>			
► Maintenance			



#### **Parameter Description**

*SNMP State:* Used to enable or disable the SNMP Agent in the switch.

*Engine ID:* SNMPv3 Engine ID. Syntax: 0 – 9, a – f, A – F. Minimum 5 Octet, Maximum 32 Octet.

# 1.1.6-2 Configuration

This section is used to configure the GET and SET community names. In this section you can also enable or disable the SET community. By doing this the NMS server will not be able to write configuration parameters to the switch.

#### Web Interface

To configure the GET and SET communities names via the Web Interface:

- 1. Click System, SNMP and Configuration.
- 2. Enter the GET and SET community names.
- 3. Select whether you want to enable or disable the SET function, via the drop down box.
- 4. Click the Apply button to save your changes.

Archine Painer Diverses	ANG-UT165PV V ver Austin Products Group IIm Products Avialia servicem 📓 Rulls integration, pittern A. 🔚 Results - Quilianiver Pro II		
← → C © 192.168.1.1			
AMS-24T6SFP		Auto-Logout	Logout Hein
* System	SNMP Configuration		
System Information			
Time Account	Get Community public		
* IP	Set Community private Enable -		
► Syslog ▼ SNMP			
System	Apply		
Configuration			
Communities			
Groups			
Views Access			
Trap			
► Configuration			
<ul> <li>Security</li> <li>Maintenance</li> </ul>			
	- K		

Fig. 15 SNMP Community Configuration

- Get Community:Set the community name for the SNMP Get function.Set Community:Set the community name for the SNMP Set function.
- *Enable/Disable:* Used to Enable or Disable the SNMP Set function.

# 1.1.6-3 Communities

This section is used to configure additional communities. These communities can be used to secure the SNMP information by allowing only certain users and IP Addresses to be able to access a specific community. The maximum number of communities that can be created is four.

#### Web Interface

To configure communities via the Web Interface:

- 1. Click System, SNMP and Communities.
- 2. Click add new community.
- 3. Enter a valid community name, a username, Source IP Address and subnet mask.
- 4. Click Save to apply your changes.



Fig. 16 SNMP Additional Community Configuration

#### **Parameter Description**

*Delete:* Select the tick box and click the apply button to delete a community name.

Add New Community: Used to add a new community.

	-			_				
24T6SFP	ALOP Martin Martin		<del>11111</del> 111				Auto-Logout	Legaul
em stem information ne count	Delete	Communities to Sec Community	urity Configuration User Name	Scott	Source IP 192, 168, 3, 2	Source Mask 255 255 255.0		
slog MP onfiguration ommunities sers sers sers coups ems coups ems sers iguration rity	Add new community	Austy			0000	0000		
tenance								

Fig. 17 SNMP Add New Community window

Delete:	Select the delete button next to the community you would like to delete.
Community:	Enter a valid community name. Valid length is from 1 to 32. The community string will be treated as a security name and map a SNMPc1 or SNMPv2c community string.
Username:	The Username string is used to permit access to the SNMP agent. The length of the Username can be from 1 to 32 characters.
Source IP:	Indicates what IP Addresses are able to communicate with the SNMP agent. The subnet mask can be used to allow access to entire subnets or individual IP Addresses.
Source Mask:	Enter the required subnet mask based on the source IP Address.

# 1.1.6-4 Users

SNMPv3 brings some important and much needed authentication and encryption options to the SNMP protocol. This section is used to configure SNMPv3 users.

#### Web Interface

To configure SNMP Users via the Web Interface:

- 1. Click System, SNMP and Users.
- 2. Click on Add New User to configure a new user. Enter the required user details.
- 3. Click Save to apply your changes.

Aussiet Patrier Diversity	185-24165PP 🔹 🖉 Austa Products Group for 👘 👔 Production Justic Services 🤉 🎆 Rick Integration Entrancia 🖉 Baseda - Quinciper Pre Fr. 🛛 💥 Simple Netword Manager		- F
C 192.168,1.1			台
ALLOY			
AMS-24T6SFP		Auto-Logout	Logaut Treis
System + System Information	SNMPv3 Users Configuration		
<ul> <li>System information</li> <li>Time</li> </ul>			
Account     IP	Delete User Security Authentication Authentication Privacy Privacy Name Level Protocol Password Protocol Password		
Syslog	Add menu use: Apply		
SNMP	Cardinate Card		
System Configuration			
Communities			
Users			
Groups Views			
Access			
Тгар			
Configuration lecurity			
Vaintenance			

Fig. 18 SNMPv3 Users

#### **Parameter Description**

*Delete:* Select the tick box and click the apply button to delete a User.

Add New User: Used to add a new user.
	-6SEP	Auto Product			-					
C 🗋 192.168.1.1										
ALLOY	Common State	_								
ALLOY	HUDS 	. <u> </u>	10000 00		ALCOHOF -					
S-24T6SFP		- Ka Kaka	ARALICA		and the owner where the					
5-24 103PP									Auto-Logout	Logaut Help
									Contra Della	
item system information	SNMPv3 Us	ers Confic	nuration							
ime					Authentication	-				
ccount	Delete	User Name	Security	Protocol	Password	Privacy Protocol	Privacy Password			
vslog	Delete		Auth, Priv	MD5 +		DES .				
NMP										
ystem	Add new user	Apply.								
Configuration Communities										
Isers										
iroups										
/iows										
Access										
figuration										
urity										
intenance										

Fig. 19 adding a new SNMPv3 User

Delete:	Select the delete button next to the community you would like to delete.
Username:	Enter a username to identify the user. Allowed length is 1 to 32 characters.
Security Level:	Indicates the security model set for the user. Possible security options: <b>NoAuth, NoPriv:</b> No Authentication and No Privacy <b>Auth, NoPriv:</b> Authentication and No Privacy <b>Auth, Priv:</b> Authentication and Privacy once the security level for a user has been set it cannot be changed. If you need to modify the security level you will need to delete and re-create the user.
Authentication Protoco	<ul> <li>Indicates the Authentication protocol used for the user. Options are:</li> <li>None: No Authentication Protocol</li> <li>MD5: Select to use the MD5 Authentication Protocol</li> <li>SHA: Select to use the SHA Authentication Protocol</li> <li>Once the Authentication Protocol has been set for a user it cannot be changed. If you need to modify the Authentication Protocol you will need to delete and re-create the user.</li> </ul>
Authentication Passwor	rd: The password used for both the MD5 and SHA Authentication Protocols. The MD5 protocol allows a password length of 8 to 32 characters and the SHA protocol allows a password length of 8 to 40 characters.
Privacy Protocol:	Indicates the Privacy protocol used for the user. Options are: None: No privacy protocol used.

**DES:** Select to use the DES encryption method once the Privacy Protocol has been set for a user it cannot be changed. If you need to modify the Privacy Protocol you will need to delete and recreate the user.

*Privacy Password:* The password used for both the DES Privacy Protocol. The allowed password length is 8 to 32 characters.

### 1.1.6-5 Groups

This section is used to configure SNMPv3 groups.

#### Web Interface

To configure SNMP Groups via the Web Interface:

- 1. Click System, SNMP and Groups.
- 2. Click on Add New Group to configure a new Group. Enter the required group details.
- 3. Click Save to apply your changes.

Account Patrier Diversify	MS-2476599 🐘 Rudon Predicate Group Br. 👘 Preduction Justice Services 📲 Roll Integrations, Entern A. 🗖 Parate - Quintine Pre Fr. 🛛 🕱 Viewers Minner Pre Fr.		
• • C 🗋 192.168.1.1			☆
ALLOY	ANY DESCRIPTION OF THE REAL PROPERTY AND ADDRESS OF THE REAL PROPERTY AND ADDRESS OF THE REAL PROPERTY AND ADDRESS OF THE REAL PROPERTY ADDRESS OF THE REAL PROPE		
AMS-24T6SFP		Auto-Logout	Logaut Help
		OFF .	Cogoor Hole
System	SNMPv3 Groups Configuration		
System information     Time			
+ Account	Delete Security Model Security Name Group Name		
> IP > Syslog	Add new group Apply		
Y SNMP			
System			
Configuration			
Users			
Groups Views			
Access			
Trap Configuration			
Security			
Maintenance			

Fig. 12 SNMPv3 Group

#### **Parameter Description**

*Delete:* Select the tick box and click the apply button to delete a Group.

Add New Group: Used to add a new group.

192.168.1.1			📕 Rill Integration: Taran A 👘 🤷 Results - Quilssiv	W second s	
LOY	Martine C. C.		unter and a second s		Auto-Logout
	SNMPv3 Groups Confi	Gauration			
Information	Delete Security Model	Security Name	Group Name		
e.	Delete Security Model		Group Name		
aration unities s stion nce	(Add man group) (Add by)				

Fig. 13 Add a new SNMPv3 Group

Delete:	Select the delete button next to the group you would like to delete.
Security Model:	Select the required security model that the group will belong to. Options are: v1: Reserved for SNMPv1 and will be available once a SNMPv1 community has been created in the communities section. v2c: Reserved for SNMPv2c and will be available once a SNMPv2c community has been created in the communities section USM: Reserved for User-based Security and will be available once a user has been created in the Users section.
Security Name:	The security name can be selected from any of the SNMP communities that you have created under the communities section.
Group Name:	Enter a group name to identify the group you are creating. Allowed length of 1 to 32 characters.

### 1.1.6-6 Views

This section is used to configure SNMPv3 views.

#### Web Interface

To configure SNMP Views via the Web Interface:

- 1. Click System, SNMP and Views.
- 2. Click on Add New View to configure a new View. Enter the required view details.
- 3. Click Save to apply your changes.

	Account: Palmer Diversit		S Audio: Producty Group Fro	Parduction Audio Services	Risk Integration: Taran A	an - Qalainer Pro Franc	🖉 Penúlts - Daksilver Fra Fr	🔠 somp old - Google Search	How do SNMP, Mills and	
Add-logoid on a contraction formation formatio	← · · C 🗋 192.168.1	1								(김 프
More Information     More Security     Provide		<b>HAR</b> This Part	<b></b>		n denir nimin				Auto-Logout	Legout Help
	An and a second	-							OFF .	
Mon     Account     Accou	<ul> <li>System</li> <li>System informatio</li> </ul>	SNMP	v3 Views Configuration							
• Product     Add Amar andmail     Address       • Partong		Delete	View Name View Type O	D Subtree						
• Bylog • Sales Sales Comparison Communities Ueers Ueers 10° cys 10° cys 10	► IP	Add.net	e view Apply							
9sten Configuration Comparison Groups Vens Acces Portgrayment	► Syslog ▼ SNMP									
Communities Univers Groups Views Access Trap * Configuration *	System									
Groups Vens Access Trap ▶ Centifyuration ▶ Security	Communities									
Access Trap * Centinguration * Sentinguration * Sentinguration										
Top  Conspuration  Security  Securit										
+ Security	Trap									
Mantenare	Configuration     Security									
	► Maintenance									

Fig. 14 SNMPv3 View

#### **Parameter Description**

*Delete:* Select the tick box and click the apply button to delete a View.

Add New View: Used to add a new view.

Account Patrier Diversify AM	-24T6SFP	udio Products Group Br	] Production Justic Services 👘 🧧	PSB Integration: Extran Ac	Line - Qualitions Pro Fran	Resulty - Quistoliner Pro Fr.	III merg col-Gropie Sewahi	How do SNMP, Mills and	- 8. v
→ C □ 192.168.1.1									1
ALLOY				ALL DECK					
ALLOY	ALC: The Martin		HOCIDO dada da	in since a					
AMS-24T6SFP			and the second second second second	and a second				Auto-Logout	
								OFF .	Logaul Help
System	1	and and and							
<ul> <li>System information</li> </ul>	and the second second	s Configuration							
Time     Account	Delete View Na		OID Subtree						
+ IP	Delete	included ·		1					
Syslog SNMP	Add new view	Apply							
System									
Configuration Communities									
Users									
Groups									
Views Access									
Trap									
Configuration Security									
Maintenance									

Fig. 15 Add a new SNMPv3 View

Delete:	Select the delete button next to the view you would like to delete.
View Name:	Enter a view name to identify the view you are creating. Allowed length of 1 to 32 characters.
View Type:	Select the view type from the options below: Included: Used to allow a particular OID subtree to be displayed in the view. Excluded: Used to block a particular OID subtree from being displayed. If you exclude an OID from a view you can allow other OID's to view by adding include views.
OID Subtree:	The OID defining the root of the subtree. The allowed OID length is from 1 to 128. Wildcards (*) can also be used in the OID subtree.

### 1.1.6-7 Access

This section is used to configure SNMPv3 access lists.

#### Web Interface

To configure SNMP Access lists via the Web Interface:

- 1. Click System, SNMP and Access.
- 2. Click Add new Access.
- 3. Specify the SNMP Access parameters.
- 4. Click Save to apply your changes.



Fig. 16 SNMPv3 Access

#### Parameter Description

*Delete:* Select the tick box and click the apply button to delete an Access rule.

Add New Access: Used to add a new Access rule.

C 3 192.168.1.1	45-311629 x 🐂 kada Postata Grag Fas i 🖕 Pestatara kada Sanaya 🦷 🗱 Kili Seteparan Jima A 📲 Lan- Galakar Pas Fas 🦷 💶		1-10 女
ALLOY AMS-24T6SFP		Auto-Logout	Legaul Hel
System > System information	SNMPv3 Accesses Configuration		
<ul> <li>Time</li> <li>Account</li> </ul>	Delete Group Name Security Model Security Level Read View Name Write View Name		
Provide Control of Control o	Address access (App)		

Fig. 17 Add a new SNMPv3 Access Rule

Delete:	Select the delete button next to the Access Rule you would like to delete.
Group Name:	Select the Group name from the drop down box. Please ensure you have created a group from the Group section. (See section 1.1.6-5)
Security Model:	<ul> <li>Select the required security model that the group will belong to. Options are:</li> <li>v1: Reserved for SNMPv1 and will be available once a SNMPv1 community has been created in the communities section.</li> <li>v2c: Reserved for SNMPv2c and will be available once a SNMPv2c community has been created in the communities section.</li> <li>USM: Reserved for User-based Security and will be available once a user has been created in the Users section.</li> </ul>
Security Level:	<ul> <li>Indicates the security model set for the user. Possible security options:</li> <li>NoAuth, NoPriv: No Authentication and No Privacy</li> <li>Auth, NoPriv: Authentication and No Privacy</li> <li>Auth, Priv: Authentication and Privacy</li> <li>once the security level for a user has been set it cannot be changed. If you need to modify the security level you will need to delete and re-create the user.</li> </ul>
Read View Name:	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32.

*Write View Name:* The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32.

### 1.1.6-8 Trap

This section is used to create SNMP traps.

#### Web Interface

To configure SNMP Traps via the Web Interface:

- 1. Click System, SNMP and Trap.
- 2. Select an SNMP Trap number and click the number to add the trap information. Up to 6 traps can be configured.
- 3. If you have any Trap entries that you would like to delete, click on the delete button next to the Trap that you would like to delete.
- 4. Click the Save button to apply changes.

count Patres Divenifi	MS-2016SFP 🔹 🖉 Audes Products Group Br 👘 Production Jude Services 🖉 RGB Integration, Extern J 🖉 Readts - Oxforinge Pro Fr 👘 🔝	- 8
C 192.168.1.1		<b>会</b>
MS-24T6SFP		Auto-Logout Logated Theor
System information	Trap Hosts Configuration	
Account     BP     Syslog     Syslog     System     Configuration     Communities	Detects to Version Series IP UDP Prot Community/Series/ Idams Series/ Society Automaticates Thicky east Lawel Perticute 8 8 8 8 8 8 8 8 8 8 8 8 8	
Users Groups Views Access Trap	(Acety)	
Configuration Security Maintenance		

Fig. 18 SNMP Traps

#### **Parameter Description**

*Delete:* Click the delete button to delete an existing Trap.

*No:* This identifies the Trap number, click on the Trap number to create a new SNMP Trap. Up to 6 Traps can be created.

ALLOT/	-			4
ALLOY		COC COCCESSION and the same		
MS-24T6SFP			Auto-Logout	
			OFF .	Logaul Help
System				
System information	Trap Host Configuration			
Time Account	Trap Version	2c •		
P	ServerIP			
golays	UDP Port	62		
INMP	Community/Security Name			
System Configuration		do (*)		
Communities		InAuth NoPrix +		
Users		ADS =		
Groups	Authentication Password			
Views Access		IES +		
Trap	Privacy Password			
figuration	Privacy Paramona			
surity	Apply Reset			
aintenance				

Fig. 19 Add a new SNMP Trap

Trap Version:	Select the required Trap Version SNMP v1, v2c or v3 trap.
Server IP:	Enter the IP Address of the server that will receive the SNMP Traps.
UDP Port:	Enter the UDP port used for sending the SNMP Traps, default is 162.
Community/Security:	Enter the Community/Security name, this value can be 1 to 32 characters in length.
Security Level:	Select the type of information you want sent in the SNMP Trap. Options are Emergency, Alert, Critical, Error, Warning, Notice, Info and Debug.
Security Level:	Set the required security level. Possible security options: NoAuth, NoPriv: No Authentication and No Privacy Auth, NoPriv: Authentication and No Privacy Auth, Priv: Authentication and Privacy
Authentication Protoco	<ul> <li>Indicates the Authentication protocol used for the Trap. Options are:</li> <li>MD5: Select to use the MD5 Authentication Protocol</li> <li>SHA: Select to use the SHA Authentication Protocol</li> </ul>
Authentication Passwo	<i>rd:</i> The password used for both the MD5 and SHA Authentication Protocols. The MD5 protocol allows a password length of 8 to 32 characters and the SHA protocol allows a password length of 8 to 40 characters.
Privacy Protocol:	Indicates the Privacy protocol used for the user. Options are: <b>DES:</b> Select to use the DES encryption method

*Privacy Password:* The password used for both the DES Privacy Protocol. The allowed password length is 8 to 32 characters.

# **1.2 Configuration**

This chapter describes the network configuration options available in the AMS Series of switches. All Layer 2 features such as VLAN's, Port Trunking, IGMP, ACL's and QoS can be configured in this section.

## 1.2.1 Port

The Port section is used to configure specific port parameters and view statistics related to individual ports.

## 1.2.1-1 Configuration

Use this section to configure parameters for each of the ports. You can force the speed of a port, set the maximum frame size, set frame collision parameters and also configure the power saving options for each of the ports.

### Web Interface

To configure the ports of the switch via the Web Interface:

- 1. Click Configuration, Port and Configuration.
- 2. Configure the parameters needed for your network.
- 3. Click the Apply button to save your changes or the Reset button to revert to previous settings.

← C [] 192.168.1.1								_			
AMS-24T6SFP			Tr,	. 6666					Auto-Logout	Logod	it H
System Configuration	Port	Cont	iguration	1						Refre	sh
* Port	-	_		Speed		Flow Control		Maximum	Excessive	Power	
Configuration Port Description	Port	Link	Current	Configured	Current Rx	Current Tx	Configured	Frame Size	Collision Mode	Control	
Traffic Overview				0				10 ····	0 -	0.	8
Detailed Statistics	1		1Głdx	Auto	x	х		9600	Discard 💌	Disabled 💌	0
QoS Statistics	2		Down	Auto	x	×		9600	Discard -	Disabled -	ü -
SFP Information	3	ě	Down	Auto		×		9600	Discard -	Disabled -	ñ .
EEE ACL	4		Down	Auto		x	n	9600	Discard -	Disabled .	51
► Aggregation	5		Down	Auto		x		9600	Discard -	Disabled •	
Spanning Tree					ad the second second		E				
► IGMP Snooping	6	•	Down	Auto		×		9600	Discard -	Disabled -	
MLD Snooping	7	•	Down	Auto		×		9600	Discard 💌	Disabled -	
MVR LLDP	8		Down	Auto	· ×	×		9600	Discard -	Disabled 💌	
Filtering Data Base	9		Down	Auto	×	×		9600	Discard -	Disabled .	6
+ VLAN	10.		Down	Auto	×	x	D.	9600	Discard *	Disabled .	8
Voice VLAN	11		Down	Auto	×	x		9600	Discard -	Disabled .	ë -
F GARP	12		Down	Auto	×	×		9600	Discard -	Disabled -	i -
> QoS	13		Down	land the second s	i x	×	17	9600	Discard -	Disabled -	
Thermal Protection	14		Down		x	x		9600	Discard •	Disabled •	A. ( )
sFlow Agent						x		9600	Discard •	and a second second	
<ul> <li>Loop Protection</li> <li>Single IP</li> </ul>	15		Down	-							4.11
Easy Port	16		Down	Auto	-	×		9600	Discard 💌	Disabled -	
Mirroring	17	•	Down	Auto	-	×		9600	Discard -	Disabled .	- C
Trap Event Seventy	18		Down	Auto	· ×	×		9600	Discard -	Disabled .	
SMTP Configuration	19		Down	Auto	×	×		9600	Discard -	Disabled .	6
UPnP Security	20		Down	Auto	×	×		9600	Discard -	Disabled .	6
Maintenance	21		Down	SFP_Auto_AMS	x	x	1	9600	Discard *	Disabled .	
	22		Down	SFP Auto AMS	x	x	ñ	9600	Discard -	Disabled .	1
	23		Down	SFP Auto AMS		x		9600	Discard •	Disabled .	
	2.5	-	Down	SFP Auto AMS	-	÷		9600	Discard •		

Fig. 20 Port Configuration

Port:	The logical port number for the switch.
Link:	The current link state of the port is shown. Green indicates link is active, Red indicates the link is down.
Speed-Current:	Displays the current port link speed.
Speed-Configured:	Here you can force the speed of a port. Forcing the speed of a port is not recommended and should only be done if you are having linking issues when connecting to a particular device. Speed options available are: <b>10Gb FDX</b> – 10GbE Full Duplex (AMS-24T4S4SFP and AMS-48T4S4SFP only) <b>1Gb FDX</b> – 10GbE Full Duplex (AMS-24T4S4SFP and AMS-48T4S4SFP only) <b>1Gb FDX</b> – 1GB Full Duplex <b>100Mbps FDX</b> – 100Mbps Full Duplex <b>100Mbps HDX</b> – 100Mbps Half Duplex <b>10Mbps HDX</b> – 10Mbps Full Duplex <b>10Mbps HDX</b> – 10Mbps Half Duplex <b>10Mbps HDX</b> – 10Mbps Half Duplex <b>Auto</b> – Auto Negotiation <b>10G-X_AMS</b> – 10Gbps (AMS-24T4S4SFP and 48T4S4SFP SFP+ ports only) <b>100FX_AMS</b> – 100Mbps (Paired UTP/SFP Ports Only) <b>1000-X_AMS</b> – 100Mbps Full Duplex(SFP Ports Only) <b>100Mbps FDX</b> – 100Mbps Full Duplex(SFP Ports Only) <b>1Gbps FDX</b> – 100Mbps Full Duplex(SFP Ports Only)
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. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.
Maximum Frame Size:	Enter the maximum frame size allowed for each switch port. Valid ranges are from 1518 to 9600 bytes.
Excessive Collision Mod	de: Used to set the ports response to excessive collisions on the port. Discard: Discard frames after 16 collisions (Default) Restart: Restart backoff algorithm after 16 collisions
Power Control:	Used to configure the power savings features of each port. <b>Disabled:</b> All power saving mechanisms are disabled

**ActiPHY:** Link down power savings enabled. Power saving occurs if no active link.

**PerfectReach:** Link up power savings enabled. Reduced power used by the port depending on the length of the cable.

**Enabled:** Both Link up and Link Down power saving mechanisms enabled.



NOTE:

At the top of the column there is an \*. The \* is a global setting and a way of changing the settings for every port simultaneously.

### **1.2.1-2 Port Description**

Use this section to help identify what devices are connected to each port of your switch. Each Port can have a description assigned to it.

#### Web Interface

To add a description to the ports of the switch via the Web Interface:

- 1. Click Configuration, Port and Description.
- 2. Enter the description for the required ports.
- 3. Click Apply to save changes or Reset to return to previous values.

C 192.168.1.1	-				¢
AMS-24T6SFP	ALC'		<b>HAR IN IN IN 19</b>	Auto-Logout	Logout Hel
System Configuration	Port Descri	ption			
* Port	Port	Description			
Configuration	1	Description			
Port Description	2				
Traffic Overview Detailed Statistics	1 ALM 1				
QoS Statistics	3				
SFP Information	4				
EEE	5				
ACL	6				
Aggregation	7				
Spanning Tree     IGMP Snooping	the second second				
MLD Snooping	8				
- MVR	9				
LLDP	10				
Filtering Data Base	-11				
VLAN	12	1			
Voice VLAN	13				
GVRP	14				
QoS	and the second s				
Thermal Protection	15				
SFlow Agent	16				
Loop Protection	17				
Single IP     Easy Port	18				
Mirroring	19	1			
Trap Event Sevenity	20				
SMTP Configuration	21				
UPnP	and the second second				
Security	22				
anne ance	. 23				
	24				
	25	1			

Fig. 21 Port Descriptions

#### **Parameter Description**

*Port:* The logical port number for the switch.

Description:Enter a description of each of the ports. Descriptions cannot include ", #, %,<br/> $\&, `, +, \setminus$ 

### 1.2.1-3 Traffic Overview

Use this section to view basic traffic statistics for each of the switch ports.

#### Web Interface

To view the port statistics via the Web Interface:

- 1. Click Configuration, Port and Traffic Overview.
- 2. Click on an individual port number to show the detailed statistics for that port.
- 3. If you would like the page to auto-refresh the port statistics, check the Auto-Refresh tick box at the top of the page, or alternatively hit the refresh button to refresh the page manually.
- 4. To clear the current statistics, use the Clear button at the top of the page.

- C 🗋 192.168.1.1	_	_		_		_	_	_		\$
ALLOY AMS-24 T6 SFP	ALCY Statement		<b>.</b>					Auto-	Logout	Logout H
System Configuration	Port	Statistics	Overview					A	uto-refresh 🗖 🖡	Refresh
* Port	1 Parts	Pa	ckets	B	ytes	E	rrors	D	rops	Filtered
Configuration	Port	Received	Transmitted		Transmitted	Received	Transmitted		Transmitted	Received
Port Description	1	5007882	569404	656563813	320146515	0	0	.0	0	2880492
Traffic Overview	2	0	0	0	0	0	0	0	0	0
Detailed Statistics	- 2	0	0	0	0	0	0	D	0	0
QoS Statistics	4	0	0	Q	0	0	0	U	0	U
SFP Information	2	0	0	0	0	0	0	0	0	0
EEE	5	0	0	0	0	0	0	0	0	0
ACL	4	0	0	0	0	0	0	0	0	0
Aggregation	e 9	ő	ő	ő	ő	ő	ő	ő	ő	ő
Spanning Tree	2 10	0	0	0	0	0	0	0	0	ū
IGMP Snooping	11	0	0	0	0	0	0	a	0	0
MLD Snooping	12 13 14 15 15 15	0	0	.0	0	0	0	U	0	0
MVR	13	0	0	0	0	0	0	0	0	0
LLDP	14	0	0	0	0	0	0	0	0	0
Filtering Data Base	15	0	0	0	0	0	0	0	0	0
VLAN	10	0	0	0	0	0	0	0	0	0
Voice VLAN	18	0	0	0	ő	ů.	0	ŭ	ő	Ő
GARP	18 19 20 21	0	0	0	0	0	0	0	0	0
	20	0	0	0	0	0	0	0	0	0
GVRP		0	Ó	0	0	0	0	Ű	0	Ó
QOS	22	0	0	0	Q	0	0	0	0	0
Thermal Protection	23	0	0	0	0	0	0	.0	0	.0
SFlow Agent	24	0	0	0	0	0	0	0	0	0
Loop Protection	25 26	0	0	0	0	0	0	0	0	0
Single IP     Easy Port	- 22	0	0		Ų	0	0	0	0	.0.

Fig. 22 Port Statistics

Click on the port number to view the detailed statistics.
The number of transmitted and received packets per port.
The number of transmitted and received Bytes per port.
The number of transmitted and received errors per port.
The number of frames discarded due to ingress or egress congestion.

The number of file to file to file to file the second by the switch.	Filtered:	The number of filtered frames	received by the switch.
--	-----------	-------------------------------	-------------------------

- Auto-Refresh: To enable auto-refreshing of the statistics on the screen, tick this tick box.
- *Refresh:* Used to manually refresh the statistics.
- *Clear:* Used to clear the current statistical data.

### **1.2.1-4 Detailed Statistics**

This sections displays in depth details of the traffic being transmitted and received by the switch. If you are having problems on your network, this page can be useful for diagnosing packet errors being received or transmitted by the switch.

#### Web Interface

To view the detailed port statistics via the Web Interface:

- 1. Click Configuration, Port and Detailed Statistics.
- 2. Select the Port you would like to view from the drop down box near the top of the page.
- 3. If you would like the page to auto-refresh the port statistics, check the Auto-Refresh tick box at the top of the page, or alternatively hit the refresh button to refresh the page manually.
- 4. To clear the current statistics, use the Clear button at the top of the page.

AMS-24T6SFP	And Personnel Statements		1000		
C I ISCLOULL					tu.
ALLOY	ALLON CONTRACTOR OF THE SECOND		-	107	
ALL DO					
AMS-24T6SFP				Auto-Logout	
				OFF I	ogout He
System	· · · · · · · · · · · · · · · · · · ·				
Configuration	Detailed Port Statistics Po	rt 1		Port 1 · Auto-refresh Refresh	Clear
* Port					
Configuration	Receive Tota		Tx Packets	Transmit Total 569923	
Port Description	Rx Packets Rx Octets	657343438		320473500	
Traffic Overview	Rx Unicast		Tx Unicast	569908	
Detailed Statistics	Rx Multicast		Tx Multicast	10	
QoS Statistics	Rx Broadcast		Tx Broadcast	5	
SEP Information	Rx Pause	0	Tx Pause	0	
	Receive Size Cou	inters	Tr	ansmit Size Counters	
EEE	Rx 64 Bytes		Tx 64 Bytes	23754	
► ACL	Rx 65-127 Bytes	2114843	Tx 65-127 Bytes	658	
<ul> <li>Aggregation</li> </ul>	Rx 128-255 Bytes		Tx 128-255 Bytes	102021	
Spanning Tree	Rx 256-511 Bytes		Tx 256-511 Bytes	222037	
IGMP snooping	Rx 512-1023 Bytes		Tx 512-1023 Bytes	60	
MLD Snooping	Rx 1024-1526 Bytes		Tx 1024-1526 Bytes	221393	
► MVR	Rx 1527- Bytes Receive Oueue Co		Tx 1527- Bytes	nsmit Queue Counters	
+ LLDP	Rx Q0	5013802		nsmit Quede Counters	
Filtering Data Base	Rx Q1		Tx Q1	0	
► VLAN	Rx Q2		Tx Q2	0	
Voice VLAN	Rx Q3		Tx Q3	0	
- GARP	Rx Q4		Tx Q4	0	
> GVRP	Rx Q5	0	Tx Q5	0	
	Rx Q6		Tx Q6	0	
► QoS	Rx Q7		Tx Q7	569923	
<ul> <li>Thermal Protection</li> </ul>	Receive Error Co			ansmit Error Counters	
sFlow Agent	Rx Drops		Tx Drops	0	
Loop Protection	Rx CRC/Alignment		Tx Late/Exc. Coll.	0	
► Single IP	Rx Undersize	0			
Easy Port	<ul> <li>Rx Oversize</li> </ul>	0			

Fig. 23 Detailed Port Statistics

Port:	Select the port you wish to view the statistics for from the drop down box at the top of the page.
Auto-Refresh:	To enable auto-refreshing of the statistics on the screen, tick this tick box.
Refresh:	Used to manually refresh the statistics.

*Clear:* Used to clear the current statistical data.

- Receive Total:The total number of received Rx traffic including good and bad packets.Types of traffic displayed are Rx Packets, Rx Octets, Rx Unicast, Rx Multicast,<br/>Rx Broadcast and Rx Pause packets.
- Transmit Total:The total number of transmitted Tx traffic including good and bad packets.Types of traffic displayed are Tx Packets, Tx Octets, Tx Unicast, Tx Multicast,<br/>Tx Broadcast and Tx Pause packets.
- Receive Size Counters: The total number of received packets categorised based on the size in Bytes of the packets received. Sizes displayed are Rx 64 Bytes, Rx 65-127 Bytes, Rx 128-255 Bytes, Rx 256-511 Bytes, Rx 512-1023 Bytes, Rx 1024-1526 Bytes and Rx 1527+ Bytes.
- *Transmit Size Counters:* The total number of transmitted packets categorised based on the size in Bytes of the packets transmitted. Sizes displayed are TX 64 Bytes, TX 65-127 Bytes, Tx 128-255 Bytes, Tx 256-511 Bytes, Tx 512-1023 Bytes, Tx 1024-1526 Bytes and Tx 1527+ Bytes.
- *Receive Queue Counters:* The total number of packets received by the port based upon the QoS Queues. Queues displayed are from RX Q0 through to RX Q7.

*Transmit Queue Counters:* The total number of packets transmitted by the port based upon the QoS Queues. Queues displayed are from Tx Q0 through to Tx Q7.

- Receive Error Counters: The total number of errors received by the port. Error types displayed are Rx Drops, Rx CRC/Alignment, Rx Undersize, Rx Oversize, Rx Fragments and Rx Jabber, Rx Filtered.
- *Transmit Error Counters:* The total number of errors transmitted by the port. Error types displayed are Tx Drops and Tx Late/Excessive Collisions.

### 1.2.1-5 QoS Statistics

This section displays the QoS Queuing details for each of the ports. By clicking on an individual port detailed statistic can be shown.

#### Web Interface

To view the detailed QoS statistics via the Web Interface:

- 1. Click Configuration, Port and QoS Statistics.
- 2. Click on an individual port number to show the detailed statistics for that port.
- 3. If you would like the page to auto-refresh the QoS statistics, check the Auto-Refresh tick box at the top of the page, or alternatively hit the refresh button to refresh the page manually.
- 4. To clear the current statistics, use the Clear button at the top of the page.

- C 🗋 192.168.1.1																			\$2
ALLOY		MART NAME			.8		É É	Ê	<b>HH</b>					140.311077	1				
AMS-24T6SFP				- 6	1 10.0				<u></u>					COLUMN TWO IS			uto-Logout	Log	gout Help
• System																			
Configuration	- mail	Queu	ing Co	unte	ers												Auto-refresh	Refresh	Clear
* Port		-	QU		0		Q2		Q3		04		25	Q6		97			
Configuration		Port	Rx	Tx	Rx	Tx		Tx	Rx T	R		Rx	Tx	Rx Tx	Rx	Tx			
Port Description		1	5821870	0	0	0	0	0	0		0 0	0	0	0 0		622519			
Traffic Overview		2	0	0	0	0	Ő	0	ő	0	0 0	0	0	0 0		0			
Detailed Statistics		3	0	0	0	0	Ó.	0	0	0	0 0	0	0	0 0	0	0			
QoS Statistics		4	0	0	0	.0	Q	0	0	0	0 0	0	0	0 0	0	0			
SFP Information		5	0	0	0	0	0	0	0	0	0 0	0	0	0 0	0	0			
EEE		6	0	0	0	0	0	0	0	0	0 0	0	0	0 0	0	0			
► AGL		8	0	0	0	0	0	0	0	0		0	0	0 0	0	0			
► Aggregation	=	2	0	0	0	0	0	0	0	n	0 0	0	0	0 0	0	0			
► Spanning Tree		10	Ő	õ	õ	Ő	õ	0	õ	0	0 0	ŏ	Ő	0 0	0	õ			
► IGMP Snooping		11	0	0	0	0	Ó	0	0	0	0 0	0	0	0 0	0	0			
► MLD Snooping		12	0	0	0	0	0	0	0	0	0 0	0	0	0 0	0	0			
► MVR		13	0	0	0	0	0	0	0	0	0 0	0	0	0 0	0	0			
+ LLDP		14 15	0	0	0	0	0	0	0	0	0 0	0	0	0 0	0	0			
Filtering Data Base		16	0	0	0	0	0	0	0	0	0 0	0	0	0 0	0	0			
+ VLAN		17	Ő	Ő	0	0	0	0	0	0	0 0	0	Ő	0 0	0	0			
► Voice VLAN		18	0	Ó	0	0	0	0	0	0	0 0	0	Ó	0 0	0	Ó.			
+ GARP		19	0	0	0	0	0	0	0	0	0 0	0	0	0 0	0	0			
P GVRP		20	0	0	0	0	0	0	0	0	0 0	0	0	0 0	0	0			
► Q05		21	0	0	0	0	0	0	0	0	0 0	0	0	0 0	0	0			
Thermal Protection		22 23	0	0	0	0	0	0	0	0	0 0	0	0	0 0	0	0			
► sFlow Agent		24	0	0	0	0	0	0	0	0	0 0	0	0	0 0	0	0			
Loop Protection		25	0	0	0	0	0	0	0	0	0 0	0	0	0 0	0	0			
<ul> <li>Single IP</li> </ul>		26	0	0	0	0	0	0	0	0	0 0	0	0	0 0	0	0			
Easy Port																			

Fig. 24 QoS Statistics

Port:	Click on the port number to view the detailed statistics.
Q0-Q7 RX/TX:	The number of transmitted and received packets for Q0 to Q7 per port.
Auto-Refresh:	To enable auto-refreshing of the statistics on the screen, tick this tick box.
Refresh:	Used to manually refresh the statistics.
Clear:	Used to clear the current statistical data.

### 1.2.1-6 SFP Information

This section displays the detailed information regarding the SFP module(s) installed in the switch.

#### Web Interface

To view the detailed SFP Information via the Web Interface:

- 1. Click Configuration, Port and SFP Information.
- 2. Select the port you want to view.
- 3. If you would like the page to auto-refresh the SFP Information, check the Auto-Refresh tick box at the top of the page, or alternatively hit the refresh button to refresh the page manually.

C 1921681.1	ALON		(annua)	2
AMS-24T6SFP		HELEC HELEC AND	Auto-Logout	Logout Help
• System	SFP Information for	Bort 21	[2+107]] (1+1)	fresh Refresh
Configuration	SFF Information for	FOILZI	Port 21 Auto-re	trean La Kettesh
* Port	Connector Type	SFP LC		
Configuration	Fiber Type	Reserved		
Port Description	Tx Central Wavelength	850		
Traffic Overview	Bit Rate	1000 Mbps		
Detailed Statistics	Vendor OUI	00-00-00		
QoS Statistics	Vendor Name	ALLOY		
SFP Information	Vendor P/N	MGBIC-MLC		
EEE	Vendor Revision	0000		
► ACL	Vendor Serial Number	C009F11000413		
Aggregation	Date Code	050211		
► Spanning Tree	Temperature	none		
► IGMP Snooping	Vcc	none		
► MLD Snooping	Mon1 (Bias)	none		
► MVR	Mon2 (TX PWR)	none		
► LLDP	Mon3 (RX PWR)	none		
► Filtering Data Base				
► VLAN				
► Voice VLAN				
- GARP				
- GVRP				
P 005				
Thermal Protection				
► sFlow Agent				
Loop Protection				
<ul> <li>Single IP</li> </ul>				

Fig. 25 SFP information

#### **Parameter Description**

*Connector Type:* Displays the connector type of the SFP module, normally this would be UTP, LC or SC.

*Fibre Type:* Displays the fibre type, multimode or single mode.

*Tx Central Wavelength:* Displays the optical fibre wavelength, normally 850nm, 1310nm or 1550nm.

*Baud Rate:* Displays the speed of the SFP module, 100Mbps, 1000Mbps, 10Gb.

*Vendor OUI:* OUI number of the vendors SFP Module.

Vendor Name:	Vendor's name of the SFP Module.
Vendor P/N:	The part number of the Vendors SFP module.
Vendor Revision:	The revision number of the Vendors SFP module.
Vendor Serial Number:	The serial number of the SFP module.
Date Code:	Date the SFP module was manufactured.
Temperature:	Shows the current temperature of the SFP module.
Vcc:	Shows the current DC voltage being used by the SFP module.
Mon1 (Bias):	Shows the Bias current of the SFP module in mA.
Mon2 (TX PWR):	Shows the transmit power of the SFP module.
Mon3 (RX PWR):	Shows the receive sensitivity of the SFP module.

AMS User Manual

### 1.2.1-7 EEE

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

EEE works by powering down circuits when there is no traffic. When a port has data to be transmitted all circuits are powered up. The time it takes to power up the circuits is called the wakeup time. The default wakeup time is 17  $\mu$ s for 1Gbit links and 30  $\mu$ s 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 devices have all circuits powered up when traffic is transmitted. Each device can exchange information about the devices individual wakeup time using the LLDP protocol.

For maximizing the power saving, the circuit isn't started as soon as data is ready for a port, but is instead queued until 3000 bytes of data is ready to be transmitted. To eliminate large delay's in cases where the data is less than 3000 bytes, data will always be transmitted after 48  $\mu$ s, giving a maximum latency of 48  $\mu$ s + the wakeup time.

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 only.

#### Web Interface

To configure the EEE Power Saving options via the Web Interface:

- 1. Click Configuration, Port and EEE.
- 2. To enable the EEE function for a port tick the box next to the corresponding port.
- 3. Select the desired EEE Urgent Queue values for each port.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.

- C 192.168.1.1			_			_		_	_			-		53
ALLOY	ALLON 24 Part Manager Digetel Boeten		- 1	6		÷	-	Ê	Ě	1 P		1		
AMS-24T6SFP		100			ų.	64	ι.	i i i i		9 M.			Auto-Logout	
AW3-24103FF													OFF -	Logout Help
► System														
▼ Configuration	EEE	Configuratio	ior	1										
▼ Port	1.000													
Configuration						= 1	Inc	-	+ 0		ues			
Port Description	Port	EEE Enabled			2			jen 4				8		
Traffic Overview	Fort *	ELE Ellabled			-	-						0	1	
Detailed Statistics	1						1 16							
QoS Statistics	2					-								
SFP Information	3			긝										
EEE										-				
► ACL	4					E	110							
Aggregation	.5					E	1/[	1				(E		
Spanning Tree	6													
► IGMP Snooping	7			١		E	1 6	3))		E	E	E	1	
MLD Snooping	8					E						E	1	
► MVR	9		I			E	16					E		
► LLDP	10					F					E	E	1	
Filtering Data Base	11		Ĩ			F	115			E	E	F		
► VLAN	12					F	1 6	-		E	F	F		
Voice VLAN	13					IF.	1.6			-		F		
► GARP	14					E					10			
► GVRP	14	P												
► QoS										-			1	
Thermal Protection	16									-				
sFlow Agent	17					L	U IL							
Loop Protection	18													
► Single IP	19					E	UE	10						
Easy Port	20		1			E	I E					E		
Mirroring	21					E	1/6					E	0	
Trap Event Severity	22					E						E	1	
SMTP Configuration UPnP	23		C			E	1 6				E	E		
Security	24		0			E	IE	11			E	E	1	
<ul> <li>Security</li> <li>Maintenance</li> </ul>				-						-		-		
Maintenance	Apply	Reset												



#### **Parameter Description**

*Port:* Physical port of the switch.

*EEE Enabled:* Used to enable or disable EEE for each port.

EEE Urgent Queues:Queues set will activate transmission of data as soon as it is available. If no<br/>queue is set then transmission of data will only occur once 3000 bytes are<br/>ready to be transmitted. Queues 1 to 8 are mapped to QoS Queues 0 to 7.<br/>E.g. EEE Urgent Queue 1 uses QoS Queue 0.

## 1.2.2 ACL

The AMS Series switches access control list (ACL) is probably the most commonly used object in the IOS. It is used for packet filtering but also for selecting types of traffic to be analyzed, forwarded, or influenced in some way. The ACLs are divided into EtherTypes, IPv4, ARP protocol, MAC and VLAN parameters etc. Here we will just go over the standard and extended access lists for TCP/IP. As you create ACEs for ingress classification, you can assign a policy for each port, the policy number range from 1-8. However each policy can be applied to any port. This makes it very easy to determine what type of ACL policy you will be working with.

### 1.2.2-1 Ports

The section describes how to configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE rule.

#### Web Interface

To configure the ACL Ports Configuration via the Web Interface:

- 1. Click Configuration, ACL and Ports.
- 2. Configure the required ACL settings for each of the ports.
- 3. Click the Apply button to save your changes or the Reset button to revert to previous settings.

ALLOV	ALLOY	-	index a				MB	20TDBR/P			
AMS-24T6SEP	Cl Part Managed Digate Rooter					dee m	* * * *				
AW3-24103FF							OFF	Auto-Logout	L	ogout He	
System											
Configuration	ACLI	ACL Ports Configuration									
► Port	600	Policy		Rate	Port						
* ACL	Port	ID	Action	Limiter ID	Redirect	Mirror	Logging	Shutdown	State	Counter	
Ports	( The second sec				Disabled .						
Rate Limiters Access Control List	*	-	< •	•	Port 1 E	• •	< •	• •	•	*	
ACL Status					Port 2 Port 3 -						
► Aggregation											
<ul> <li>Spanning Tree</li> </ul>					Disabled A Port 1						
► IGMP Snooping	1	0	Permit 💌	Disabled -	Port 2	Disabled 💌	Disabled -	Disabled -	Enabled -	4327469	
► MLD Snooping					Port 3 +						
► MVR	(*******				Disabled .						
► LLDP	2	0	Permit 💌	Disabled -	Port 1 E	Disabled -	Disabled -	Disabled -	Enabled -	0	
Filtering Data Base	-		I GITTIN .	Disabled	Port 2	District	District	Disabled	Chaples [1]		
► VLAN					Port 3 -						
Voice VLAN					Disabled •						
► GARP	3	0	Permit 💌	Disabled 💌	Port 1 E Port 2	Disabled 💌	Disabled 💌	Disabled 💌	Enabled 💌	0	
► GVRP					Port 3 -						
► QoS					Disabled .						
Thermal Protection	4	0	Permit 💌	Disabled -	Port 1 E	Disabled -	Disabled -	Disabled -	Enabled -	0	
▶ sFlow Agent	4	U	Permit	Disabled •	Port 2	Disabled	Disabled	Disabled	Enabled V	U	
Loop Protection     Single IP					Port 3 +						
Easy Port					Disabled *						
Mirroring	5	0	Permit 💌	Disabled -	Port 1 E Port 2	Disabled -	Disabled -	Disabled -	Enabled -	Ó	
Trap Event Severity					Port 2 Port 3 +						
SMTP Configuration					Disabled A						
UPnP					Port 1 E						
Security	6	0	Permit 💌	Disabled 💌	Port 2	Disabled -	Disabled -	Disabled 👻	Enabled -	0	
Maintenance					Port 3 +						
					Disabled .						
	7	0	Permit 💌	Disabled -	Port 1 E	Disabled -	Disabled -	Disabled -	Enabled -	0	
		-			Port 2 Port 3 *					0	
					Port 3 *						

Fig. 27 Port ACL Configuration

Port:	Physical port of the switch.
Policy ID:	Select the Policy to apply to this port. The allowed vales are 1 through 8. The default value is 1.
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.
Port Redirect:	Select which port frames are copied on. The allowed values are Disabled or a specific port number. The default value is Disabled.
Mirror:	Specify the mirror operation of this port. The allowed values are: <b>Enabled:</b> Frames received on the port are mirrored.

	Disabled: Frames received on the port are not mirrored.
	The default value is "Disabled".
Logging:	<ul> <li>Specify the logging operation of this port. The allowed values are:</li> <li>Enabled: Frames received on the port are stored in the System Log.</li> <li>Disabled: Frames received on the port are not logged.</li> <li>The default value is Disabled.</li> <li>Please note that the System Log memory size and logging rate is limited.</li> </ul>
Shutdown:	Specify the port shut down operation of this port. The allowed values are: <b>Enabled:</b> If a frame is received on the port, the port will be disabled. <b>Disabled:</b> Port shut down is disabled. The default value is Disabled.
State:	Used to enable or disable the selected port. The allowed values are: <b>Enabled:</b> Enables the port and allows packets to be sent and received. <b>Disabled:</b> Disables the port. The default value is Enabled.
Counter:	Displays the amount of frames that match this ACE.
Refresh Button:	Used to refresh the values displayed in the counter section.
Clear Button:	Used to clear the counters.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply:	Used to save the settings configured on this page.

### 1.2.2-2 Rate Limiters

The section describes how to configure the ACL Rate Limiting Parameters. Up to 16 different rate limits can be set and applied to individual ports. Rate Limits can be set in either pps (Packets Per Second) or Kbps (Kilo Bits Per Second). Only 1 rate limit can be applied to each port.

#### Web Interface

To configure the ACL Rate Limiters via the Web Interface:

- 1. Click Configuration, ACL and Rate Limiters.
- 2. Configure up to 16 Rate Limiters, using either pps or Kbps.
- 3. Click the Apply button to save your changes or the Reset button to revert to previous settings.

C 🔒 🗋 192.168.1.1				_	tr 🔁
ALLOY	Citheri Maraget Bapet Kontern				18977 
AMS-24T6SFP			NAME AND A	uto-Logout OFF	Logout Hel
v System	*				
▼ System Information	ACL Rate Limit	er Config	uration		
Information	Rate Limiter ID	Rate	Unit		
Configuration CPU Load			< •		
► Time	1	24000	kbps 💌		
► Account	2	8000	kbps 👻		
► IP	3		1		
► Syslog		1	pps 💌		
► SNMP	4	1	pps 💌		
<ul> <li>Configuration</li> <li>Port</li> </ul>	- 5	1	pps 💌		
V ACL	E 6	1	pps 💌		
Ports	7	1	pps 💌		
Rate Limiters	8	1	pps 💌		
Access Control List	9	1	pps 💌		
ACL Status  Aggregation	10	1			
<ul> <li>Spanning Tree</li> </ul>					
► IGMP Snooping	11	1	pps 💌		
MLD Snooping	12	1	pps 💌		
► MVR	13	1	pps 💌		
<ul> <li>LLDP</li> <li>Filtering Data Base</li> </ul>	14	1	pps 👻		
<ul> <li>Filtering Data Base</li> <li>VLAN</li> </ul>	15	1	pps 💌		
Voice VLAN	16	1	pps 💌		
► GARP			ppo i		
► GVRP	Apply Reset				
<ul> <li>QoS</li> <li>Thermal Protection</li> </ul>					

Fig. 28 Rate Limiter Configuration

#### **Parameter Description**

Rate Limiter ID:The Rate Limiter ID, from 1 through to 16.Rate:Enter the required rate that you want to limit traffic flow to. If you are using<br/>Kbps, rates must be set in increments of 100.

Unit:	Select to limit traffic in units of either pps (Packets Per Second) or Kbps (Kilo Bits Per Second).
Reset Button:	Used to reset unsaved changes to original configuration.
Apply:	Used to save the settings configured on this page.

## 1.2.2-3 Access Control List

The section describes how to configure Access Control List rules. An Access Control List (ACL) is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted. Other actions can also be invoked when a matching packet is found, including rate limiting, mirroring, redirecting matching packets to another port or to the system log, or shutting down a port.

This page shows the Access Control List (ACL), which is made up of the ACE's defined on this switch. Each row describes the ACE that is defined. The maximum number of ACE's is 256 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACE's used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority for these entries is the highest.

#### Web Interface

To configure the ACL Rules via the Web Interface:

- 1. Click Configuration, ACL and Access Control List.
- 2. Click the 😌 icon to add a new ACL or use the other ACL modification buttons, to edit or remove an existing ACL entry.
- 3. Click the Apply button to save your changes or the Reset button to revert to previous settings.

When editing an entry on the ACE Configuration page, note that the Items displayed depend on various selections, such as Frame Type and IP Protocol Type. Specify the relevant criteria to be matched for this rule, and set the actions to take when a rule is matched (such as Rate Limiter, Port Redirection, Logging, and Shutdown).

- C fi 🗋 192.168.1.1								1	
ALLOY	CE Part Manager						SCHTHER P		
AMS-24T6SFP				a kakak	A	uto-Logout 0	FF 💽	Logout F	H
System									
▼ System Information	Access C	control List C	Configura	tion	Auto-refresh	Refresh	Clear	Remove All	J
Information Configuration	Ingress	Policy /	Frame	Action	Rate	Port Redirect	Mirror	Counter	
CPU Load	Port	Bitmask	Туре		Limiter	Redirect			
► Time									
► Account									
► IP									
► Syslog									
► SNMP									
Configuration									
► Port	=								
V ACL									
Ports									
FUILS									
Rate Limiters									
Rate Limiters									
Rate Limiters Access Control List									
Rate Limiters Access Control List ACL Status									
Rate Limiters Access Control List ACL Status Aggregation									
Rate Limiters Access Control List ACL Status Aggregation Spanning Tree IGMP Snooping MLD Snooping									
Rate Limiters Access Control List ACL Status Aggregation Spanning Tree I GMP Snooping MLD Snooping MVR									
Rate Limiters Access Control List ACL Status Aggregation Spanning Tree IGMP Snooping MLD Snooping									
Rate Limiters Access Control List ACL Status Aggregation Spanning Tree IGMP Snooping MLD Snooping MVR LLDP Filtering Data Base									
Rate Limiters Access Control List ACL Status Aggregation Spanning Tree IGMP Snooping MLD Snooping MVR LLDP Filtering Data Base VLAN									
Rate Limiters Access Control List ACL Status Aggregation Spanning Tree IGMP Snooping MLD Snooping MVR LLDP Filtering Data Base									
Rate Limiters Access Control List ACL Status Aggregation Spanning Tree IGMP Snooping MLD Snooping MVR LLDP Filtering Data Base VLAN									
Rate Limiters Access Control List ACL Status Aggregation Spanning Tree IGMP Snooping MLD Snooping MVR LLDP Filtering Data Base VLAN Voice VLAN									



Ingress Port:	<ul> <li>Indicates the ingress port of the ACE. Possible values are:</li> <li>Any: The ACE will match any ingress port.</li> <li>Policy: The ACE will match ingress ports with a specific policy (Policy must be created in the Ports Section before it will appear in the list).</li> <li>Port: The ACE will match a specific ingress port.</li> </ul>
Policy / Bitmask:	Indicates the Policy or Bitmask that the filter will match.
Frame Type:	<ul> <li>Indicates the frame type of the ACE. Possible values are:</li> <li>Any: The ACE will match any frame type.</li> <li>Ethernet Type: The ACE will match Ethernet Type frames. Note that an</li> <li>Ethernet Type based ACE will not get matched by IP and ARP frames.</li> <li>ARP: The ACE will match ARP/RARP frames.</li> <li>IPv4: The ACE will match all IPv4 frames.</li> </ul>
Action:	Indicates the forwarding action of the ACE. <b>Permit:</b> Frames matching the ACE may be forwarded and learned. <b>Deny:</b> Frames matching the ACE are dropped.
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 Copy:	Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port copy operation is disabled.
Mirror:	Specify the mirror operation of this port. The allowed values are: <b>Enabled:</b> Frames received on the port are mirrored. <b>Disabled:</b> Frames received on the port are not mirrored. The default value is "Disabled".
Logging:	Indicates the logging operation of the ACE. Possible values are: Enabled: Frames matching the ACE are stored in the System Log. Disabled: Frames matching the ACE are not logged. Please note that the System Log memory size and logging rate is limited.
Shutdown:	Indicates the port shut down operation of the ACE. Possible values are: <b>Enabled:</b> If a frame matches the ACE, the ingress port will be disabled. <b>Disabled:</b> Port shut down is disabled for the ACE.
Counter:	The counter indicates the number of times the ACE was hit by a frame. <b>Modification Buttons:</b> You can modify each ACE (Access Control Entry) in the table using the

	following buttons:
	🕀 Inserts a new ACE before the current row.
	Edits the ACE row.
	🕥 Moves the ACE up the list.
	Moves the ACE down the list.
	🗵 Deletes the ACE.
	🕀 The lowest plus sign adds a new entry at the bottom of the ACE
	listings.
Refresh Button:	Used to refresh the values displayed in the ACL section.
Clear Button:	Used to clear the selected ALC entry.
Remove All:	Used to remove all entries from the ACL list.
Ingress Port, Policy	Filter and Frame Type
Ingress Port:	Indicates the ingress port of the ACE. Possible values are:
	All: The ACE will match all ingress ports.
	<b>Port:</b> The ACE will match a specific ingress port.
Policy Filter:	Specify the policy number filter for this ACE.
	<b>Any:</b> 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
	value. Two fields for entering a policy value and bitmask will appear, enter
	the specific policy ID and bitmask.
	(Policy must be created in the Ports Section before it will appear in the list)
Frame Type:	Indicates the frame type of the ACE. Possible values are:
	Any: The ACE will match any frame type.
	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 0600 hexadecimal).
	<b>ARP:</b> Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with Ethernet type.
	<b>IPv4:</b> Only IPv4 frames can match this ACE. Notice the IPv4 frames won't
	match the ACE with Ethernet type.

Filter Criteria based on Selected Frame Type

#### **Ethernet – Mac Parameters**

*SMAC Filter:* The type of source MAC address. Options: Any, Specific Default: Any

DMAC Filter:The type of destination MAC address. Options: Any, MC - multicast, BC -<br/>broadcast, UC - unicast, Specific<br/>Default: Any

#### **Ethernet – EtherType Filter Parameters**

EtherType Filter:This option can only be used to filter Ethernet II formatted packets. Options:<br/>Any, Specific (600-ffff hex)<br/>Default: Any<br/>a detailed listing of Ethernet protocol types can be found in RFC1060. A few<br/>of the more common types include 0800 (IP), 0806(ARP), 8137 (IPX).

#### **ARP – Mac Parameters**

SMAC Filter:	The type of source MAC address. Options: Any, Specific Default: Any
DMAC Filter:	The type of destination MAC address. Options: Any, MC - multicast, BC - broadcast, UC - unicast, Specific Default: Any

#### **ARP – ARP Parameters**

SMAC Filter:	The type of source MAC address. Options: Any, Specific Default: Any
ARP/RARP:	Specifies the type of ARP packet.
	Any: no ARP/RARP opcode flag is specified.
	ARP: frame must have ARP/RARP opcode set to ARP
	<b>RARP:</b> frame must have ARP/RARP opcode set to RARP.
	Other: frame has unknown ARP/RARP opcode flag;
	Default: Any
Request/Reply:	Specifies whether the packet is an ARP request, reply, or either type.
	Any: no ARP/RARP opcode flag is specified.
	Request: frame must have ARP Request or RARP Request opcode flag set.
	Reply: frame must have ARP Reply or RARP Reply opcode flag.
	Default: Any
Sender IP Filter:	Specifies the sender's IP address.
	Any: no sender IP filter is specified
	Host: specifies the sender IP address in the SIP Address field.
	Network: specifies the sender IP address and sender IP mask in the SIP
	Address and SIP Mask fields.
	Default: Any

Target IP Filter:	Specifies the destination IP address. <b>Any:</b> no target IP filter is specified <b>Host:</b> specifies the target IP address in the Target IP Address field. <b>Network:</b> specifies the target IP address and target IP mask in the Target IP Address and Target IP Mask fields Default: Any
ARP SMAC Match:	<ul> <li>Specifies whether frames can be matched according to their sender hardware address (SHA) field settings.</li> <li>Any: any value is allowed.</li> <li>0: ARP frames where SHA is not equal to the SMAC address.</li> <li>1: ARP frames where SHA is equal to the SMAC address.</li> <li>Default: Any</li> </ul>
RARP DMAC Match:	<ul> <li>Specifies whether frames can be matched according to their target hardware address (THA) field settings.</li> <li>Any: any value is allowed.</li> <li>0: RARP frames where THA is not equal to the DMAC address.</li> <li>1: RARP frames where THA is equal to the DMAC address.</li> <li>Default: Any</li> </ul>
IP/Ethernet Length:	<ul> <li>Specifies whether frames can be matched according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.</li> <li>Any: any value is allowed.</li> <li>O: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must not match this entry.</li> <li>1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must match this entry.</li> <li>Default: Any</li> </ul>
IP:	<ul> <li>Specifies whether frames can be matched according to their ARP/RARP hardware address space (HRD) settings.</li> <li>Any: any value is allowed.</li> <li>O: ARP/RARP frames where the HRD is equal to Ethernet (1) must not match this entry.</li> <li>1: ARP/RARP frames where the HRD is equal to Ethernet (1) must match this entry.</li> <li>Default: Any</li> </ul>
Ethernet:	Specifies whether frames can be matched according to their ARP/RARP protocol address space (PRO) settings. Any: any value is allowed. 0: ARP/RARP frames where the PRO is equal to IP (0x800) must not match this entry.

1: ARP/RARP frames where the PRO is equal to IP (0x800) must match this entry. Default: Any

#### IPv4 – MAC Parameters

DMAC Filter:	The type of destination MAC address. Options: Any, MC - multicast, BC -
	broadcast, UC - unicast, Specific
	Default: Any

#### IPv4 – IP Parameters

IP Protocol Filter:	The type of destination MAC address. Options: Any, MC - multicast, BC -
	broadcast, UC - unicast, Specific
	Default: Any

The following additional fields are displayed when these protocol filters are selected.

#### **ICMP** Parameters

ICMP Type Filter:	Specifies the type of ICMP packet to filter for this rule. Options: Any, Specific: 0-255; Default: Any
ICMP Code Filter:	Specifies the ICMP code of an ICMP packet to filter for this rule. Options: Any, Specific (0-255); Default: Any

#### **UDP** Parameters

- Source Port Filter:Specifies the UDP source filter for this rule. Options: Any, Specific (0-65535),<br/>Range (0-65535);<br/>Default: AnyDest. Port Filter:Specifies the UDP destination filter for this rule. Options: Any, Specific (0-
- Dest. Port Filter: Specifies the UDP destination filter for this rule. Options: Any, Specific (0-65535), Range (0-65535); Default: Any

#### **TCP Parameters**

Source Port Filter:	Specifies the TCP source filter for this rule. Options: Any, Specific (0-65535),
	Range (0-65535);
	Default: Any
Dest. Port Filter:	Specifies the TCP destination filter for this rule. Options: Any, Specific (0- 65535), Range (0-65535);
	Default: Any
TCP FIN:	<ul> <li>Specifies the TCP "No more data from sender" (FIN) value for this rule.</li> <li>Any: any value is allowed.</li> <li>0: TCP frames where the FIN field is set must not match this entry.</li> <li>1: TCP frames where the FIN field is set must match this entry.</li> </ul>
----------	---
	Default: Any
TCP SYN:	Specifies the TCP "Synchronize sequence numbers" (SYN) value for this rule. Any: any value is allowed.
	<ul><li>0: TCP frames where the SYN field is set must not match this entry.</li><li>1: TCP frames where the SYN field is set must match this entry.</li><li>Default: Any</li></ul>
TCP RST:	Specifies the TCP "Reset the connection" (RST) value for this rule. Any: any value is allowed.
	<ul><li>0: TCP frames where the RST field is set must not match this entry.</li><li>1: TCP frames where the RST field is set must match this entry.</li><li>Default: Any</li></ul>
TCP PSH:	<ul> <li>Specifies the TCP "Push Function" (PSH) value for this rule.</li> <li>Any: any value is allowed.</li> <li>0: TCP frames where the PSH field is set must not match this entry.</li> <li>1: TCP frames where the PSH field is set must match this entry.</li> </ul>
	Default: Any
ТСР АСК:	Specifies the TCP "Acknowledgment field significant" (ACK) value for this rule. Any: any value is allowed.
	<b>0:</b> TCP frames where the ACK field is set must not match this entry.
	<ol> <li>TCP frames where the ACK field is set must match this entry.</li> <li>Default: Any</li> </ol>
TCP URG:	<ul> <li>Specifies the TCP "Urgent Pointer field significant" (URG) value for this rule.</li> <li>Any: any value is allowed.</li> <li>0: TCP frames where the URG field is set must not match this entry.</li> <li>1: TCP frames where the URG field is set must match this entry.</li> </ul>
	Default: Any
IP TTL:	Specifies the time-to-Live settings for this rule. <b>Any:</b> any value is allowed. <b>Non-zero:</b> IPv4 frames with a TTL field greater than zero must match this
	entry. <b>Zero:</b> IPv4 frames with a TTL field greater than zero must not match this entry. Default: Any

IP Fragment:	Specifies the fragment offset settings for this rule. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame. <b>Any:</b> any value is allowed. <b>Yes:</b> IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must match this entry. <b>No:</b> IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not match this entry. Default: Any
IP Option:	<ul> <li>Specifies the options flag setting for this rule.</li> <li>Any: any value is allowed.</li> <li>Yes: IPv4 frames where the options flag is set must match this entry.</li> <li>No: IPv4 frames where the options flag is set must not match this entry.</li> <li>Default: Any</li> </ul>
SIP Filter:	Specifies the source IP filter for this rule. <b>Any:</b> no source IP filter is specified. <b>Host:</b> specifies the source IP address in the SIP Address field. <b>Network:</b> specifies the source IP address and source IP mask in the SIP Address and SIP Mask fields. Default: Any
DIP Filter:	<ul> <li>Specifies the destination IP filter for this rule.</li> <li>Any: no destination IP filter is specified.</li> <li>Host: specifies the destination IP address in the DIP Address field.</li> <li>Network: specifies the destination IP address and destination IP mask in the DIP Address and DIP Mask fields.</li> <li>Default: Any</li> </ul>
Response to take when	a rule is matched
Action:	Permits or denies a frame based on whether it matches an ACL rule. Default: Permit
Rate Limiter:	Specifies a rate limiter to apply to the port. Range 1 – 16. Default: Disabled
Port Copy:	Defines a port to which matching frames are copied. Range: 1-10. Default: Disabled
Mirror:	Mirrors matching frames from this port. Default: Disabled ACL-based port mirroring set by this parameter and port mirroring set on the general Mirror Configuration page are implemented independently. To

	use ACL-based mirroring, enable the Mirror parameter on the ACE Configuration page. Then open the Mirror Configuration page, set the "Port to mirror on" field to the required destination port, and leave the "Mode" field Disabled.
Logging:	Enables logging of matching frames to the system log. Default: Disabled Open the System Log Information menu to view any entries stored in the system log for this entry. Related entries will be displayed under the "Info" or "All" logging levels.
Shutdown:	Shuts down a port when a matching frame is seen. Default: Disabled
Counter:	Shows the number of frames which have matched any of the rules defined for this ACL.
VLAN Parameters	
802.1Q Tagged:	Specifies whether or not frames should be 802.1Q tagged. Options: Any, Disabled, Enabled; Default: Any
VLAN ID Filter:	Specifies the VLAN to filter for this rule. Options: Any, Specific (1-4095); Default: Any
Tag Priority:	Specifies the User Priority value found in the VLAN tag (3 bits as defined by IEEE 802.1p) to match for this rule. Options: Any, Specific (0-7); Default: Any
Reset Button:	Used to reset unsaved changes to original configuration.
Apply:	Used to save the settings configured on this page.
Cancel:	Used to disregard any changes made.

## 1.2.2-4 ACL Status

The section displays the current ACL rules configured on the switch

### Web Interface

To view the ACL Rate rules via the Web Interface:

- 1. Click Configuration, ACL and ACL Status.
- 2. If you would like the page to auto-refresh the ACL Information, check the Auto-Refresh tick box at the top of the page, or alternatively hit the refresh button to refresh the page manually.

C fi 🗋 192.168.1.1											2 🕏
AMS-24T6SFP	RLCCY In has thread			<b>H</b>	in a			Auto-Lo	ogout OF	Loge	out Hel
System     System Information	ACL Statu	s					Combin	ed	Auto-	efresh 🗉 📑	Refresh
Information Configuration	User	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter	Conflic
CPU Load	IP Management	All	ARP	Deny	Disabled	Disabled	Disabled	Yes	No	18900	No
► Account	IP .	All	IPv4/UDP 68 DHCP	Denv	Disabled	Disabled	Disabled	Yes	No	0	No
► IP	Management Reserved	All	Server EType	Permit	Disabled	Disabled	Disabled		No		No
► Syslog		All	EType	Permit	Disabled	Disabled	Disabled		No		No
► SNMP											
Configuration     Port											
Y ACL											
Ports											
Rate Limiters											
Access Control List											
ACL Status											
► Aggregation											
Spanning Tree											
► IGMP Snooping											
MLD Snooping											
► MVR											
FLLDP											
Filtering Data Base											
+ VLAN											
a second data second											
► Voice VLAN											
F GARP											

Fig. 31 Viewing the Access Control List Rules

User:	Indicates the ACL user.
Ingress Port:	Indicates the ingress port of the ACE. Possible values are: All: The ACE will match all ingress port. Port: The ACE will match a specific ingress port.
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.
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. 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".
CPU:	Forward packet that matched the specific ACE to CPU.
CPU Once:	Forward first packet 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. The specific ACE is not applied to the hardware due to hardware limitations.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.

# 1.2.3 Aggregation

The AMS Series switches support two types of link aggregation, Static Trunk and LACP. Static Trunk is a non-protocol based aggregation method where the connections are determined via source and destination MAC Addresses. LACP is an IEEE standardized protocol used to aggregate ports. Because it is an IEEE standard LACP trunking or aggregation can be used across multi-vendor equipment.

By Aggregating ports between two devices this allows the bandwidth to be increased. For example if we aggregate 3 Gigabit Ports, the link between the two devices is increased to a 3Gb.

# 1.2.3-1 Static Trunk

This section is used to configure the static trunk settings. Here you will determine the method used to create the static trunk and also create your aggregation groups.

Ports using Static Trunk as their trunk method can choose their unique Static Group ID to form a logic "trunked port". The benefit of using the Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should be aggregated together to form a "logical trunked port". Using Static Trunk on both ends of a link is strongly recommended. Both devices must be configured to use the same speed and duplex settings.

### Web Interface

To configure the Static Trunk settings via the Web Interface:

- 1. Click Configuration, Aggregation and Static Trunk.
- 2. Select the type of method used to initiate the trunk.
- 3. Create the trunk group using the radio buttons in the table. Each Group ID is an individual trunk group, add the required ports into the desired trunk group.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Fig. 32 Configuring a static trunk group

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, 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, 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, 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, TCP/UDP Port Number is enabled.
Group ID:	Indicates the group ID for the trunk group. Up to 13 trunk groups can be created. Each port can only belong to one trunk group. The Group ID normal is used when no trunk groups are to be used.

Port Members:Each switch port is listed for each group ID. Select a radio button to include a<br/>port in a trunk group, or select normal to remove the port from a trunk<br/>group. By default, no ports belong to any trunk group. Only full duplex ports<br/>can join a trunk group and ports must be the same speed in each group.

*Reset Button:* Used to reset unsaved changes to original configuration.

Apply Button: Used to save the settings configured on this page.

## 1.2.3-2 LACP

Ports using Link Aggregation Control Protocol (according to IEEE 802.3ad specification) as their trunking method can choose their unique LACP Group ID to form a logical "trunked port". The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a ready member of a "trunk group" (also called aggregator). LACP is safer than other trunking methods, such as static trunking.

### 1.2.3-2-1 Configuration

This section is used to add ports to a LACP based trunk/aggregation group. Here you can also assign a specific key for each trunking group you are creating or allow the switch to automatically assign a key to the configured group.

### Web Interface

To configure the LACP settings via the Web Interface:

- 1. Click Configuration, Aggregation, LACP and Configuration.
- 2. Tick the LACP Enabled check box next to the port(s) you want to enable.
- 3. Select to either assign a Key automatically or manually assign a key. If you are manually assigning a key enter the key into the space provided.
- 4. Select the Role that you wish the port to play, either Active or Passive.

								2 🔁
ALLOY	HION					Adres 1	-	
ALL LOY	Hofeet Barrant				1100			
AMS-24T6SFP			-			A	uto-Logout OFF	- Logout Hel
▼ System								
▼ System Information	LACP	Port Config	uratio	n				
Information	Port	LACP Enabled	-	Key	Rol	100		
Configuration CPU Load			0		0	-		
► Time	1		Auto	-	Active	-		
► Account	2		Auto	-	Active	-		
► IP ► Syslog		m	Auto		Active			
Sysiog	3					<u>•</u> ]		
· Configuration	4		Auto		Active	•		
► Port	5		Auto	•	Active			
F ACL	6		Auto		Active	•		
Aggregation     Static Trunk	7		Auto	-	Active	-		
* LACP	8		Auto	-	Active	-		
Configuration	9		Auto		Active	-		
System Status Port Status	10		Auto		Active	-		
Port Statistics	100000000			and it is				
Spanning Tree	11		Auto		Active	•		
► IGMP Snooping	12	Ę	Auto	-	Active	-		
MLD Snooping MVR	13		Auto	•	Active	-		
> LLDP	14		Auto	-	Active	-		
Filtering Data Base	15		Auto		Active	-		
► VLAN ► VOICE VLAN	16		Auto		Active	-1		
	10		Colto.	100	Active			

Fig. 33 Configuring a LACP trunk group

Port:	Physical port of the switch.
LACP Enabled:	Used to enable or disable LACP on the desired port. To enable LACP on an individual port check the tick box.
Key:	The Key is used to determine a specific trunk/aggregation group. The key can be generated automatically by the switch or you can enter a key manually. If entering manually valid values are 1 through to 65535. For multiple ports to belong to the same group the key must be the same on each port.
Role:	The role determines who the port(s) handle LACP traffic. If set to Active the port will initiate the LACP group, by sending LACP packets to the connecting device each second. When set to Passive the port will wait to receive LACP packets from the connecting device.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

### 1.2.3-2-2 System Status

This section displays the current status of the LACP groups.

### Web Interface

To view the LACP status via the Web Interface:

- 1. Click Configuration, Aggregation, LACP and System Status.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

- C fi 🗋 192.168.1.1		\$ 🔁
ALLOY		
AMS-24T6SFP		Auto-Logout OFF . Logout He
• System	-	
* System Information	LACP System Status	Auto-refresh 🔲 [Refresh]
Information Configuration CPU Load	Aggr ID Partner Partner Last Local System ID Key Changed Ports No ports enabled or no existing partners	
Time     Account	Construction of the second	
► IP		
► Syslog		
► SNMP		
▼ Configuration		
► Port		
- ACL		
▼ Aggregation		
Static Trunk		
* LACP		
Configuration		
System Status Port Status		
Port Statistics		
► Spanning Tree		
► IGMP Snooping		
MLD Snooping		
► MVR		
+ LLDP		
► Filtering Data Base		
+ VLAN		
► Voice VLAN		
► GARP		
► GVRP	3	

#### **Parameter Description**

Fig. 34 LACP Status

Aggr ID:	The Aggregation ID associated with this aggregation instance.
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 the aggregation changed.
Local Ports:	Display which ports belong to the Aggregation Group.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.

### 1.2.3-2-3 Port Status

**Parameter Description** 

This section displays the current port status of the LACP groups.

### Web Interface

To view the Port status via the Web Interface:

- 1. Click Configuration, Aggregation, LACP and Port Status.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

- C fi 🗋 192.168.1.1	_	_			_		2	12
ALLOY	ALLON THE REAL OF	r I						
AMS-24T6SFP		_			and an other to		the local division of the second division of	Hel
* System	1	15						
▼ System Information	LAC	P State	IS				Auto-refresh	0
Information	1000				Partner	Partner		
Configuration	Por	LACP	Key	Aggr ID	System ID	Port		
CPU Load	in the second	No	4			-		
► Time	100	2 No				-		
► Account		No						
► IP		No	-					
► Syslog		i No	.7		τ	-		
► SNMP		i No						
▼ Configuration		No		1		-		
► Port		3 No			-	-		
► ACL		8 No	•		-	-		
▼ Aggregation	1					-		
Static Trunk		No No			-			
* LACP	-1				-			
Configuration		No						
System Status		Na						
Port Status	1							
Port Statistics		No	1			2		
Spanning Tree	1	No No						
IGMP Snooping	1	No No			-	-		
MLD Snooping	2			1		5		
► MVR	2					-		
► LLDP	2							
Filtering Data Base		R No				-		
► VLAN	2		7			-		
Voice VLAN		i No	•		-			
. GARP	2	i No		÷	-	-		
► GVRP	1							

Fig. 35 Port Status

Port:	Physical port of the switch.
LACP:	If LACP is enabled on the port <b>Yes</b> will be shown if LACP is disabled then <b>No</b> will be displayed.
Key:	The key assigned to this port. Only ports with the same key can be aggregated together.
Aggr ID:	The Aggregation ID assigned to this group.
Partner System ID:	The partners system ID. (MAC Address)
Partner Port:	The port number of the partner device.

*Auto*-Refresh: Tick the box to enable the information to be automatically refreshed.

*Refresh:* Used to manually refresh the information on the page.

### 1.2.3-2-4 Port Statistics

This section displays the current port statistics relating to the LACP information.

### Web Interface

To view the Port statistics via the Web Interface:

- 1. Click Configuration, Aggregation, LACP and Port Statistics.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

C fi 🗋 192.168.1.1	-					
ALLOY	ALLOY In The Manual County Trans		- Beet			
AMS-24T6SFP			A 2 Buildenbuildenb			Auto-Logout OFF + Logout H
▼ System ▼ System Information	LACE	Statistic	s			Auto-refresh 🔲 Refresh Clear
information	1000	LACP	LACP	Discar	had	
Configuration	Port		Transmitted			
CPU Load	1	0	0	0	0	
► Time	2	ő	ő	ő	0	
► Account	3	0	0	0	0	
F IP	4	0	0	0	0	
Syslog	5	0	0	0	0	
► SNMP	6	0	0	0	0	
Configuration	- 8	0	0	0	0	
Port	9	ő	0	ő	ő	
> ACL	10	ū	0	0	0	
▼ Aggregation	11	0	0	0	0	
Static Trunk	12	0	0	0	0	
* LACP	13 14	0	0	0	0	
Configuration	14	0	0	0	0	
System Status	16	0	0	0	a	
Port Status	17	ũ	Ű.	Ő	0	
Port Statistics	18	0	0	0	0	
Spanning Tree	19	0	0	0	0	
► IGMP Snooping	20	0	0	0	0	
► MLD Snooping	21 22	0	0	0	0	
► MVR	23	0	0	0	0	
+ LLDP	24	õ	ő	ő	õ	
Filtering Data Base	25	0	0	0	0	
VLAN	26	Û	0	0	0	
Voice VLAN						
F GARP						
► GVRP						
- GVRF						

Fig. 36 LACP Port Statistics

Port:	Physical port of the switch.
LACP Received:	Shows how many LACP frames have been received on each port.
LACP Transmitted:	Shows how many LACP frames have been transmitted from each port.
Discarded:	Shows how many unknown or illegal frames have been discarded from each port.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.

Refresh:

Used to manually refresh the information on the page.

# 1.2.4 Spanning Tree

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

STP uses a distributed algorithm to select a bridging device (STP- compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.



Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

STP can run in one of three modes: STP, RSTP or MSTP. A device running RSTP is compatible with other devices running STP; a device running MSTP is compatible with other devices running RSTP or STP. By default, on a device in MSTP mode each port automatically detects the mode of the device connected to it (MSTP, RSTP or STP), and responds in the appropriate mode by sending messages (BPDUs) in the corresponding format. Ports on a device in RSTP mode can automatically detect and respond to connected devices in RSTP and STP mode. Particular ports can also be forced to only operate in a particular mode (spanning-tree force-version command).

### STP

The Spanning Tree Protocol (STP) is the original protocol defined by IEEE standard 802.1D-1988. It creates a single spanning tree over a network.

STP mode may be useful for supporting applications and protocols whose frames may arrive out of sequence or duplicated, for example NetBeui.

### RSTP

Rapid Spanning Tree Protocol (RSTP) also creates a single spanning tree over a network. Compared with STP, RSTP provides for more rapid convergence to an active spanning tree topology. RSTP is defined in IEEE standard 802.1D-2004.

### MSTP

The Multiple Spanning Tree Protocol (MSTP) addresses the limitations in the previous spanning tree protocols, STP and RSTP, within networks that use multiple VLANs with topologies that employ alternative physical links. It supports multiple spanning tree instances on any given link within a network, and supports large networks by grouping bridges into regions that appear as a single bridge to other devices.

MSTP is defined in IEEE standard 802.1Q-2005. The protocol builds on, and remains compatible with, the previous IEEE standards defining STP and RSTP.

## 1.2.4-1 Bridge Settings

This section is used to configure the spanning tree bridge settings, allowing full configuration of all spanning tree parameters. Here you can select what Spanning Tree Protocol you would like the switch to use, STP, RSTP or MSTP.

### Web Interface

To configure the Bridge Settings for STP via the Web Interface:

- 1. Click Configuration, Spanning Tree and Bridge Settings.
- 2. Select the required STP protocol and configure the appropriate basic and advanced STP parameters.
- 3. Click the Save button to save your changes or the Reset button to revert to previous settings.

- C fi 🗋 192.168.1.1			<u>☆</u>
ALLOY			
AMS-24T6SFP			Auto-Logout OFF 💽 Logout He
• System	4		
▼ System Information	STP Bridge Config	uration	
Information	Basic Settings		
Configuration			
CPU Load	Protocol Version	MSTP 💌	
► Time	Bridge Priority	32768 🔹	
► Account	Forward Delay	15	
► IP	Max Age	20	
<ul> <li>Syslog</li> <li>SNMP</li> </ul>		1	
Configuration	Maximum Hop Count		
► Port	Transmit Hold Count	6	
► ACL			
► Aggregation	Advanced Settings		
V Spanning Tree	Edge Port BPDU Filte	ering	
Bridge Settings	Edge Port BPDU Gua		
MSTI Mapping	Port Error Recovery		
MSTI Priorities	Port Error Recovery	Timeout	
CIST Ports		Contraction of March 1 and 1	
MSTI Ports	Apply Reset		
Bridge Status	Apply Reset		
Port Status Port Statistics			
► IGMP Snooping			
<ul> <li>MLD Snooping</li> </ul>			
► MVR			
► LLDP			
► Filtering Data Base			
► VLAN			

Fig. 37 STP Bridge Settings

Protocol Version:	Select the appropriate STP protocol, STP, RTP or MSTP. Default value is MSTP.
Bridge Priority:	Controls the bridge priority. The Lower the numeric value the higher the priority. The bridge priority plus the MSTI instance number, concatenated
	with the 6-byte MAC address of the switch forms a Bridge Identifier. For

	MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP Bridge. Default is 32768.
Forward Delay:	The delay used by STP Bridges to transit Root and Designated Ports to Forwarding state (used in STP compatible mode). Valid values are in the range 4 to 30 seconds. Default is 15 seconds.
Max Age:	The maximum age of the information transmitted by the Bridge, when it is the Root Bridge. Valid values are in the range of 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2. Default is 20.
Maximum Hop Count:	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.
Transmit Hold Count:	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.
Edge Port BPDU Filtering:	Controls whether a port explicitly configured as Edge will transmit and receive BPDUs.
Edge Port BPDU Guard	Controls whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.
Port Error Recovery:	Controls whether a port in the error-disabled state will automatically be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.
Port Error Recovery Timeout:	The time to pass before a port in the error-disabled state can be enabled.
	Valid values are between 30 and 86400 seconds (24 hours).
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

## 1.2.4-2 MSTI Mapping

This section is used to map VLAN's to MSTI's when using the MSTP protocol. MSTP enables the grouping and mapping of VLANs to different spanning tree instances. So, an MST Instance (MSTI) is a particular set of VLANs that are all using the same spanning tree.

In a network where all VLANs span all links of the network, judicious choice of bridge priorities for different MSTIs can result in different switches becoming root bridges for different MSTIs. That will result in the different MSTIs choosing different active topologies on the network.

Multiple VLAN's can be mapped to a single MSTI, when entering multiple VLAN ID's, they need to be separated using a comma. An unused MSTI should be left blank, do not enter VLAN ID's into unused MSTI's.

#### Web Interface

To configure the MSTI Mapping's for MSTP via the Web Interface:

- 1. Click Configuration, Spanning Tree and MSTI Mapping.
- 2. Give the configuration a name.
- 3. Enter the required VLAN's into the configured MSTI(s).
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.

		ANC-SITER?
		in the state of the second
AMS-24T6SFP		Auto-Logout OFF 💽 Logout Help
System		
<ul> <li>System Information</li> </ul>	MSTI Configuration	
Information	Add VLANs separated by spaces or comma.	
Configuration	Unmapped VLANs are mapped to the CIST. (The default bridge	to the second
CPU Load		instance).
► lime ► Account	Configuration Identification	
► IP	Configuration Name 00-00-8c-8d-00-cb	
► Syslog	Configuration Revision 0	
► SNMP		
Configuration	MSTI Mapping	
► Port		
► ACL	MSTI VLANs Ma	pped
► Aggregation	MSTI1	
▼ Spanning Tree		
Bridge Settings MSTI Mapping	MSTI2	
MSTI Priorities		4
CIST Ports	MSTI3	
MSTI Ports	The second secon	14
Bridge Status	MSTI4	
Port Status		//
Port Statistics	MSTI5	
► IGMP Snooping		
MLD Snooping	MSTI6	
► MVR		
<ul> <li>LLDP</li> <li>Filtering Data Base</li> </ul>	MSTI7	
Flitering Data Base VLAN		
Voice VLAN		
► GARP	Apply Reset	

Fig. 38 MSTI Mappings

### **Parameter Description**

- *Configuration Name:* The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision, as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name must be no more than 32 characters.
- *Configuration Revision:* The revision of the MSTI configuration. This must be an integer between 0 and 65535.
- MSTI:The bridge instance. The CIST is not available for explicit mapping of VLAN's,<br/>as it will receive the VLANs that have not been manually mapped to an<br/>MSTI.
- VLAN's Mapped: The list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty.
- *Reset Button:* Used to reset unsaved changes to original configuration.

Apply Button: Used to save the settings configured on this page.



Fig. 39 Example MSTI Configuration

## 1.2.4-3 MSTI Priorities

This section is used to manually change the priority of the STP bridge instances. The CIST (Common and Internal Spanning Tree) is the default Bridge Instance when using MSTP and is always active. Any VLAN that has not been assigned to a MIST is assigned to the CIST. The lower the priority value, the higher the priority the bridge has.

### Web Interface

To configure the MSTI Priorities for MSTP via the Web Interface:

- 1. Click Configuration, Spanning Tree and MSTI Priorities.
- 2. Select the Bridge Priority for each of the Bridge Instances.
- 3. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Parameter Description	Fig. 40 MSTI Priority Configuration
MSTI:	The bridge instance. The CIST is the default instance, which is always active.
Priority:	Select the Bridge priority from the drop down box next to each MIST.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

## 1.2.4-4 CIST Ports

This section is used to configure individual STP Parameters for each port. Here you can enable and disable STP on individual ports, configure the ports as AdminEdge ports, give certain ports higher priority than others and much more.

#### Web Interface

To configure the CIST Port Parameters via the Web Interface:

- 1. Click Configuration, Spanning Tree and CIST Ports.
- 2. Select and configure the appropriate settings.
- 3. Click the Apply button to save your changes or the Reset button to revert to previous settings.

System       STP CIST Port Configuration         Information       Configuration         CPU Load       Port         * Time       Account         * JP       System         * System       Auto         * Dime       Account         * JP       System         * System       Auto         * Or       STP         * Account       * Dev         * JP       System         * System       Auto         * Account       * Dev         * Port       StP CiST Augunguted Pid Configuration         Port       StP         * Account       * Dev         * System       Auto         * Account       * Dev         * Port       Strip         Port       Strip         Port       Strip         Port       Strip         Port       Strip         Port       Strip         * Auto       10         * Auto       120         * Strip       Auto         * Stripping       Mato         MST Mapping       Auto         * Stabilitics       Edge         * IMLD Snooping </th <th>C fi 🗋 192.168.1.1</th> <th></th> <th>\$</th>	C fi 🗋 192.168.1.1													\$
System information information Configuration CPU Load       STP CIST Port Configuration         Port       STP       Path Cost       Priority       Admin Edge       Auto       Restricted       BPDU       Point-to- point         • Account       • Port       STP       Path Cost       Priority       Admin Edge       Auto       Restricted       BPDU       Point-to- point         • Port       STP       Path Cost       Priority       Admin Edge       Auto       Restricted       BPDU       Point-to- point         • Port       STP       Path Cost       Priority       Admin Edge       Auto       Restricted       BPDU       Point-to- point         • Adgregation       • Strings       Non-Edge       - <th></th> <th>z†</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>+</th> <th>Auto-L</th> <th>ogout OFF</th> <th>E Loge</th> <th>out</th>		z†								+	Auto-L	ogout OFF	E Loge	out
Configuration       Configuration         CPU Load       Port       STP         Port       STP       Path Cost       Priority       Admin Edge       Auto       Restricted       BPDU       Point-to-point         * Account       Port       STP       Path Cost       Priority       Admin Edge       J       Forced True         * Sylidg       StP       Port       STP       Path Cost       Priority       Admin Edge       J       Forced True         * Sylidg       StP       Port       STP       Path Cost       Priority       Admin Edge       Auto       Restricted       BPDU       Point-to-point         • Sylidg       StP       Port       STP       Path Cost       Priority       Admin Edge       Auto       Restricted       BPDU       Point-to-point         • Ord       StP       Port       StP       Path Cost       Priority       Admin Edge       Auto       Point-to-goint         • Ord       StP       Port       StP       Path Cost       Priority       Admin Edge       Auto       Point-to-goint         • Addo       II       Auto       III 20       Non-Edge       IIII       Auto       IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	System -	1.7			1.0									
Configuration CPU Load       STP Enabled       Path Cost       Priority       Admin Edge       Auto       Restricted       BPDU Guard       Point-to- point         - Account       IP       -       Auto       120       Non-Edge       -       Forced True       -         - Systog       -       -       Auto       120       Non-Edge       -       Forced True       -         - Port       -	· vystem moninadom	CI	ST Port	Conf	igura	ation								
CPU Load       Port       STP       Path Cost       Priority       Admin Edge       Auto       Restricted       BPDU       Point         Time       Account       I/I       Auto       I/I       I/I       Finality       Admin Edge       Auto       Restricted       BPDU       Point-to-point         IP       Sylidg       SiMP       Port       STP       Path Cost       Priority       Admin Edge       Auto       Restricted       BPDU       Point-to-point         Sontiguration       Fort       Enabled       Path Cost       Priority       Admin Edge       Auto       Restricted       BPDU       Point-to-point         Adgregation       Sontiguration       STP       Path Cost       Priority       Admin Edge       Auto       Auto<		ST Age	gregaled Por	l Canligu	nation	-								_
Account: IP Sysicg Port STIP Configuration Port STIP Configuration Software Port Statistics Port Port Port Port Port Port Port Port	CPU Load Po	ort			Path	Cost	Priority	Admin Edge						
Systog SNMP       Clot Hormul Port Confoundation         Port       STP Enabled       Path Cost       Priority       Admin Edge Ldge       Admin Edge Role       BPDU Guard       Point-to- point         + Orf       - Adto       -       <		-		Auto	-	1	128 -	Non-Edge 💌	J	1			Forced True	•
SiMMP     Port     STP       Contiguration     Port     STP       Port     Enabled     Plont Cost     Priority     Admin Edge     Auto     Restricted     BPDU     Point-to-point       ACL     -     -     -     -     -     -     -     -     -       AQD     -     1     Auto     122     Non-Edge     -     -     -     -     -       MSTI Mapping     3     Auto     128     Non-Edge     -     -     -     Auto     -       MSTI Mapping     3     Auto     128     Non-Edge     -     -     -     Auto     -       MSTI Mapping     5     Auto     128     Non-Edge     -     -     -     Auto     -       MSTI Mapping     5     Auto     128     Non-Edge     -     -     Auto     -       MSTI Mapping     6     Auto     128     Non-Edge     -     -     -     Auto     -       MSTI Mapping     6     Auto     128     Non-Edge     -     -     Auto     -       MSTI Mapping     6     Auto     128     Non-Edge     -     -     Auto       Port Status     7		_		_	_						_			-
Port       SIP       Path Cost       Priority       Admin Edge       Admin Edge       Restricted       BPUU       Point         - Fort       - ACL       - ACL		ST No	rmal Port Co	mouratio	on -									- 1
Port         ACL         AQ         Image: Constraint of the second sec		ort			Path	Cost	Priority	Admin Edge						
Act.         1         Auto         120         Non-Edge         0         Auto         •           f spanning Tree         Bridge Settings         3         Auto         •         120         Non-Edge         0         Auto         •           MSTI Mapping         3         Auto         •         128         Non-Edge         0         Auto         •           MSTI Mapping         3         Auto         •         128         Non-Edge         0         Auto         •           MSTI Mapping         3         Auto         •         128         Non-Edge         0         Auto         •           MSTI Priorities         6         Auto         •         128         Non-Edge         0         Auto         •           MSTI Provities         6         Auto         •         128         Non-Edge         0         Auto         •           MST Mapping         6         Auto         •         128         Non-Edge         0         Auto         •           MST Mapping         8         Auto         •         120         Non-Edge         0         Auto         •           CGMP Snooping         8         Auto				0	-	-								-
f spanning Tree Bridge Settings         2         Auto         120         Non-Edge         J         Auto         Auto           MST Mapping         3         Auto         128         Non-Edge         J         Auto				-			and the second second							-
Bridge Settings         2         Auto         128         Non-Edge         3         Auto					- Intel State	-	1						1	-
MSTI Profiles CIST Ports         4         Auto         128         Non-Edge         2         Auto         •           MSTI Ports         5         Auto         128         Non-Edge         2         Auto         •           Bridge Status         5         Auto         128         Non-Edge         2         Auto         •           Port Status         5         Auto         128         Non-Edge         2         Auto         •           Port Status         7         Auto         120         Non-Edge         2         Auto         •           IGM Snooping         8         Auto         120         Non-Edge         4         Auto         •           MVR         129         Non-Edge         4         Auto         •         Auto         •           LDP         10         Auto         128         Non-Edge         4         Auto         •           VLAN         12         Auto         128         Non-Edge         4         Auto         •		2		Auto	•		128 -						Auto	
CIST Ports         4         Auto         T28         Non-Edge         V         Auto         ×           MST Ports         6         Auto         128         Non-Edge         V         Auto         ×           Bridge Status         6         Auto         128         Non-Edge         V         Auto         ×           Port Status         6         Auto         128         Non-Edge         V         Auto         ×           Port Status         7         Auto         122         Non-Edge         V         Auto         ×           IGMP Snooping         8         Auto         122         Non-Edge         V         Auto         ×           MUS Snooping         8         Auto         128         Non-Edge         V         Auto         ×           MUR Snooping         9         Auto         128         Non-Edge         V         Auto         ×           MVR         10         Auto         128         Non-Edge         V         Auto         ×           VLAN         11         Auto         128         Non-Edge         V         Auto         ×		3		Auto	*		128 💌	Non-Edge 💌					Auto	*
MSTI Ports         6         Auto         128         Non-Edge         7         Auto         ×           Bridge Status         6         Auto         128         Non-Edge         7         Auto         ×           Port Status         7         Auto         128         Non-Edge         7         Auto         ×           ICMP Snooping         8         Auto         120         Non-Edge         7         Auto         ×           ICMP Snooping         8         Auto         120         Non-Edge         7         Auto         ×           MVR         9         Auto         128         Non-Edge         7         Auto         ×           HUPR         10         Auto         128         Non-Edge         7         Auto         ×           HUP Nove         10         Auto         128         Non-Edge         7         Auto         ×           HUP Nove         11         Auto         128         Non-Edge         7         Auto         ×           VLAN         12         Auto         128         Non-Edge         7         Auto         ×		4	0	Auto	-		128 🖛	Non-Edge 💌	I				Auto	-
Bridge Status         5         Auto         128         Non-Edge         7         Auto         Auto           Port Status         7         Auto         120         Non-Edge         7         Auto		5		Auto	-		128 -	Non-Edge 💌	V			1	Auto	-
Font Status         7         Auto         120         Non-Edge         4           Pont Statistics         7         Auto         120         Non-Edge         4 <td< td=""><td></td><td>6</td><td></td><td>Auto</td><td>-</td><td></td><td>128 -</td><td>Non-Edge -</td><td>1</td><td></td><td>Ē</td><td></td><td>Auto</td><td></td></td<>		6		Auto	-		128 -	Non-Edge -	1		Ē		Auto	
For Statistics         Auto         East         Auto		7		Auto	- Local		128 -		12				Auto	- Andrews
MLD Snooping         9         Auto         Ico         Non-Edge         7         Auto         Auto         Auto         Year           MVR         9         Auto         128         Non-Edge         7         Auto         A														
NVA         10         Auto         128         Non-Edge         27         Auto         x           Filtering Data Base         11         Auto         128         Non-Edge         27         Auto         x           VLAN         12         Auto         128         Non-Edge         27         Auto         x					-								1	
Filtering Data Base         11         Auto         128         Non-Edge         2         Auto            VLAN         12         Auto         128         Non-Edge         2         Auto          Auto          Auto          Auto          Auto           Auto           Auto           Auto           Auto            Auto		9		Auto	-		128 💌	Provide and Provide and	3				Auto	
VLAN         11         Auto         128         Non-Edge         Auto         Auto           Voice VLAN         12         Auto         128         Non-Edge         4         Auto		10		Auto	-	1	128 💌	Non-Edge 💌	V			3	Auto	*
Voice VLAN 12 Auto 💌 128 Non-Edge 🗸 . Auto 💌		11		Auto	-		128 -	Non-Edge 💌	1		E		Auto	-
		12		Auto	-		128 -	Non-Edge	4				Auto	-
▶ GARP	► VLAN ► VOICE VLAN				- Lond			A second second				3	1	_

Fig. 41 CIST Port Configuration

#### **Parameter Description**

*Port:* Physical port of the switch.

*STP Enabled:* Select to enable or disable STP on each port.

Path Cost:Controls the path cost incurred by the port. The Auto setting will set the<br/>path cost as appropriate by the physical link speed, using the 802.1D<br/>recommended values. Using a 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 favour of higher path cost ports. Valid values are in the range 1 to 200000000.

- *Priority:* Controls the port priority. This can be used to control priority of ports having identical port cost.
- Admin Edge:The Admin Edge function allows ports to be configured as Edge or Non-Edge<br/>ports. When set to an Edge Port the transition to the forwarding state is<br/>faster than Non-Edge ports. A port should be set as an Edge port if there are<br/>no other Bridges attached to this port. E.g. no STP enabled devices<br/>connected.
- Auto Edge: Controls whether the bridge should enable automatic edge detection on the bridge port.
- Restricted Role: If enabled, the port cannot be selected as a Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.
- Restricted TCN: If enabled, the port will not propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.
- BPDU Guard:If enabled, causes the port to disable itself upon receiving valid BPDU's.Contrary to the similar bridge setting, the port Edge status does not affect<br/>this setting. A port entering error-disabled state due to this setting is subject<br/>to the bridge Port Error Recovery setting as well.
- Point-to-Point:Controls whether the port connects to a point-to-point LAN rather than to a<br/>shared medium. This can be automatically determined, or forced either true<br/>or false. Transition to the forwarding state is faster for point-to-point LANs<br/>than for shared media.

*Reset Button:* Used to reset unsaved changes to original configuration.

Apply Button: Used to save the settings configured on this page.

# 1.2.4-5 MSTI Ports

This section is used to configure MSTI Port parameters. An MSTI Port is a virtual port and each MSTI has its own virtual port. The MSTI must be configured before the individual port configuration options can be applied. This section is much the same as the CIST Port settings but configuration done here is for each MSTI rather than the CIST.

### Web Interface

To configure the MSTI Port Parameters via the Web Interface:

- 1. Click Configuration, Spanning Tree and MSTI Ports.
- 2. Select the MSTI you would like to configure and press the GET button.
- 3. Now you can configure the appropriate port settings for the MSTI.
- 4. Repeat for all MSTIs.
- 5. Click the Apply button to save your changes or the Reset button to revert to previous settings.

AMS-24T6SFP ×		- • • ×
← ← C ff 🖞 192.168.1.1		🗘 👧 🗏
AMS-24T6SFP		Auto-Logout OFF
System     System Information     Information     Configuration	MSTI Port Configuration	
CPU Load Time Account	E Get	

Fig. 42 MSTI selection

C f 🖞 192.168.1.1				1. I
ALLOY	ALLOY Diversional Death Texts	-		Addateset
And the second s	GTer Managel Dodge Textur	🖬		CCCCCC State where where
MS-24T6SFP	-			Auto-Logout OFF - Logout
System	-		a the factor of the	
<ul> <li>System Information</li> </ul>	MST1	MSTI Port	Configuration	
Information	MSTLA	ogregated Ports C	onliguration	
Configuration CPU Load	Port	Path (	Cost Priority	
Time		Auto -	128 •	
Account		Design and the	and the second s	
- IP	MSTIN	ormal Ports Confi	guration	
- Syslog	Port	Path (	Cost Priority	
SNMP		0 .	0.	
Configuration Port			128 -	
ACL		and the second second		
Aggregation	2	Auto 💌	128 💌	
Spanning Tree	3	Auto 💌	128 -	
Bridge Setlings	4	Auto -	128 -	
MSTI Mapping MSTI Priorities	5	Auto -	128 -	
CIST Ports		Long Long		
MSTI Ports	6	Auto 💌	128 💌	
Bridge Status	7	Auto 📼	128 -	
Port Status	8	Auto 💌	128 -	
Port Statistics	9	Auto 💌	128 -	
IGMP Snooping		the second second		
MLD Snooping	10	Auto -	128 •	
LLDP	11	Auto 💌	128 💌	
Filtering Data Base	12	Auto 💌	128 -	
		Contraction of the local distance of the loc		



Port:	Physical port of the switch.
Path Cost:	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using a 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 favour of higher path cost ports. Valid values are in the range 1 to 20000000.
Priority:	Controls the port priority. This can be used to control priority of ports having identical port cost.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

## 1.2.4-6 Bridge Status

This section is used to display the status information for each of the configured STP Bridges.

### Web Interface

To view the Bridge Status via the Web Interface:

- 1. Click Configuration, Spanning Tree and Bridge Status.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

C fi 192.168.1.1							Ę	2 1
ALLOY	ALLOY District Manual District Statist				MAGINT			
AMS-24T6SFP	-					Auto-Log	out OFF 💽 Logout	Hel
System		and the second se					1	
<ul> <li>System Information</li> </ul>	STPE	ridges					Auto-refresh	esh
Information	( ALCONOMIC )	2100 22	Root		Topology	Topology		
Configuration	MSTI	Bridge ID	ID	Port Cost		Change Last		
CPU Load	CIST	80.00-00.00.8C 00.00 F2	80.00-00.00 8C.00.00 F2			-		
► Time		and so that and the first of the source of the source of	and the state of the second					
Account								
► IP								
► Syslog								
SNMP								
Configuration								
► Port ► ACL								
<ul> <li>Aggregation</li> <li>Spanning Tree</li> </ul>								
Bridge Settings								
MSTI Mapping								
MSTI Priorities								
CIST Ports								
MSTI Ports								
Bridge Status								
Port Status								
Port Statistics								
► IGMP Snooping								
MLD Snooping								
MVR								
► LLOP								
Filtering Data Base								
► VLAN								
► Voice VLAN								

### Fig. 44 Bridge Status Information

MSTI:	The Bridge Instance. This is also a link to the STP Detailed Bridge Status
Bridge ID:	The Bridge ID of this Bridge instance.
Root ID:	The Bridge ID of the currently elected root bridge.
Root Port:	The switch port currently assigned the root port role.
Root Cost:	Root Path Cost. For the Root Bridge it will be zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

- *Topology Flag:* The current state of the Topology Change Flag of this Bridge instance.
- *Topology Change Last:* The time since the last Topology Change occurred.
- *Auto*-Refresh: Tick the box to enable the information to be automatically refreshed.
- *Refresh:* Used to manually refresh the information on the page.

## 1.2.4-7 Port Status

This section is used to display the status information for each of the configured STP CIST Ports.

### Web Interface

To view the STP CIST Port Status via the Web Interface:

- 1. Click Configuration, Spanning Tree and Port Status.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

🗟 C 🕺 🗋 192.168.1.1					 C 😨
ALLOY	ALLOY D'Inter Manager		_ 666		HIRY I
AMS-24T6SEP				AMERICA	Auto-Logout OFF - Logout He
					Auto-Logour orr v togette
System	STR	Port Statu	c		Auto-refresh
* System Information	SIF	Fort Statu	5		Auto-reliesh 🖂 [Kellesh]
Information	Port	CIST Role	CIST State	Uptime	
Configuration	1	Non-STP	Forwarding		
CPU Load	2	Non-STP	Forwarding		
► Time	3	Non-STP	Forwarding	2	
► Account	4	Non-STP	Forwarding		
► IP		Non-STP	Forwarding		
► Syslog	6	Non-STP	Forwarding		
► SNMP	1	Non-STP	Forwarding	1	
Configuration	8	Non-STP Non-STP	Forwarding Forwarding		
► Port		Non-STP	Forwarding		
► AGL		Non-STP	Forwarding		
		Non-STP	Forwarding		
<ul> <li>Aggregation</li> </ul>		Non-STP	Forwarding	2	
* Spanning Tree		Non-STP	Forwarding		
Bridge Settings	15	Non-STP	Forwarding		
MSTI Mapping		Non-STP	Forwarding	-	
MSTI Priorities		Non-STP	Forwarding	*	
CIST Ports		Non-STP	Forwarding	÷	
MSTI Ports		Non-STP	Forwarding		
Bridge Status	20	Non-STP Non-STP	Forwarding	-	
Port Status		Non-STP Non-STP	Forwarding Forwarding	2	
Port Statistics		Non-STP	Forwarding		
► IGMP Snooping	23	Non-STP	Forwarding		
MLD Snooping		Non-STP	Forwarding		
MUD shooping MVR		Non-STP	Forwarding		
► LLDP					
Filtering Data Base					
► VLAN					
► Voice VLAN					

Fig. 45 Port Status Information

Port:	Physical port of the switch.
CIST Role:	The current STP port role of the CIST port. The port role can be one of the following values: Non-STP, AlternatePort, Backup Port, RootPort, DesignatedPort Disabled.
CIST State:	The current STP port state of the CIST port. The port state can be one of the following values: Blocking, Learning and Forwarding.
Uptime:	The time since the bridge port was last initialized.

*Auto*-Refresh: Tick the box to enable the information to be automatically refreshed.

*Refresh:* Used to manually refresh the information on the page.

## 1.2.4-8 Port Statistics

This section is used to display the port statistics for of the configured STP CIST Ports.

### Web Interface

To view the Port Statistics via the Web Interface:

- 1. Click Configuration, Spanning Tree and Port Statistics.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

C fi 🗅 192.168.1.1		立 <b>强</b>
C A 192.168.1.1 C State of Content of Conte	STP Statistics Port MSTP RSTP STP TCN MSTP RSTP STP TCN M No ports enabled	Auto-Logout OFF  Clean Auto-refresh Refresh Clean Discarded
Port Status Port Status Port Statistics IGMP Snooping MLD Snooping		
► MVR ► LLDP ► Filtering Data Base		
► VLAN		

Fig. 46 Port Statistics

Port:	Physical port of the switch.
MSTP:	The number of MSTP Configuration BPDU's received/transmitted on the port.
RSTP:	The number of RSTP Configuration 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.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.

AMS User Manual

## 1.2.5 IGMP Snooping

IGMP Snooping is a way for Layer 2 switches to reduce the amount of multicast traffic on a LAN.

Without IGMP Snooping, Layer 2 switches handle IP multicast traffic in the same manner as broadcast traffic and forward multicast frames received on one port to all other ports in the same VLAN. IGMP Snooping allows switches to monitor network traffic, and determine hosts to receive multicast traffic, by looking into IGMP packets to learn which attached hosts need to receive which multicast groups. This allows the switch to forward multicast traffic only out the appropriate ports. If it sees multiple reports sent for one group, it will forward only one of them.

#### Joining a multicast group (Membership report)

When a host wants to receive a stream, referred to as "joining a group", it sends out an IGMP packet containing the address of the group it wants to join. This packet is called an IGMP Membership report, often referred to as a "join packet". This packet is forwarded through the LAN to the local IGMP querier, which is typically a router. Once the querier has received an IGMP join message, it knows to forward the multicast stream to the host. If it is not already receiving the stream, it must tell the devices between itself and the multicast source, which may be some hops away from the querier, that it wishes to receive the stream. This might involve a process of using Layer 3 multicast protocols to signal across a WAN, or it might be as simple as receiving a stream from a locally connected multicast server.

#### Staying in the multicast group (Query message)

The Query message is used by a querier to determine whether hosts are still interested in an IGMP group. At certain time intervals (the default is 125 seconds), the querier sends an IGMP query message onto the local LAN. The destination address of the query message is a special "all multicast groups" address. The purpose of this query is to ask "Are there any hosts on the LAN that wish to remain members of multicast groups?" After receiving an IGMP query, any host that wants to remain in a multicast group must send a new join packet for that group. If a host is a member of more than one group, then it sends a join message for each group it wants to remain a member of. The querier looks at the responses it receives to its query, and compares these to the list of multicast streams that it is currently registered to forward. If there are any items in that list for which it has not received query responses, it will stop forwarding those streams. Additionally, if it is receiving those streams through a Layer 3 network, it will send a Layer 3 routing protocol message upstream, asking to no longer receive that stream.

#### Leaving the multicast group (Leave message)

How a host leaves a group depends on the IGMP version that it is using. Under IGMP version 1, when a host has finished with a data stream, the local querier continues to send the stream to the host until it sends out the next query message and receives no reply back from the host. IGMP version 2 introduced the Leave message. This allows a host to explicitly inform its querier that it wants to leave a particular multicast group. When the querier receives the Leave message, it sends out a group specific query asking whether any hosts still want to remain members of that specific group. If no hosts respond with join messages for that group, then the querier knows that there are no hosts on its LAN that are still members of that group. This means that for that specific group, it can ask to be pruned from the multicast tree. IGMP version 3 removed the Leave message. Instead a host leaves a group by sending a join message with no source specified.

The AMS Series supports IGMP Snooping V1, V2 and V3 and supports up to 1024 multicast groups, both IGMP Querier and IGMP Proxy are also supported.

# **1.2.5-1 Basic Configuration**

This section is used to enable and configure IGMP Snooping on the AMS Series switches.

### Web Interface

To configure the IGMP Snooping parameters via the Web Interface:

- 1. Click Configuration, IGMP Snooping and Basic Configuration.
- 2. Select to enable or disable IGMP Snooping on the switch.
- 3. Configure ports to be Router Ports, Fast Leave Ports and select whether you would like to enable throttling.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.

C fi 🖞 192.168.1.1							\$ <u>1</u>
MS-24T6SFP	B Ten Minard Date Tent			HIH		Auto-Logout OFF	Logaut H
System • System Information	IGMP	Snooping	Configura	ation			
Information	1000		Global Confi	guration			
Contiguration CPU Load		g Enabled		0			
CPU Load ► Time	and a second sec	ered IPMCv4 Flo	oding Enabled	×.			
Account	IGMP S	SM Range		232.0.0.0	/ 8		
- IP	Proxy E	nabled					
- Syslog	Bort	Related Co	oficuratio				
- SNMP	Foiti	telateu co	inigurauo				
Configuration	E Port	Router Port	Fast Leave	Throttling			
Port			11	0 .			
ACL Aggregation	1			unlimited -			
<ul> <li>Aggregation</li> <li>Spanning Tree</li> </ul>	2			unlimited *			
V IGMP Snooping	3			unlimited -			
Basic Contiguration	4			unlimited -			
VLAN Configuration	5	n		unlimited •			
Port Group Filtering	6	E		unlimited •			
Status	the second se			and the second se			
Groups information IPv4 SSM Information	7			unlimited *			
MLD Snooping	8			unlimited 💌			
MVR	9			unlimited *			
LLDP	10			unlimited 💌			
Filtering Data Base	11			unlimited 💌			
► VLAN	12			unlimited -			
Voice VLAN	13			unlimited *			
	14			unlimited +			

Fig. 47 IGMP Snooping Configuration

Snooping Enabled:	Enable IGMP Snooping on the switch.
Unregister IPMCv4 Flooding Enabled:	Enable unregistered IPMCv4 flooding enabled.
IGMP SSM Range:	SSM (Source –Specific Multicast) range allows SSM-aware hosts and routers that run the SSM service model to use groups in the configured address range. Format: <ip address="">/<subnet mask=""></subnet></ip>
Proxy Enabled:	Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave message to the IGMP router.
Port:	Physical port of the switch.
Router Port:	Specify which ports are connected to a Layer 3 multicast device of IGMP Querier. If an aggregation member port is selected as a router port, the whole aggregation group will act as a router port.
Fast Leave:	Enable Fast Leave on the port. Fast Leave allows the switch to remove an interface from the IGMP table if there are no members listening on that multicast group. Normally the group would not be removed until the expiration timer has exceeded.
Throttling:	Throttling is used to limit the amount of multicast groups a switch port can belong to. Valid values are unlimited or 1 through to 10. Default is unlimited.

# **1.2.5-2 VLAN Configuration**

This section is used to configure specific IGMP Settings for each of the configured VLAN groups. IGMP Snooping can be enable or disabled for every individual VLAN group. 20 VLAN groups will be displayed on the screen by default this can be increased to a maximum of 99. The VLAN with the lowest VID will be displayed at the top of the table. To browse to additional pages use the arrow keys at the top of the page.

### Web Interface

To configure the IGMP VLAN Configuration parameters via the Web Interface:

- 1. Click Configuration, IGMP Snooping and VLAN Configuration.
- 2. Select the appropriate IGMP parameters for the specific VLAN group.
- 3. Repeat for all VLAN groups configured on the switch. Use the arrow keys to move between pages. The Refresh button can be used to refresh the page for the latest information.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Fig. 48 IGMP VLAN Configuration

### **Parameter Description**

VLAN ID: The VLAN ID of each VLAN group.
Snooping Enabled:	Enable IGMP Snooping for each individual VLAN group. A maximum of 32 VLAN's can be enabled at any one time.
IGMP Querier:	A router is used to send IGMP query messages to IGMP enabled hosts. The IGMP router can also be called the IGMP Querier. This option is used to enable the IGMP Querier function on an individual VLAN.
Compatibility:	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, and Forced IGMPv3. Default compatibility value is IGMP-Auto.
RV:	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255; Default robustness variable value is 2.
QI:	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; Default query interval is 125 seconds.
QRI:	Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; Default query response interval is 100 in tenths of seconds (10 seconds).
LLQI (LMQI for IGMP):	Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds; Default last member query interval is 10 in tenths of seconds (1 second).
URI:	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds. Default unsolicited report interval is 1 second.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.
Refresh:	Used to manually refresh the information on the page.
<<, >>:	The arrow keys are used to navigate between the pages, displaying the current VLAN's configured on the switch.

# 1.2.5-3 Port Group Filtering

With this feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and when applied to a port to deny access to that port on the configured multicast address. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group.

IGMP filtering controls only IGMP membership join reports and has no relationship to the function that directs the forwarding of IP multicast traffic.

## Web Interface

To configure the IGMP Port Group Filtering entries via the Web Interface:

- 1. Click Configuration, IGMP Snooping and Port Group Filtering.
- 2. Click Add New Filtering Group.
- 3. Specify the Multicast IP Address and click Apply to save the settings.
- 4. If you wish to delete an entry check the delete tick box and click Apply.
- 5. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Fig. 49 Multicast Address Filtering

Delete:	Check to delete the entry, and click Apply save the changes and remove the selected entry.
Port:	Select the Port you would like to enable filtering for the configured Multicast address.
Filtering Groups:	Enter the IP Address of the Multicast group to be filtered. Valid values are 224.x.y.z to 239.x.y.z.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

## 1.2.5-4 Status

This section is used to view the status of all configured IGMP parameters on the AMS Series switches.

### Web Interface

To view the IGMP Status via the Web Interface:

- 1. Click Configuration, IGMP Snooping and Status.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.



Fig. 50 IGMP Status

VLAN ID:	The VLAN ID of the entry.
Querier Version:	The current version of the IGMP Querier.
Host Version:	The current version of the host.
Querier Status:	Shows the Querier status of either "Active" or "Idle".
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.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.

## **1.2.5-5 Groups Information**

This section displays the learnt IGMP groups. The IGMP Group Table is sorted first by VLAN ID, and then by group. They 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.

### Web Interface

To view the IGMP Group Information via the Web Interface:

- 1. Click Configuration, IGMP Snooping and Groups Information.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.



Fig. 51 IGMP group information

VLAN ID:	The VLAN ID of the entry.
Groups:	IGMP group address.
Port Members:	Physical Ports on the switch that belong to the IGMP Multicast Group.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.

## *Refresh:* Used to manually refresh the information on the page.

<<, >>: The arrow keys are used to navigate between the pages, displaying the current VLAN's configured on the switch.

## 1.2.5-6 IPv4 SSM Information

Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core network technology of IP multicast targeted for audio and video broadcast application environments.

For the SSM delivery mode, an IP multicast receiver host must use IGMP Version 3 (IGMPv3) to subscribe to channel (S, G). By subscribing to this channel, the receiver host is indicating that it wants to receive IP multicast traffic sent by source host S to group G. The network will deliver IP multicast packets from source host S to group G to all hosts in the network that have subscribed to the channel (S, G).

SSM does not require group address allocation within the network, only within each source host. Different applications running on the same source host must use different SSM groups. Different applications running on different source hosts can arbitrarily reuse SSM group addresses without causing any excess traffic on the network.

Addresses in the range 232.0.0.0/8 (232.0.0.0 to 232.255.255.255) are reserved for SSM by IANA. The AMS also allows you to configure SSM for arbitrary IP multicast addresses also.

## Web Interface

To view the IPv4 SSM Information via the Web Interface:

- 1. Click Configuration, IGMP Snooping and IPv4 SSM Information.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.



Fig. 52 IPv4 SSM information

VLAN ID:	The VLAN ID of the entry.
Group:	Multicast Group Address.
Port:	Physical port number of the switch.
Mode:	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
Source Address:	Source IP Address of the group, current limit on the system for filtering is 128 IP addresses.
Туре:	Indicates the type, either Allow or Deny.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.
<<, >>:	The arrow keys are used to navigate between the pages, displaying the current VLAN's configured on the switch.

# 1.2.6 MLD Snooping

Multicast Listener Discovery (MLD) snooping constrains the flooding of IPv6 multicast traffic on VLANs on a switch. When MLD snooping is enabled on a VLAN, the AMS Series Switches examine MLD messages between hosts and multicast routers and learn which hosts are interested in receiving traffic for a multicast group. Based on what it learns, the switch then forwards multicast traffic only to those interfaces in the VLAN that are connected to interested receivers instead of flooding the traffic to all interfaces.

By default, a switch floods Layer 2 multicast traffic on all interfaces on a switch, except for the interface that is the source of the multicast traffic. This behaviour can consume significant amounts of bandwidth.

You can enable MLD snooping to avoid this flooding. When you enable MLD snooping, the switch monitors MLD messages between receivers and multicast routers and uses the content of the messages to build an IPv6 multicast forwarding table—a database of IPv6 multicast groups and the interfaces that are connected to members of the groups. When the switch receives multicast traffic for a multicast group, it uses the forwarding table to forward the traffic only to interfaces that are connected to the multicast group.

The AMS Series switches support MLD v1 and v2.

## **1.2.6-1 Basic Configuration**

This section is used to enable and configure MLD Snooping on the AMS Series switches.

## Web Interface

To configure the MLD Snooping parameters via the Web Interface:

- 1. Click Configuration, MLD Snooping and Basic Configuration.
- 2. Select to enable or disable MLD Snooping on the switch.
- 3. Configure ports to be Router Ports, Fast Leave Ports and select whether you would like to enable throttling.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.

C fi 🗋 192.168.1.1							52. 9
ALLOY	ALCON Diversion						
MS-24T6SFP	-					Auto-Logout OFF	Logaut He
Account	1 ML	Snooping	Configurat	ion			
Syslog	1.1		Gle	obal Configuration			
SNMP Configuration		ping Enabled					
+ Port		istered IPMCv6 Flo		2	L. Lor		
ACL	#10-10-10	SSM Range Enabled		ff3e::	/ 96	4	
Aggregation     Spanning Tree							
IGMP Snooping	Por	t Related Co	nfiguration	1			
V MLD Snooping	Por	t Router Port	Fast Leave	Throttling			
Basic Configuration			1	0 .			
VLAN Configuration Port Group Filtering		1 11		unlimited -			
Status		2		unlimited *			
Groups Information	E.	3 🗇		unlimited -			
IPv6 SSM Information	and the second sec	4		unlimited -			
MVR		5 1		unlimited •			
LLDP		6		unlimited -			
Filtering Data Base VLAN		7	-	unlimited -			
Voice VLAN			Ē	and the second se			
GARP	and the second sec			unlimited •			
- GVRP		9		unlimited •			
► QoS	1.22	0		unlimited 💌			
Thermal Protection	1	1		unlimited 💌			
sFlow Agent Loop Protection	1	2		unlimited -			
Single IP	1	3		unlimited •			
Easy Port	- 1	4		unlimited .			

Fig. 53 MLD Snooping Configuration

Snooping Enabled:	Enable MLD Snooping on the switch.
Unregister IPMCv6 Flooding Enabled:	Enable unregistered IPMCv6 flooding enabled.
MLD SSM Range:	SSM (Source –Specific Multicast) range allows SSM-aware hosts and routers that run the SSM service model to use groups in the configured address range. Format: <ip address="" v6="">/<subnet mask=""></subnet></ip>
Proxy Enabled:	Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave message to the MLD router.
Port:	Physical port of the switch.
Router Port:	Specify which ports are connected to a Layer 3 multicast device of MLD Querier. If an aggregation member port is selected as a router port, the whole aggregation group will act as a router port.
Fast Leave:	Enable Fast Leave on the port. Fast Leave allows the switch to remove an interface from the MLD table if there are no members listening on that multicast group. Normally the group would not be removed until the expiration timer has exceeded.

Throttling:Throttling is used to limit the amount of IPv6 multicast groups a switch port<br/>can belong to. Valid values are unlimited or 1 through to 10.<br/>Default is unlimited.

## **1.2.6-2 VLAN Configuration**

This section is used to configure specific MLD Settings for each of the configured VLAN groups. MLD Snooping can be enabled or disabled for every individual VLAN group. 20 VLAN groups will be displayed on the screen by default this can be increased to a maximum of 99. The VLAN with the lowest VID will be displayed at the top of the table. To browse to additional pages use the arrow keys at the top of the page.

## Web Interface

To configure the MLD VLAN Configuration parameters via the Web Interface:

- 1. Click Configuration, MLD Snooping and VLAN Configuration.
- 2. Select the appropriate MLD parameters for the specific VLAN group.
- 3. Repeat for all VLAN groups configured on the switch. Use the arrow keys to move between pages. The Refresh button can be used to refresh the page for the latest information.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Fig. 54 MLD VLAN Configuration

### **Parameter Description**

VLAN ID: The VLAN ID of each VLAN group.

Snooping Enabled:	Enable MLD Snooping for each individual VLAN group. A maximum of 32 VLAN's can be enabled at any one time.
MLD Querier:	A router is used to send MLD query messages to MLD enabled hosts. The MLD router can also be called the MLD Querier. This option is used to enable the MLD Querier function on an individual VLAN.
Compatibility:	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is MLD-Auto, Forced MLDv1 and Forced MLDv2. Default compatibility value is MLD-Auto.
RV:	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255; Default robustness variable value is 2.
QI:	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; Default query interval is 125 seconds.
QRI:	Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; Default query response interval is 100 in tenths of seconds (10 seconds).
LLQI (LMQI for MLD):	Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds; Default last member query interval is 10 in tenths of seconds (1 second).
URI:	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds. Default unsolicited report interval is 1 second.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.
Refresh:	Used to manually refresh the information on the page.
<<, >>:	The arrow keys are used to navigate between the pages, displaying the current VLAN's configured on the switch.

# 1.2.6-3 Port Group Filtering

With this feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and when applied to a port to deny access to that port on the configured multicast address. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group.

MLD filtering controls only MLD membership join reports and has no relationship to the function that directs the forwarding of IP multicast traffic.

## Web Interface

To configure the MLD Port Group Filtering entries via the Web Interface:

- 1. Click Configuration, MLD Snooping and Port Group Filtering.
- 2. Click Add New Filtering Group.
- 3. Specify the Multicast IP Address and click Apply to save the settings.
- 4. If you wish to delete an entry check the delete tick box and click Apply.
- 5. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Fig. 55 Multicast Address Filtering

Delete:	Check to delete the entry, and click Apply save the changes and remove the selected entry.
Port:	Select the Port you would like to enable filtering for the configured Multicast address.
Filtering Groups:	Enter the IP Address of the Multicast group to be filtered.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

## 1.2.6-4 Status

This section is used to view the status of all configured MLD parameters on the AMS Series switches.

## Web Interface

To view the MLD Status via the Web Interface:

- 1. Click Configuration, MLD Snooping and Status.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

- C fi 🗋 192.168.1.1		_								公 🤻
ALLOY	ALLOY Citer Managel Code Texts			***			ARCHITE	**]		
	Deep Text	-		***	<b>a</b> aaaa			1		
AMS-24T6SFP								Auto-Lo	ogout OFF	Logout H
► Account									1.	-
► IP	MLD	Snoopin	g Status	6				Auto-n	efresh 🖾 [Refres	h Clear
► Syslog	Statisti	C5								
► SNMP	and shares									
Configuration		Querier	Host	Querier	Queries	Queries	V1 Reports	V2 Reports		
► Port	ID	Version	Version	Status	Transmitted	Received	Received	Received	Received	
. ACL	Router	Port								
Aggregation	-	Status								
Spanning Tree	Port	Status								
IGMP Snooping     MLD Snooping	1									
Basic Configuration	3									
VLAN Configuration	4									
Port Group Filtering	5									
Status	6	-								
Groups information	E 7									
IPv6 SSM Information	8									
► MVR	9	14								
+ LLDP	10	4								
Filtering Data Base	11									
+ VLAN	12									
► Voice VLAN	13									
F GARP	14									
+ GVRP	15									
+ QoS	10									
Thermal Protection	18									
► sFlow Agent	19									
► Loop Protection	20									
► Single IP	21	12								
Easy Port	- 22									

Fig. 56 MLD Status

VLAN ID:	The VLAN ID of the entry.
Querier Version:	The current version of the MLD Querier.
Host Version:	The current version of the host.
Querier Status:	Shows the Querier status of either "Active" or "Idle".
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.
- V1 Leaves Received: The number of Received V2 Leaves.
- *Auto*-Refresh: Tick the box to enable the information to be automatically refreshed.
- *Refresh:* Used to manually refresh the information on the page.

## **1.2.6-5 Groups Information**

This section displays the learnt MLD groups. The MLD Group Table is sorted first by VLAN ID, and then by group. They 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.

### Web Interface

To view the MLD Group Information via the Web Interface:

- 1. Click Configuration, MLD Snooping and Groups Information.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

C fi 🗋 192.168.1.1		<u>ර</u> ත
ALLOY		AND THE REAL PROPERTY
AMS-24T6SFP		Auto-Logout OFF E Logout Hal
Account     IP	MLD Snooping Groups Information	Auto-refresh 🗌 Refresh 🛛 😣
► Syslog	Start from VLAN 1 and group address #00	with 20 entries per page
SNMP Configuration		mun Kn. enumer her heide
Port	Port Members	
ACL	VLAN ID Groups 123456789101112131415161718192021222 No more entries	23 24 25 26
Aggregation	INO more entries	
Spanning Tree		
IGMP Snooping		
MLD Snooping		
Basic Configuration VLAN Configuration		
Port Group Filtening		
Status		
Groups Information		
IPv6 SSM Information		
MVR		
LLDP		
Filtering Data Base VLAN		
Voice VLAN		
GARP		
GVRP		
QoS		
Thermal Protection		
sFlow Agent		
Loop Protection     Single IP		

Fig. 57 MLD group information

VLAN ID:	The VLAN ID of the entry.
Groups:	MLD group address.
Port Members:	Physical Ports on the switch that belong to the MLD Multicast Group.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.

## *Refresh:* Used to manually refresh the information on the page.

<<, >>: The arrow keys are used to navigate between the pages, displaying the current VLAN's configured on the switch.

## 1.2.6-6 IPv6 SSM Information

Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core network technology of IP multicast targeted for audio and video broadcast application environments.

For the SSM delivery mode, an IP multicast receiver host must use IGMP Version 3 (IGMPv3) to subscribe to channel (S, G). By subscribing to this channel, the receiver host is indicating that it wants to receive IP multicast traffic sent by source host S to group G. The network will deliver IP multicast packets from source host S to group G to all hosts in the network that have subscribed to the channel (S, G).

SSM does not require group address allocation within the network, only within each source host. Different applications running on the same source host must use different SSM groups. Different applications running on different source hosts can arbitrarily reuse SSM group addresses without causing any excess traffic on the network.

## Web Interface

To view the IPv6 SSM Information via the Web Interface:

- 1. Click Configuration, MLD Snooping and IPv6 SSM Information.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.





VLAN ID:	The VLAN ID of the entry.
Group:	Multicast Group Address.
Port:	Physical port number of the switch.
Mode:	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
Source Address:	Source IP Address of the group, current limit on the system for filtering is 128 IP addresses.
Туре:	Indicates the type, either Allow or Deny.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.
<<, >>:	The arrow keys are used to navigate between the pages, displaying the current VLAN's configured on the switch.

# 1.2.7 MVR

Multicast VLAN registration (MVR) allows you to efficiently distribute IPTV multicast streams across an Ethernet ring-based Layer 2 network and reduce the amount of bandwidth consumed by this multicast traffic.

In a standard Layer 2 network, a multicast stream received on one VLAN is never distributed to interfaces outside that VLAN. If hosts in multiple VLANs request the same multicast stream, a separate copy of that multicast stream is distributed to the requesting VLANs.

MVR introduces the concept of a multicast source VLAN (MVLAN), which is created by MVR and becomes the only VLAN over which IPTV multicast traffic flows throughout the Layer 2 network. The Alloy AMS Series Switches that are enabled for MVR selectively forward IPTV multicast traffic from interfaces on the MVLAN (source interfaces) to hosts that are connected to interfaces that are not part of the MVLAN. These interfaces are known as MVR receiver ports. The MVR receiver ports can receive traffic from a port on the MVLAN but cannot send traffic onto the MVLAN, and they remain in their own VLANs for bandwidth and security reasons.

## 1.2.7-1 Configuration

This section is used to enable and configure MVR on the AMS Series switches.

## Web Interface

To configure the MVR parameters via the Web Interface:

- 1. Click Configuration, MVR and Configuration.
- 2. Select to enable or disable MVR.
- 3. Configure settings for each individual port.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.

C fi 🗋 192.168.1.1		-	_			_	_	sh 🔁
ALLOY	ANOT					- ALANA		
AMS-24T6SFP							Auto-Logout OFF	<ul> <li>Logout Help</li> </ul>
▼ System	A 1. /							
V System Information	MVR	Configur	ation					
Information	MVR	Made Die	abled 👻					
Configuration			hand -					
CPU Load	VLAN	ID 100						
Time     Account								
> IP	1.	1.1.1	ter de la					
> Syslog	Port	Configura	ation					
► SNMP	Port	Mode	Туре	Immediate Le	ave			E
▼ Configuration		0	0 .	0	1-			
► Port		Deabled	Receiver *	Disabled				
► ACL		And	Land Land					
Aggregation	2	Disabled 💌	tana tana					
Spanning Tree	3	Disabled -	Receiver 💌	Disabled				
<ul> <li>IGMP Snooping</li> <li>MLD Snooping</li> </ul>	4	Disabled -	Receiver -	Disabled				
T MVR	6	Disabled -	Receiver -	Disabled	-			
Configuration	6	Disabled .	Receiver .					
Groups Information	0	Contract of the second	- Amond	and the second s				
Statistics	7	Disabled -	Receiver -	Disabled				
> LLDP	8	Disabled -	Receiver -	Disabled	-			
Filtering Data Base	9	Disabled -	Receiver -	Disabled				
VLAN Voice VLAN	10	Disabled -	Receiver -	Disabled				
F VOICE VLAN	11	and a second second	Receiver -					
► GVRP			Receiver -					
► QoS	12	Disabled -	Contract of the		and the second se			
► Thermal Protection	13	Disabled -	Receiver 💌	Disabled				
► sFlow Agent	- 14	Disabled -	Receiver -	Disabled	-			

Fig. 59 MVR Configuration

MVR Mode:	Used to enable or disable MVR globally on the switch.
VLAN ID:	Specify the VLAN ID used for Multicasting.
Port:	Physical port of the switch.
Mode:	Enable MVR on a per port basis.
Туре:	Specify the port type, this can be either Receiver or Source. When set to source, the port should be connected to a device that is sending the multicast stream. If set to receiver, the port will be connected to a device that is wanting to receive the multicast stream.
Immediate Leave:	Enable Multicast's fast leave parameter on the port.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

## **1.2.7-2 Groups Information**

This section displays the learnt MVR groups. The MVR Group Table is sorted first by VLAN ID, and then by group. They 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.

### Web Interface

To view the MVR Group Information via the Web Interface:

- 1. Click Configuration, MVR and Groups Information.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.



Fig. 60 MVR group information

VLAN ID:	The VLAN ID of the entry.
Groups:	MVR group address.
Port Members:	Physical Ports on the switch that belong to the MLD Multicast Group.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.

*Refresh:* Used to manually refresh the information on the page.

<<, >>: The arrow keys are used to navigate between the pages, displaying the current VLAN's configured on the switch.

## 1.2.7-3 Statistics

This section is used to view the statistics of all configured MVR parameters on the AMS Series switches.

## Web Interface

To view the MVR Statistics via the Web Interface:

- 1. Click Configuration, MVR and Statistics.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.



Fig. 61 MVR Statistics

VLAN ID:	The VLAN ID of the entry.
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.
- *Auto*-Refresh: Tick the box to enable the information to be automatically refreshed.
- *Refresh:* Used to manually refresh the information on the page.

# 1.2.8 LLDP

LLDP enables Ethernet network devices, such as switches and routers, to transmit and/or receive device-related information to or from directly connected devices on the network, and to store such information learned about other devices. The data sent and received by LLDP is useful for many reasons. The switch can discover neighbours—other devices directly connected to it. Devices can use LLDP to advertise some parts of their Layer 2 configuration to their neighbours, enabling some kinds of misconfiguration to be more easily detected and corrected.

LLDP is a link level ("one hop") protocol; LLDP information can only be sent to and received from devices that are directly connected to each other, or connected via a hub or repeater. Advertised information is not forwarded on to other devices on the network.

The information transmitted in LLDP advertisements flows in one direction only, from one device to its neighbours, and the communication ends there. Transmitted advertisements do not solicit responses, and received advertisements do not solicit acknowledgement.

LLDP operates over physical ports (Layer 2) only. For example, it can be configured on switch ports that belong to static or dynamic aggregated links (channel groups), but not on the aggregated links themselves; and on switch ports that belong to VLANs, but not on the VLANs themselves.

## 1.2.8-1 LLDP Configuration

This section is used to enable and configure LLDP on the AMS Series switches.

### Web Interface

To configure the LLDP parameters via the Web Interface:

- 1. Click Configuration, LLDP and LLDP Configuration.
- 2. Modify any LLDP timing parameters if needed.
- 3. Disable, enable two way communication, Tx only or Rx only on a per port basis.
- 4. Specify the information to include in the TLV field of advertised messages.
- 5. Click the Apply button to save your changes or the Reset button to revert to previous settings.

G 🖌 🗋 192.168.1.1									S2 🔁
ALLOY	ALLOY Citien Manual Dealer Texast		. Cent		****		ANSINGUIY		
AMS-24T6SFP		126	<b>UKADA</b> A		a.a.a.			Auto-Logout OF	F Logout Hel
System									
V System Information	LLDP	Configura	ation						
Information Configuration	LLDP P	arameters							
CPU Load	Tx Int	erval 30	seconds						
Time     Account	Tx Ho	ld 4	times						
F IP	Tx De	lav 2	seconds						
► Syslog	Tx Re		seconds						
► SNMP	TA IN	2	securius						
Configuration Port					(	Optional TLV	5		
ACL	Port	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr	
<ul> <li>Aggregation</li> </ul>		0 .		2					
Spanning Tree	1	Disabled 💌	4	×.	1	4	¥.	d.	
IGMP Snooping	2	Disabled *	2	7	1	7		1	
MLD Snooping	3	Disabled -		1	12	4	17	12	
► MVR ▼ LLDP	4	Disabled +	2	2	V	7	1	3	
LLDP Configuration	5	Disabled -		j.	N.	1		J	
LLDP Neighbours	6	Disabled -	E	2	V	2	V	7	
LLDP-MED Contiguration	7	Disabled +		1	3	1	U)		
LLOP-MED Neighbours	8	Disabled -	G	V	V	N N	2	T	
EEE Port Statistics	9	Disabled •		J	i vi	1	14	3	
Filtering Data Base	10	Disabled •	3	2	2	e d		7	
► VLAN	10	Disabled +		7	IV.	IV.	3	J.	
> Voice VLAN	Concession of the local division of the loca	- And	144 1	V.	V		8	V	
	12	Disabled • Disabled •		7	IV.	a de la companya de l	N.	T.	

Fig. 62 LLDP Configuration

Tx Interval:	The switch will periodically transmit LLDP frames to its neighbours to ensure the discovery information is kept 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:	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:	When configuration changes are made to a device, a new LLDP frame is transmitted to update its information. The time between the frames being sent will always be at least the value of "Tx Delay". Tx Delay cannot be larger than a ¼ of the Tx Interval value. Valid values are restricted to 1 – 8192 seconds.
Tx Reint:	When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighbouring units, signalling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

Port:	Physical port of the switch.
Mode:	Used to select the LLDP mode for each port. <b>RX Only</b> – The switch will not transmit LLDP frames from this port, but is able to receive LLDP frames from other devices. <b>TX Only</b> – Any received LLDP frames will be dropped, but the switch is able to send LLDP frames. <b>Disabled</b> – The switch will drop incoming LLDP frames and will not transmit LLDP information. <b>Enabled</b> – The switch can send and receive LLDP frames.
CDP Aware:	The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled. Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbours table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbours table. Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbours table. If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbour devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch. Tick the box to enable CDP on each individual port.
Port Descr:	Optional TLV: When checked the "port description" is included in LLDP information transmitted.
Sys Name:	Optional TLV: When checked the "system name" is included in LLDP information transmitted.
Sys Descr:	Optional TLV: When checked the "system description" is included in LLDP information transmitted.
Sys Capa:	Optional TLV: When checked the "system capability" is included in LLDP information transmitted.
Mgmt Addr:	Optional TLV: When checked the "management address" is included in LLDP information transmitted.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

## 1.2.8-2 LLDP Neighbors

This section is used to display the neighbors that have been discovered by the AMS Series switch.

## Web Interface

To view the LLDP neighbors via the Web Interface:

- 1. Click Configuration, LLDP and LLDP Neighbors.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

C 🕺 🗋 192.168.1.1								2 2
ALLOY AMS-24T6SFP	ELLER IS first Records		<b></b>				Auto-Logout OFF	Logout He
¥ System	LIDAN	alabbour	Informatio	-			6.0.0	fresh 🔲 Refresh
<ul> <li>System Information Information</li> </ul>								
Configuration	Local	Chassis	Remote	System	Port	System	System	Management
CPULoad	Port	ID	Port ID	Name	Description OP neighbour info	Capabilities	Description	Address
► Time				NO LLI	or neighbour into	ormation round	and the second sec	
► Account								
► IP								
► Syslog								
► SNMP								
Configuration	-							
▶ Port								
► ACL								
► Aggregation								
<ul> <li>Aggregation</li> <li>Spanning Tree</li> </ul>								
<ul> <li>Aggregation</li> <li>Spanning Tree</li> <li>IGMP Snooping</li> </ul>								
Aggregation     Spanning Tree     IGMP Snooping     MLD Snooping								
Aggregation     Spanning Tree     IGMP Snooping     MLD Snooping     MVR								
Aggregation     Spanning Tree     IGMP Snooping     MLD Snooping     MVR     VLDP								
Aggregation     Spanning Tree     IGMP Snooping     MLD Snooping     MWR     VLDP     LLDP Configuration								
Aggregation     Spanning Tree     IGMP Snooping     MLD Snooping     MVR     VLDP     LLDP Configuration     LLDP Neighbours								
Aggregation     Spanning Tree     IGMP Snooping     MLD Snooping     MLD Snooping     VLDP     LLDP Configuration     LLDP Neighbours     LLDP-MED Configuration								
Aggregation     Spanning Tree     IGMP Snooping     MLD Snooping     MUS nooping     MVR     LLDP Configuration     LLDP Neighbours     LLDP-MED Configuration     LLDP-MED Neighbours	_							
Aggregation     Spanning Tree     IGMP Snooping     MULD Snooping     MVR     VLDP Configuration     LLOP Configuration     LLOP-MED Configuration     LLOP-MED Neighbours     EEE     EEE	_							
Aggregation     Spanning Tree     IGMP Snooping     MLD Snooping     MLD Snooping     MLV R     ULDP     LLDP Configuration     LLDP-MED Neighbours     EEE     Port Statistics	_							
Aggregation     Spanning Tree     IGMP Snooping     MULD Snooping     MVR     VLDP Configuration     LLOP Configuration     LLOP-MED Configuration     LLOP-MED Neighbours     EEE     EEE	_							
Aggregation     Spanning Tree     IGMP Snooping     MLD Snooping     MLD Snooping     MLD Snooping     MUP     LLDP     LLDP Neighbours     LLDP-MED Configuration     LLDP-MED Neighbours     EEE     Port Statistics     Filtering Data Base	_							
Aggregation     Spanning Tree     IGMP Snooping     MULD Snooping     MVR     VLDP Configuration     LLOP Neighbours     LLOP-MED Configuration     LLOP-MED Neighbours     EEE     Port Statistics     Filtering Data Base     VLAN	_							

Fig. 63 LLDP Neighbour Information

Local Port:	The port on which the LLDP frame was received.
Chassis ID:	The Chassis ID is the identification of the neighbours LLDP frames.
Remote Port ID:	The Remote Port ID is the identification of the neighbour port.
System Name:	System Name is the name advertised by the neighbour unit.
Port Description:	Port Description is the port description advertised by the neighbour unit.

System Capabilities:	System Capabilities describes the neighbour unit's capabilities. The possible capabilities are:
	Other, Repeater, Bridge, WLAN Access Point, Router, Telephone, DOCSIS cable device, Station only or Reserved. When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).
System Description:	System Description is the port description advertised by the neighbour unit.
Management Address:	Management Address is the neighbour unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbour's IP address.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.

## 1.2.8-3 LLDP-MED Configuration

Media Endpoint Discovery is an enhancement of LLDP, known as LLDP-MED that provides the following facilities:

Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and Differentiated services (Diffserv) settings) enabling plug and play networking.

Device location discovery to allow creation of location databases and, in the case of Voice over Internet Protocol (VoIP), Enhanced 911 services.

Extended and automated power management of Power over Ethernet (PoE) end points.

Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, and serial or asset number).

This page allows you to configure the LLDP-MED. This function applies to VoIP devices which support LLDP-MED.

## Web Interface

To configure the LLDP-MED parameters via the Web Interface:

- 1. Click Configuration, LLDP and LLDP-MED Configuration.
- 2. Modify the fast repeat setting if required.
- 3. Fill in the required fields for the location parameters.
- 4. Add a new LLDP-MED policy and configured additional settings.
- 5. Assign Policy for required ports.
- 6. Click the Apply button to save your changes or the Reset button to revert to previous settings.

⊂ ff 🗋 192.168.1.1						û 🕏
AMS-24T6SFP			10100 an an a			
AM3-24103FF					Auto-Logout	OFF - Logout Hel
* System	LLDPMED Configur	ation				
▼ System Information	LEDPMED Connigur	auon				
Information Configuration	Fast Start Repeat Count					
CPU Load	Fast start repeat count					
► Time	Past start repeat count	4				
► Account	Coordinates Location					
+ IP						10.00
► Syslog	Latitude	North - Lo	ngitude 0 Ea	st - Altitude 0	Meters •	Map Datum WGS84 •
► SNMP	degrees		degrees			Datum
Configuration	Civic Address Location					
► Port						
ACL     Aggregation	E Country code	61	State	Victoria	County	Australia
<ul> <li>Spanning Tree</li> </ul>	City	Notting Hill	City district	-	Block (Neighbourhood)	
IGMP Snooping	Street	Blackburn	Leading street direction	-	Trailing street suffix	
► MLD Snooping			Construction of the second second	1. Contraction of the second sec		
► MVR	Street suffix	Road	House no.	4/585	House no. suffix	
* LLOP	Landmark	1	Additional location info		Name	
LLDP Configuration	Zip code	1.	Building		Apartment	
LLDP Neighbours LLDP-MED Configuration	Floor		Room no.		Place type	
LLOP-MED Neighbours	Postal community name		P.O. Box		Additional code	
EEE	Postal community name	1	P.O. Box		Additional code	
Port Statistics	Emergency Call Service					
Filtering Data Base	Territoria de la composición de la comp	-				
• VLAN	Emergency Call Service	000				
Voice VLAN     GARP	Policies					
GVRP		In the second		1. Company and the		
+ QoS		Application Type		Priority DSCP		
Thermal Protection	D Vol	ce 💌	Tagged • 1 0	0		

Fig. 64 LLDP-MED Configuration

### Fast Start Repeat Count:

Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbour has been detected in order to share LLDP-MED information as fast as possible to new neighbours.

Because there is a risk of an LLDP frame being lost during transmission between neighbours, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbours receiving the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission will be repeated. The recommended value is 4 times,

given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.

It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.

Latitude:	Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either North of the equator or South of the equator.
Longitude:	Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.
Altitude:	Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters). <b>Meters:</b> Representing meters of Altitude defined by the vertical datum specified.
	<b>Floors:</b> Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.
Map Datum:	The Map Datum is used for the coordinates given in these options:
	<b>WGS84:</b> (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, and Prime Meridian Name: Greenwich.
	NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; the associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).
	NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; the associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Country Code:	The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.			
State:	National subdivisions (state, canton, region, province, prefecture).			
County:	County, parish, gun (Japan), district.			
City:	City, township, shi (Japan) - Example: Melbourne.			
City District:	City division, borough, city district, ward, chou (Japan).			
Block:	Neighbourhood, block.			
Street:	Street name.			
Leading Street Direction: Leading street direction - Example: N.				
Trailing Street suffix:	Trailing street suffix - Example: SW.			
Street Suffix:	Street suffix - Example: Ave			
House No:	House number - Example: 585			
House no. suffix:	House number suffix - Example: A, ½			
Landmark:	Landmark or vanity address - Example: Monash University.			
Additional Location Info: Additional location info - Example: South Wing.				
Name:	Name (residence and/or office occupant) - Example: John Smith			
Zip Code:	Postal/zip code - Example: 3168			
Building:	Building (structure) - Example: Low Library.			
Apartment:	Unit (Apartment, suite) - Example: 4			
Floor:	Floor number.			
Room no:	Room number – Example: 56			
Place Type:	Place Type – Example: Technical Area			
Postal Community Name: Postal community name - Example: Leonia.				
<i>P</i> .O. Box:	Post office box (P.O. BOX) - Example: PO Box 16			
Additional Code:	Additional code - Example: 1320300003			
*Emergency Call Service*: Emergency Call Service (e.g. 000 and others), such as defined by TIA or NENA.

Policies:Network Policy Discovery enables the efficient discovery and diagnosis of<br/>mismatch issues with the VLAN configuration, along with the associated<br/>Layer 2 and Layer 3 attributes, which apply for a set of specific protocol<br/>applications on that port. Improper network policy configurations are a very<br/>significant issue in VoIP environments that frequently result in voice quality<br/>degradation or loss of service. Policies are only intended for use with<br/>applications that have specific 'real-time' network policy requirements, such<br/>as interactive voice and/or video services.

The network policy attributes advertised are:

- 1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
- 2. Layer 2 priority value (IEEE 802.1D-2004)
- 3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

this network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

- 1. Voice
- 2. Guest Voice
- 3. Softphone Voice
- 4. Video Conferencing
- 5. Streaming Video

6. Control / Signalling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Delete:

Click the delete button next to a policy to remove that policy.

Policy ID:ID for the policy. This is auto generated and shall be used when selecting the<br/>policies that shall be mapped to the specific ports.

Application Type: Intended use of the application types:

1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.

2. Voice Signalling (conditional) - for use in network topologies that require a different policy for the voice signalling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.

3. Guest Voice - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.

4. Guest Voice Signalling (conditional) - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.

5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.

6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.

	8. Video Signalling (conditional) - for use in network topologies that require a separate policy for the video signalling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.
Tag:	Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN.
	Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.
	Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.
VLAN ID:	VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003.
L2 Priority:	L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.
DSCP:	DSCP value to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.
Add New Policy:	Click to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Save".
Port:	The port number to which the configuration applies.
Policy ID:	The set of policies that shall apply to a given port. The set of policies is selected by ticking the checkboxes corresponding to the policies.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

# 1.2.8-4 LLDP-MED Neighbors

This page provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbour is detected. This function applies to VoIP devices which support LLDP-MED.

### Web Interface

To view the LLDP-MED neighbors that have been learnt from the switch via the Web Interface:

- 1. Click Configuration, LLDP and LLDP-MED Neighbors.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.



Fig. 65 LLDP-MED Neighbours

### **Parameter Description**

*Port:* The port on which the LLDP frames have been received.

*Device Type:* LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.

LLDP-MED Network Connectivity Device Definition

LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint

	<ul> <li>Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:</li> <li>1. LAN Switch/Router</li> <li>2. IEEE 802.1 Bridge</li> <li>3. IEEE 802.3 Repeater (included for historical reasons)</li> <li>4. IEEE 802.11 Wireless Access Point</li> <li>5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.</li> </ul>
LLDP-MED Endpoint	
<i>Device Definition:</i>	LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework. Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.
	broken into further enapoint Device Classes, as defined in the following.
	Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).
LLDP-MED Generic	
Endpoint (Class I):	The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057. Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.
LLDP-MED Media	
Endpoint (Class II):	The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.

	Discovery services defined in this class include media-type-specific network layer policy discovery.
LLDP-MED	
Communication	
Endpoint (Class III):	The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management.
LLDP-MED	
Capabilities:	LLDP-MED Capabilities describes the neighbourhood unit's LLDP-MED capabilities. The possible capabilities are: 1. LLDP-MED capabilities 2. Network Policy 3. Location Identification 4. Extended Power via MDI – PSE 5. Extended Power via MDI – PD 6. Inventory 7. Reserved
Application Type:	Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.
	1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
	2. Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media.
	3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.

	4. Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media.
	5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.
	6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
	7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
	8. Video Signalling - for use in network topologies that require a separate policy for the video signalling than for the video media.
Policy:	Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown
	<b>Unknown:</b> The network policy for the specified application type is currently unknown. <b>Defined:</b> The network policy is defined.
TAG:	TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged.
	<b>Untagged:</b> The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. <b>Tagged:</b> The device is using the IEEE 802.1Q tagged frame format.
VLAN ID:	VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.
Priority:	Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).
DSCP:	DSCP is the DSCP value to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).

*Auto*-Refresh: Tick the box to enable the information to be automatically refreshed.

*Refresh:* Used to manually refresh the information on the page.

## 1.2.8-5 EEE

This page provides an overview of EEE information exchanged by LLDP.

### Web Interface

To view the LLDP EEE information that has been discovered from the switch via the Web Interface:

- 1. Click Configuration, LLDP and EEE.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

AMS-24T6SFP ×	00
- C f 192168.1.1	· · · · · · · · · · · · · · · · · · ·
AMS-24T6SFP	Auto-Logout OFF C Logout He
System	
* System Information	LLDP Neighbors EEE Information Auto-retresh
Information Configuration CPU Load	Local Port Tx Tw Rx Tw Fallback Receive Tw Echo Tx Tw Echo Rx Tw Resolved Tx Tw Resolved Rx Tw EEE activated No LLDP EEE information found
► Time	
+ Account	
► IP	
Syslog	
► SNMP	
Configuration	
Port	
► ACL	
<ul> <li>Aggregation</li> </ul>	
Spanning Tree	
IGMP Snooping	
MLD Snooping	
► MVR ▼ LLDP	
LLDP Configuration	
LLDP Neighbours	
LLDP-MED Configuration	
LLDP-MED Neighbours	
EEE	
Port Statistics	
Filtering Data Base	
► VLAN	
Voice VLAN	
- GARP	
GVRP	
+ QoS	
Thermal Protection	
► sFlow Agent	71

Fig. 66 LLDP EEE Information

Local Port:	The port on which the LLDP EEE information frames have been transmitted or received.
Tx Tw:	The link partner's maximum time that the transmit path can hold off sending data after reassertion of LPI.
Rx Tw:	The link partner's time that the receiver would like the transmitter to hold off to allow time for the receiver to wake from sleep.
Fallback Receive Tw:	The link partner's fallback receive Tw. A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for

	savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.
Echo Tx Tw:	The link partner's Echo Tx Tw value. The respective echo values shall be defined as the local link partner's reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.
Echo Rx Tw:	The link partner's Echo Rx Tw value.
Resolved Tx Tw:	The resolved Tx Tw for this link. Note: NOT the link partner the resolved value that is the actual "tx wakeup time" used for this link (based on EEE information exchanged via LLDP).
Resolved Rx Tw:	The resolved Rx Tw for this link. Note: NOT the link partner the resolved value that is the actual "rx wakeup time" used for this link (based on EEE information exchanged via LLDP).
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.

## **1.2.8-6 Port Statistics**

This section displays two types of counters. Global counters are counters that refer to the whole switch, while local counters refer to per port counters for the currently selected switch.

#### Web Interface

To view the LLDP Port Statistics from the switch via the Web Interface:

- 1. Click Configuration, LLDP and Port Statistics.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

AM5-24165FP ×									<u>ن</u>
C II [] 192-100-1.1									M 3
ALLON/	-	_		_					
ALLOY	ALLOY Differ Manual		-			- Hard Contractor			
			CCCC			and the second se			
AMS-24T6SFP								Auto-Logout OF	F 🖌 Logout He
System	-								
▼ System Information								Auto-refresh	Retresh Clear
Information			Global Cour	tare					
Configuration	Neinhbour or	tries were las			00 (3615821 sec. ago)				
CPU Load		ours Entries A			0				
► Time		ours Entries D			0				
► Account		ours Entries D			0				
► IP		ours Entries A			0				
► Syslog									
► SNMP	LLDP Stat	Intian							
Configuration	LLOP Stat	ISUCS							
• Port					Local Counters				
- ACL	Local Port	Tx Frames	<b>Rx Frames</b>	Rx Errors		TLVs Discarded	<b>TLVs Unrecognized</b>	Age-Outs	
Aggregation	1	1	ú	0	0	0	0	0	
Spanning Tree	2	0	0.	0	a	0	D	0	
► IGMP Snooping	3	Ó	à	0	0	0	0	Ó	
MLD Snooping	4	0	0	0	0	0	0	0	
► MVR	.5	0	0	0	0	0	0	0	
* LLOP	6	0	0	0	0	0	0	0	
LLDP Configuration	7	0	0	0	0	0	0	0	
LLDP Neighbours	8	0	.0	0	0	0	0	0	
LLDP-MED Configuration	9	0	0	0	0	0	0	0	
LLOP-MED Neighbours	10	0	u 0	0	0	0	0	0	
EEE	12	0	0	0	0	0	0	0	
Port Statistics	13	0	0	0	0	0	0	0	
Filtering Data Base	14	0	0	0	0	0	0	0	
► VLAN	15	0	Ű.	0	0	0	0	0	
► Voice VLAN	16	0	0	0	0	0	0	0	
► GARP	17	0.	0.	0	0	0	0	0	
► GVRP	18	0	0	0	0	D	0	0	
+ QoS	19	Ú	ú	0	D	0	0	Û	
Thermal Protection	20	0	0	0	0	0	D	:0	
EFlow Agent	7 . 74	0	0	0	0	0	0	0	

Fig. 67 LLDP Port Statistics

Neighbour 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 Neighbours Entries Added:	Shows the number of new entries added since switch reboot.
Total Neighbours Entries Deleted:	Shows the number of new entries deleted since switch reboot.

AMS User Manual

Total Neighbours Entries Dropped:	Shows the number of new entries dropped since switch reboot.
Total Neighbours Entries Aged Out:	Shows the number of entries deleted due to Time-To-Live expiring.
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 an 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 Neighbours" 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.
TLV's 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.
TLV's Unrecognised:	The number of well-formed TLVs, but with an unknown type value.
Org. Discarded:	The number of organizationally received TLVs
Age-Outs:	Each LLDP frame contains information about how long 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.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.

# 1.2.9 Filtering Data Base

Switching of frames is based upon the Destination MAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the Destination MAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the Destination MAC address and switch ports. The frames also contain a Source MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time.

# 1.2.9-1 Configuration

This section is used to configure MAC Address settings on the AMS Series switches.

### Web Interface

To configure the MAC filtering parameters via the Web Interface:

- 1. Click Configuration, Filtering Database and Configuration.
- 2. Specify the Disable Automatic Aging and Aging Time.
- 3. Change the way individual ports can learn MAC Address information.
- 4. Configure static MAC Address entries if required.

- 8 - 8
승 💩 🛎
Auto-Logout OFF • Logout Help 3(28)

Fig. 68 MAC Filtering Configuration

Aging Configuration:	By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging. Configure aging time by entering a value here in seconds. The allowed range is 10 to 1000000 seconds. Disable the automatic aging of dynamic entries by checking Disable automatic aging.					
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:	Learning is done automatically as soon as a frame with unknown SMAC is received.					
Disable:	MAC Addresses will not be learnt.					
Secure:	Only static MAC entries are learned, all other frames are dropped.					
i	<b>NOTE:</b> Make 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.					
MAC Address Table:	The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries. The MAC table is sorted first by VLAN ID and then by MAC address.					
Delete:	Check to delete the entry. It will be deleted during the next save.					
VLAN ID:	The VLAN ID of the entry.					
MAC Address:	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.					
Add new Static Entry:	Click to add a new static MAC entry.					
Reset Button:	Used to reset unsaved changes to original configuration.					
Apply Button:	Used to save the settings configured on this page.					

# 1.2.9-2 Dynamic MAC Table

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

### Web Interface

**Parameter Description** 

To view the MAC Address that have been learnt by the switch via the Web Interface:

- 1. Click Configuration, Filtering Database and Dynamic MAC Table.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

C fi 192.168.1.1										17 B
ALLOY	BLUETY Birther Barnet		C. MARKET	* *			10	HACODE		
	Spectary.			104	1.0			Real Property lies		A COLOR OF A COLOR
AMS-24T6SFP										Auto-Logout OFF 💽 Logout He
configuration	.1									
CPU Load	MAC AC	dres	s Table							Auto-refresh Refresh Clear IKK >>
► Time										Contraction According Colonial According
► Account	Start from V	LAN 1	and MAC a	ddress	00-00	-00-00-00-00	with 20	entries p	ber page.	
► IP										
► Syslog	Trees	VLAN	MAR Adda	enul	a Islai	Alelalelala		embers	19 20 21 22 23 24 25	25
► SNMP			00-00-8C-00-00-F2		1 23	applylelal	10 11 12 13 1	4 15 10 17 10	19 20 21 22 23 24 25	20
Configuration	Static	1								
► Port	Dynamic	1	00-00-8C-00-C8-20							
► ACL	Dynamic	1	00-08-78-08-6E-DC							
<ul> <li>Aggregation</li> </ul>	Dynamic	1	00-08-98-C9-A7-FA							
Spanning Tree	Dynamic	1	00-08-EA-00-59-A7							
IGMP snooping	Dynamic	1	00-0F-EA-57-2E-98							
MLD Snooping	Dynamic	1	00-1A-4D-43-26-4D							
MVR	Dynamic		00-1D-7D-01-CB-86							
+ LLDP		-								
Filtering Data Base	Dynamic	1	00-1F-D0-8D-71-C6	-						
Configuration	Dynamic	1	00-1F-D0-D1-F7-67							
Dynamic MAC Table VLAN	Dynamic	1	00-20-85 FB-0C-D3							
VLAN Voice VLAN	Dynamic	1	00-24-1D-16-87-5F							
GARP	Dynamic	1	00-24-1D-1D-95-D2							
GVRP	Dynamic	1	00-24-1D-1F-28-82							
- QoS	Dynamic	+	00-24-10-1E-E5-DC							
Thermal Protection	Dynamic		00-24-10-70-AB-FD							
sFlow Agent	and the second sec	-	00-24-10-8A-64-19							
Loop Protection	Dynamic	1								
Single IP	Dynamic	1	00-26-F0-48-36-48							
Easy Port	Dynamic	1	00-50-56-AC-04-EF							
Mirroring	Dynamic	1	00-50-56-AC-04-F5							
Trap Event Seventy SMTP Configuration UPnP	1.1									

### Fig. 69 MAC Address Table

Туре:	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.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.
<<, >>:	The arrow keys are used to navigate between the pages, displaying the current VLAN's configured on the switch.

# 1.2.10 VLAN

The virtual LAN (VLAN) allows you to group physically separate users into the same broadcast domain. The use of VLANs improves security, segmentation, and flexibility. The use of VLANs also decreases the cost of arranging users, because no extra cabling is required.

VLANs allow an administrator to define user groups logically rather than by their physical locations. For example, you can arrange user groups such as accounting, engineering, and finance rather than grouping everyone on the first floor, everyone on the second floor, and so on.

- VLANs define broadcast domains that can span multiple LAN segments.
- VLAN segmentation is not bound by the physical location of users.
- Each switch port can be assigned to only one VLAN.
- Ports not assigned to the same VLAN do not share broadcasts, improving network performance.
- A VLAN can exist on one switch or on multiple switches.
- VLANs can connect across wide-area networks (WANs). The figure shows a VLAN design. VLANs are defined by user functions rather than locations.

Each VLAN on a switch behaves as if it were a separate physical bridge. The switch forwards packets (including unicasts, multicasts, and broadcasts) only to ports assigned to the same VLAN from which it originated. This reduces on network traffic. VLANs require a trunk to span multiple switches. Each trunk can carry traffic for multiple VLANs.

# 1.2.10-1 VLAN Membership

This section is used to configure VLAN settings on the AMS Series switches. Here you can create VLAN's and assign ports into specific VLAN groups. The maximum n umber of VLAN groups that can be created is 4096.

### Web Interface

To configure the VLAN settings via the Web Interface:

- 1. Click Configuration, VLAN and VLAN Membership.
- 2. Click Add New VLAN to add additional VLAN groups.
- 3. Give the VLAN group a name and assign a VLAN ID (2 4096) for the group.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.

- C f () 192.168.1.1		습 <b>원</b>
AMS-24T6SFP		Auto-Logout OFF 💌 Logout Hel
Configuration	VLAN Membership Configuration	Refresh lice 33
> ACL	VLAN Membership Comgutation	Refreah.   KC   3.8
► Aggregation	Start from VLAN 1 with 20 entries per page.	
+ Spanning Tree	and a second sec	
► IGMP Snooping	and the second sec	Port Members
MLD Snooping		5 8 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
MVR	1 detaut 222	i de la
LLOP		
Filtering Data Base	Add New VLAN	
VLAN	CONTRACTOR (STORING	
VLAN Membership	Apply Reset	
Ports Switch Status		
Port Status		
Private VLANs		
MAC-based VLAN		
Protocol-based VLAN		
Voice VLAN		
GARP		
GVRP		
Qos		
Thermal Protection		
sFlow Agent		
Loop Protection		
Single IP		
Easy Port		
Mirroring Trap Event Seventy		
SMTP Configuration		
UPnP		
Security		
Maintenance	1	

Fig. 70 VLAN Membership

Delete:	To delete a VLAN entry, tick the check box next to the corresponding VLAN entry. After you press the Apply the entry will be deleted.
VLAN ID:	The VLAN ID of the entry.
VLAN Name:	Enter a descriptive name for the VLAN. VLAN Names can contain alphanumeric characters.
Port Members:	A row of check boxes for each port is displayed for each VLAN ID. To include a port in a VLAN, check the box. To remove or exclude the port from the VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Adding a New VLAN:	Click to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4095.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

# 1.2.10-2 Ports

This section is used to configure Port specific parameters for your VLAN's. Here we can configure a port as a Tagged (Trunk) or Untagged (Access) port or as a Hybrid port allowing both tagged and untagged frames.

### Web Interface

To configure the Port settings via the Web Interface:

- 1. Click Configuration, VLAN and Ports.
- 2. Configure the parameters required for all ports.
- 3. Click the Apply button to save your changes or the Reset button to revert to previous settings.

AMS-24T6SEP ×	-			-		1			
- C 🕺 🗋 192.168.1.1								4	1
ALLOY	( ALLON	-					Nation and		
	Married Street								
AMS-24T6SFP	_	_		-				Auto-Logout OFF - Logout	He)p
Configuration									
► Port	Ether	type for Cu	stom S-ports 0x	( 38A8					
► ACL		00.00							
Aggregation     Spanning Tree	VLAN	Port Config	guration						
IGMP Snooping	Port	Port Type	Ingress Filtering	Frame	Type	Egress Rule	PVID		
MLD Snooping	2	0 .		0		0 .			
► MVR	1	Unaware	1 11	All		Hybrid -	1		
► LLOP		Unaware .		All		Hybrid •			
► Filtering Data Base					- And		1		
* VLAN	-	Unaware		All		Hybrid 💌	1		
VLAN Membership Ports	-4	Unaware .		All	٠	Hybrid •	1		
Switch Status	5	Unaware	0 1	All		Hybrid •	1		
Port Status	6	Unaware .		All	-	Hybrid +	1		
Private VLANs	7	Unaware .	1 /1	All		Hybrid 💌	1		
MAC-based VLAN	-	Unaware -	J	All	-	Hybrid +			
► Protocol-based VLAN					1.00				
Voice VLAN     GARP	.9	Unaware .		All	-	Hybrid 💌	1		
+ GVRP	e 10	Unaware -		All	-	Hybrid 🖛	1		
+ Gos	11	Unaware -	1 11	All		Hybrid 💌	- 1		
Thermal Protection	12	Unaware .		AJI	-	Hybrid -	1		
sFlow Agent	13	Unaware		All		Hybrid •	1		
Loop Protection	14	Unaware -		AJI	-	Hybrid +	4		
Single IP     Easy Port		Unaware		All		Hybrid -			
Mirroring				-	( and		1		
Trap Event Seventy				All		Hybrid 💌			
SMTP Configuration	17	Unaware		ILA	•	Hybrid 💌	1		
UPnP	18	Unaware		All		Hybrid 💌	1		
- Security Maintenance	19	Unaware .	1 🗆	All		Hybrid •	1		

Fig. 71 VLAN Port Configuration

### **Parameter Description**

*Ethertype for Custom S-Ports:* This field specifies the ether type used for Custom S-ports. This is a global setting for all the Custom S-ports. Custom Ethertype enables the user to change the Ethertype value on a port to any value to support network devices that do not use the standard 0x8100 Ethertype field value on 802.1Q-tagged or 802.1p-tagged frames.

*Port:* Physical port of the switch.

Port Type:There are several port types that can be selected depending on the role of<br/>the port. The port type available are Unaware, (Customer) C-Port, (Service)<br/>S-Port and S-Custom Port:

**Unaware** – This port type can be used when the configured port is an untagged port. All received packets will be tagged with the corresponding PVID.

This port type can also be used when using Q-in-Q VLAN's as this port type will allow a Tagged Port to re-Tagged for Q-in-Q, as long as the TPID is 0x8100. (Standard 802.1q valid Ethernet Frame)

If the frame received has a TPID of 0x88A8 (Standard 802.1ad Q-in-Q Frame) it will be discarded.

When the frame leaves the switch the TPID will be set to 0x8100.

**C-Port** – This port type can be used when the configured port is an untagged port. All received packets will be tagged with the corresponding PVID. This port can also be used for Tagged Ports. If the frame received has a TPID of 0x8100 (Standard 802.1q valid Ethernet Frame) it will be forwarded. If the frame received has a TPID of 0x88A8 (Standard 802.1ad Q-in-Q Frame) it will be discarded.

When the frame leaves the switch the TPID will be set to 0x8100.

S-Port – This port type can be used when the configured port is an untagged port. All received packets will be tagged with the corresponding PVID.
This port can also be used for Tagged Ports. If the frame received has a TPID of 0x88A8 (Standard 802.1ad Q-in-Q Frame) it will be forwarded.
If the frame received has a TPID of 0x8100 (Standard 802.1q valid Ethernet Frame) it will be discarded.

When the frame leaves the switch the TPID will be set to 0x88A8.

**S-Custom-Port** – This port type can be used when the configured port is an untagged port. All received packets will be tagged with the corresponding PVID.

This port can also be used for Tagged Ports. If the frame received has a TPID of 0x88A8 (Standard 802.1ad Q-in-Q Frame) it will be forwarded.

If the frame received has a TPID of 0x8100 (Standard 802.1q valid Ethernet Frame) it will be discarded.

When the frame leaves the switch the TPID will be set to The Ethertype specified in the **Ethertype for Custom S-Ports** field.

*Ingress Filtering:* Enable ingress filtering on a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is

	not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled.
Frame Type:	Determines whether the port accepts all frames or only tagged/untagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, the field is set to All.
Egress Rule:	This field determines what happens to the frames that leave and are received by the configured ports. There are three options Hybrid, Access and Trunk.
	<b>Hybrid</b> – The Hybrid port type will allow both untagged and tagged packets to be sent/received by the port. Use this port type when connecting to VLAN-unaware or VLAN-aware devices.
	Access – The Access port type will only allow untagged packets to be sent/received from the port. Use this port type when connecting to VLAN-unaware devices.
	<b>Trunk</b> – The Trunk port type will only allow tagged packets to be sent/received from the port. Use this port type when connecting to VLAN-aware devices.
PVID:	Configure the VLAN identifier for the port. The allowed values are 1 through 4095. The default value is 1.
i	<b>NOTE:</b> The port must be a member of the same VLAN as the Port VLAN ID.
Reset Button:	Used to reset unsaved changes to original configuration.

Apply Button: Used to save the settings configured on this page.

### 1.2.10-3 Switch Status

This section is used to view the currently configured VLAN groups. VLAN groups which have been learnt from other protocols such as GVRP can also be viewed here.

#### Web Interface

To view the current VLAN groups via the Web Interface:

- 1. Click Configuration, VLAN and Switch Status.
- 2. If you want to view specific VLAN groups based on a particular protocol, select the protocol from the drop down box near the top of the page. Only VLAN groups relating to that protocol will be displayed.
- 3. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 4. Click Refresh to manually refresh the information.

T AMS-24T6SEP		- D - X
← → C fi 192.168.1.1		순 😼 着
AUXIC ALL SEP CAUSE ALL SEP ACC ACC ACC ACC ACC ACC ACC AC	Image: State Stat	Auto-Logout OFF Lugout Hele Combined Auto-raitesh Ratesh NAS GVRP Voice VLAN Voice VLAN Voice VLAN Voice VLAN

Fig. 72 VLAN Status

#### Parameter Description

*VLAN ID:* Indicates the VLAN ID of the particular entry.

- Port Members:Displays the port members that belong to a particular VLAN group. If the<br/>check box it ticked it means that port belongs to that VLAN group.
- *Auto*-Refresh: Tick the box to enable the information to be automatically refreshed.

### *Refresh:* Used to manually refresh the information on the page.

<<, >>: The arrow keys are used to navigate between the pages, displaying the current VLAN's configured on the switch.

## 1.2.10-4 Port Status

This section is used to view the port specific values relating to the VLAN information.

#### Web Interface

To view the current Port Information via the Web Interface:

- 1. Click Configuration, VLAN and Port Status.
- 2. If you want to view specific Port information based on a particular protocol used, select the protocol from the drop down box near the top of the page. Only Port Information relating to that protocol will be displayed.
- 3. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 4. Click Refresh to manually refresh the information.

- C ń 🗄 192.168.1.1	_	_					_		순 🌹
ALLOY	ALLON Million Million Malana		72			1	ears.of	1127	
	and the second			10100 (	*****		ŵ ŵn		
AMS-24T6SFP						_			Auto-Logout OFF . Logout He
Configuration									
► Port	VLAN	Port	Status fo	r Static user					Static + Auto-refresh Refresh
► ACL									Static
► Aggregation	Port	PVID		Ingress Filtering		Tx Tag	UVID	Conflicts	NAS
Spanning Tree	1	1	UnAware	Disabled		Untag_this	1	No	GVRP
► IGMP Snooping	2	1	UnAware	Disabled	All	Untag this	1	Na	MVR Voice VLAN
MLD Snooping	3.	- 1	UnAware UnAware	Disabled Disabled		Untag this Untag this	- 1	No	MSTP
MVR	5	1	UnAware	Disabled		Untag this		No	VOL
LLDP	5	1	UnAware	Disabled		Untag this	1	No	Combined
Filtering Data Base	7	1	UnAware	Disabled		Lintag this	1	No	
VLAN	8	1	UnAware	Disabled	IA.	Untag this	1	No	
VLAN Membership	9	1	UnAware	Disabled		Untag this	1	Na	
	10	1	UnAware	Disabled		Untag this	1	No	
Ports	11	-1	Un/ware	Disabled		Untag_this	1	No	
Switch Status	12	1	UnAware	Disabled		Untag_this	1	No	
Port Status	13	1	UnAware UnAware	Disabled Disabled	Al	Untag this Untag this	- 1	No	
► Private VLANs	14		UnAware	Disabled		Untag this		No	
MAC-based VLAN	16		UnAware	Disabled		Untag this		Na	
Protocol-based VLAN	17	1	UnAware	Disabled		Untag this	÷.	No	
Voice VLAN	18	1	UnAware	Disabled		Untag this	1	No	
GARP	19	1	UnAware	Disabled		Untag this	1	No	
GVRP	20	1	UnAware	Disabled		Untag this	1	No	
QoS	21	1	UnAware	Disabled		Untag_this	1	No	
Thermal Protection	22	1	UnAware	Disabled		Untag_this	1	No	
sFlow Agent	23	- 1	UnAware UnAware	Disabled Disabled		Untag_this	1	Na	
Loop Protection	24 25	1	UnAware	Disabled		Untag_this Untag_this	-	No	
Single IP	26	1	UnAware	Disabled		Untag this	1	No	
Easy Port	20	_	Confinance	Disabled	74	ouned one	-	102	
Mirroring									
Trap Event Seventy									
SMTP Configuration									
Security Maintenance									

Fig. 73 Port Information

#### Parameter Description

*Port:* Physical port of the switch.

PVID: Shows the VLAN identifier for that port. The allowed values are 1 through 4095.The default value is 1.

Port Type:	Displays the currently configured port type, values are unaware, C-Port, S-Port and S-Custom-Port. For a full explanation of these parameters see section 1.2.10-2.
Ingress Filtering:	Displays whether the port has ingress filtering enabled or disabled.
Frame Type:	Displays what type of packets can be received by the port, Tagged, Un- Tagged or All.
Tx Tag:	Displays whether outgoing packets are tagged or untagged.
UVID:	Displays the UVID (Untagged VID). A port UVID determines how the packet will be handled when leaving the switch.
Conflicts:	Displays whether any VLAN based conflicts have occurred. Conflicts can occur when Dynamic VLAN's are being used.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.

# 1.2.10-5 Private VLAN

A private VLAN allows the administrator to configure a VLAN which contains switch ports that are restricted, such that they can only communicate with a given uplink port. The restricted ports are called private ports. Each private VLAN typically contains many private ports, and a single uplink. The uplink will typically be a port (or link aggregation group) connected to a router, firewall, server, provider network, or similar central resource.

The switch forwards all frames received on a private port out the uplink port, regardless of VLAN ID or destination MAC address. Frames received on an uplink port are forwarded in the normal way (i.e., to the port hosting the destination MAC address, or to all VLAN ports for unknown destinations or broadcast frames). Traffic from individual ports are blocked from communicating with each other, all ports can only communicate with the uplink port.

### 1.2.10-5-1 Private VLAN Membership

The Private VLAN membership configurations for the switch can be monitored and configured here. Private VLAN's can be added or deleted and port members of each Private VLAN can be added or removed here. Private VLAN's are based on the source port mask, and there are no connections to VLAN's. This means that VLAN ID's and Private VLAN ID's can be identical. A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1. A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLAN's.

### Web Interface

To configure the Private VLAN Membership settings via the Web Interface:

- 1. Click Configuration, VLAN, Private VLAN's and Private VLAN Membership.
- 2. To add a new Private VLAN click "Add New Private VLAN".
- 3. Specify the Private VLAN ID and Port Members.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Fig. 74 Private VLAN Membership

Delete:	To delete a Private VLAN entry, tick the box and press the Apply button.
PVLAN ID:	Indicates the VLAN ID of the private VLAN.
Port Members:	Displays the port members that belong to a particular VLAN group. If the check box it ticked it means that port belongs to that VLAN group.
Add New Private VLAN:	Click to add a new private VLAN. An empty row is added to the table, and the private VLAN can be configured as needed.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

### 1.2.10-5-2 Port Isolation

Port Isolation allows the administrator to configure ports so they can only communicate with certain ports, even though they are in the same VLAN group. A typical scenario is where you need to block all ports from communicating with each other, but allow all ports to communicate with a single uplink port. This section is used to configure how each port will communicate with other ports within the same private VLAN.

### Web Interface

To configure the Port Isolation settings via the Web Interface:

- 1. Click Configuration, VLAN, Private VLAN's and Port Isolation.
- 2. Tick the box next to the corresponding port to enable port isolation.
- 3. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Fig. 75 Port Isolation

Port Members:	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.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

AMS User Manual

# 1.2.10-6 MAC-based VLAN

One of the most common ways of grouping VLAN members is by port, hence the name port-based VLAN. Typically, the device adds the same VLAN tag to untagged packets that are received through the same port. Later on, these packets can be forwarded in the same VLAN. Port-based VLAN's are easy to configure, and applies to networks where the locations of terminal devices are relatively fixed. As mobile office and wireless network access gain more popularity, the ports that terminal devices use to access the networks are very often non-fixed. A device may access a network through Port A this time, but through Port B the next time. If Port A and Port B belong to different VLANs, the device will be assigned to a different VLAN the next time it accesses the network. As a result, it will not be able to use the resources in the old VLAN. On the other hand, if Port A and Port B belong to the same VLAN, after terminal devices access the network through Port A do, which brings security issues. To provide user access and ensure data security in the meantime, the MAC-based VLAN technology was developed.

MAC-based VLAN's, group VLAN members by MAC address. With MAC-based VLAN configured, the device adds a VLAN tag to an untagged frame according to its source MAC address. MAC-based VLANs are mostly used in conjunction with security technologies such as 802.1X to provide secure, flexible network access for terminal devices.

### 1.2.10-6-1 Configuration

The MAC-based VLAN entries can be configured here. This page allows for adding and deleting MACbased VLAN entries and assigning the entries to different ports. This page shows only static entries.

### Web Interface

To configure MAC-based VLAN settings via the Web Interface:

- 1. Click Configuration, VLAN, MAC-based VLAN's and Configuration.
- 2. Specify the MAC Address and VLAN ID.
- 3. Click the Apply button to save your changes or the Reset button to revert to previous settings.

- C fi 🗋 192.168.1.1		देवे <b>9</b> 2
AMS-24 T6 SFP • rort • ACL		Auto-Logout OFF 💿 Logout Help
Aggregation	MAC-based VLAN Membership Configuration	Refresh  << >>
Spanning Tree     IGMP Snooping     MLD Snooping	Delete         MAC Address         VLAN ID         12 3 4 5 6 7 8 9 10 11 2 3 14 15 16 17 18 19 20 2           Currently no entries present	21 22 23 24 25 26
► MVR	Add new entry	
LLDP     Filtering Data Base	Coverney entry	
VLAN Membership Ports Switch Status Port Status Port Status VLAN VLANS VMAC-based VLAN Configuration Status Protocol-based VLAN Voice VLAN GARP GARP GARP GVRP GOS Thermal Protection Single IP	(Apply) [Reset]	

Fig. 76 MAC-based VLAN Configuration

Delete:	To delete a MAC-based VLAN entry, check this box and press Apply. The entry will be deleted on the selected switch.
MAC Address:	Indicates the MAC Address.
VLAN ID:	Indicates the VLAN ID.
Port Members:	A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Add New Entry:	Click to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095.
	The MAC-based VLAN entry is enabled on the selected switch unit when you click on "Apply". A MAC-based VLAN without any port members on any unit will be deleted when you click "Apply".
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

### 1.2.10-6-2 Status

This section displays the current MAC-based VLAN groups configured on the switch.

#### Web Interface

To view the MAC-based VLAN groups via the Web Interface:

- 1. Click Configuration, VLAN, MAC-based VLAN's and Status.
- 2. Select to view Combined, Static or NAS based MAC entries by using the drop down box near the top of the screen.
- 3. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 4. Click Refresh to manually refresh the information.



Fig. 77 MAC-based VLAN Status

MAC Address:	Indicates the MAC Address.
VLAN ID:	Indicates the VLAN ID.
Port Members:	Port members of the Mac-based VLAN entry.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.

# 1.2.10-7 Protocol-based VLAN

This section describes Protocol -based VLAN, the AMS Series support Protocols including Ethernet LLC and SNAP.

## LLC

The Logical Link Control (LLC) data communication protocol layer is the upper sub-layer of the Data Link Layer (which is itself layer 2, just above the Physical Layer) in the seven-layer OSI reference model. It provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, Decnet and Appletalk) to coexist within a multipoint network and to be transported over the same network media, and can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

### SNAP

The Subnetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier spaces. It is used with IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11 and other IEEE 802 physical network layers, as well as with non-IEEE 802 physical network layers such as FDDI that use 802.2 LLC.

### 1.2.10-7-1 Protocol to Group

This page allows you to add new Protocols to Group Name (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the selected switch.

### Web Interface

To configure protocol to group mapping settings via the Web Interface:

- 1. Click Configuration, VLAN, Protocol-based VLAN's and Protocol to Group.
- 2. Click Add New Entry and specify the Frame Type, Ethertype Value and give the group a name.
- 3. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Fig. 78 Protocol-based VLAN's

Delete:	To delete a Protocol-based VLAN entry, check this box and press Apply. The entry will be deleted on the selected switch.
Frame Type:	Select the frame type for the group, valid values are Ethernet, LLC and SNAP.
	<b>NOTE:</b> Once you change the Frame type field, the valid value of the following text field will vary depending on the new frame type you have selected.
Value:	Valid values that can be entered in this text field depends on the option
vulue.	selected from the preceding Frame Type selection menu.
	Below is the criteria for three different Frame Types:
	<b>Ethernet</b> : Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff
	<b>LLC</b> : Valid value in this case is comprised of two different sub-values.
	a. DSAP: 1-byte long string (0x00-0xff)
	b. SSAP: 1-byte long string (0x00-0xff)
	<b>SNAP</b> : Valid value in this case also is comprised of two different sub-values.

	a. OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.
	b. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.
	In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.
Group Name:	A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers (0-9).
Add New Entry:	Click to add a new entry to the mapping table, enter the required field based on the frame type you have selected.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.
Refresh:	Used to manually refresh the information on the page.

### **1.2.10-7-2** Group to VLAN

This section is used to map the groups configured in section 1.2.10-7-1 to a VLAN Group.

### Web Interface

To map the protocol group to a VLAN group via the Web Interface:

- 1. Click Configuration, VLAN, Protocol-based VLAN's and Group to VLAN.
- 2. Specify the Group Name and enter a valid VLAN ID.
- 3. Select the required ports for the group, by ticking the check box corresponding to the port number.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Fig. 79 Group to VLAN Mapping

#### **Parameter Description**

Delete:	To delete a Group Name to VLAN entry, check this box and press Apply. The entry will be deleted on the selected switch.
Group Name:	A valid Group Name is a string of up to 16 characters, which consists of a combination of alphabets (a-z or A-Z) and integers (0-9), no special characters are allowed. When entering a Group Name the Group Name

must first exist in the Protocol to Group section.

VLAN ID:	Indicates the ID to which the Group Name will be mapped. A valid VLAN ID ranges from 1-4095.
Port Members:	A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Add New Entry:	Click to add a new entry to the mapping table. An empty row is added to the table, the Group Name, VLAN ID and port members can be configured as needed.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.
Refresh:	Used to manually refresh the information on the page.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.

# 1.2.11 Voice VLAN

The Voice VLAN function is used for networks where both data and voice traffic are running on the same network. By using a dedicated VLAN for voice traffic it allows the administrator to prioritize this traffic to ensure voice quality is kept to an optimum level.

# 1.2.11-1 Configuration

This section is used to configure the Voice VLAN settings on the AMS Series switches. The voice VLAN feature enables access ports to carry IP voice traffic from an IP phone. When the switch is connected to an IP Phone, the phone can send voice traffic with Layer 3 IP precedence and Layer 2 class of service (CoS) values. Because the sound quality of an IP phone call can deteriorate if the data is unevenly sent, the switch supports quality of service (QoS) based on IEEE 802.1p CoS. QoS uses classification and scheduling to send network traffic from the switch in a predictable manner.

The Voice VLAN QoS functionality is only applicable to IP Phones that support tagging of traffic with IP Precedence or CoS QoS values. Most IP Phones will support this feature and must be configured to do so correctly.

### Web Interface

To configure the Voice VLAN settings via the Web Interface:

- 1. Click Configuration, Voice VLAN and Configuration.
- 2. Enable the Voice VLAN from the drop box labelled Mode.
- 3. Specify the appropriate VLAN ID, Aging Time and Traffic Class.
- 4. Configure the individual port settings as required.
- 5. Click the Apply button to save your changes or the Reset button to revert to previous settings.
| C fi 🗋 192.168.1.1                            |   |                      |  |             |         |                |                |                | 公 4      | 2 =  |
|---|---|----------------------|--|-------------|---------|----------------|----------------|----------------|----------|------|
| ALLOY   | ALC'Y<br>North Contract   | -                    |  |             | 111     |                | Hissman<br>R R |                |          |      |
| AMS-24T6SFP                                   |   |                      | and the second   |             | -       | and the second |                | Auto-Logout OF | Logout H | lelp |
| ► Time  | ÷   |                      |  |             |         |                |                |                |          |      |
| ► Account                                     | Voice   | VLAN C               | onfigurati   | ion         |         |                |                |                |          |      |
| ► IP  | Mode  |                      | isabled  | *           |         |                |                |                |          |      |
| <ul> <li>Syslog</li> <li>SNMP</li> </ul>      | VLAN  |                      | 000  | 1.1         |         |                |                |                |          |      |
| Configuration                                 |   |                      |  |             |         |                |                |                |          |      |
| ► Port  | Aging   | Participation of the | i de la compañía de la | conds       |         |                |                |                |          |      |
| - ACL   | Traffi  | c Class 7            | (High)   |             |         |                |                |                |          |      |
| ► Aggregation                                 |   |                      |  |             |         |                |                |                |          |      |
| Spanning Tree                                 |   |                      |  |             |         |                |                |                |          |      |
| ► IGMP Snooping                               | Port  | Configur             | ation  |             |         |                |                |                |          | =    |
| <ul> <li>MLD Snooping</li> <li>MVR</li> </ul> | Port  | Mode                 | Security   | Discovery P | rotocol |                |                |                |          |      |
| + LLDP  | *   | 0 1                  | 0 .  | 0           | *       |                |                |                |          |      |
| ► Filtering Data Base                         | 1   | Disabled -           | Disabled -   | OUI         | -       |                |                |                |          |      |
| ► VLAN  | 4   | Disabled -           | Disabled •   | OUI         | -       |                |                |                |          |      |
| Voice VLAN                                    | and the second se |                      | and the second second  | OUI         |         |                |                |                |          |      |
| Configuration                                 | 3   | Disabled ¥           | a contract of the second   |             |         |                |                |                |          |      |
| ► GARP  | n <u>4</u>  | Disabled -           | Disabled .   | OUI         |         |                |                |                |          |      |
| ► GVRP  | 5   | Disabled 💌           | Disabled 💌   | OUI         |         |                |                |                |          |      |
| + QoS   | 6   | Disabled -           | Disabled -   | OUI         | Ŧ       |                |                |                |          |      |
| Thermal Protection                            | 7   | Disabled -           | Disabled -   | OUI         |         |                |                |                |          |      |
| ► sFlow Agent                                 | 8   | Disabled -           | Disabled •   | OUI         | •       |                |                |                |          |      |
| Loop Protection     Single IP                 |   | Desabled -           | and the second second  | OUI         |         |                |                |                |          |      |
| Easy Port                                     |   |                      |  | OUI         |         |                |                |                |          |      |
| Mirroring                                     | 10  | Disabled -           | Courses from   | 1000        |         |                |                |                |          |      |
| Trap Event Severity                           | 11  | Disabled -           | Disabled •   | OUI         |         |                |                |                |          |      |
| SMTP Configuration                            | 12  | Disabled -           | Disabled 💌   | OUI         |         |                |                |                |          |      |
| UPnP<br>Security                              | 13  | Disabled *           | Disabled -   | OUI         | *       |                |                |                |          |      |
| Security     Maintenance                      | 14  | Disabled -           | Disabled •   | OUI         |         |                |                |                |          |      |

### Fig. 80 Voice VLAN Configuration

Mode:	Select to enable or disable the Voice VLAN function. Please Note: MSTP must be disabled when using Voice VLAN to avoid conflicting ingress filtering information.
VLAN ID:	Specify a unique VLAN ID for the voice VLAN. This VLAN ID cannot be the same as any other VLAN ID configured on the switch. The allowed range is 1 to 4095.
Aging Time:	Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.
Traffic Class:	Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.
Port:	Physical port of the switch.
Mode:	Select the appropriate mode for the selected port. Options are:
	<b>Disabled:</b> Does not belong to the Voice VLAN.

	<ul><li>Auto: Will auto detect whether an IP Phone is connected to the port and will automatically join the Voice VLAN.</li><li>Forced: Will force the port to be part of the Voice VLAN.</li></ul>
Security:	Used to enable or disable the Voice VLAN port security mode. When the function is enabled, all non-IP Phone MAC addresses in the Voice VLAN will be blocked for 10 seconds.
Discovery Protocol:	Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are: OUI: Detect telephony device by OUI address. LLDP: Detect telephony device by LLDP. Both: Both OUI and LLDP.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

## 1.2.11-2 OUI

This section is used to configure the Voice VLAN OUI table. The maximum number of entries is 16. Modifying the OUI table will restart auto detection of OUI process.

### Web Interface

To configure the Voice VLAN OUI settings via the Web Interface:

- 1. Click Configuration, Voice VLAN and OUI.
- 2. Click Add New Entry to add additional OUI information.
- 3. Specify the OUI and Description.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Fig. 81 OUI Configuration

#### **Parameter Description**

*Delete:* Check to delete the entry. It will be deleted during the next save.

Telephony OUI:A telephony OUI address is a globally unique identifier assigned to a vendor<br/>by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a<br/>hexadecimal digit).

Description:	The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.
Add New Entry:	Click to add a new entry to the Voice VLAN OUI table. An empty row is added to the table, please enter the Telephony OUI and Description.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

# 1.2.12 GARP

The Generic Attribute Registration Protocol (GARP) provides a generic framework whereby devices in a bridged LAN, e.g. end stations and switches, can register and de-register attribute values, such as VLAN Identifiers, with each other. In doing so, the attributes are propagated to devices in the bridged LAN, and these devices form a reachability tree that is a subset of an active topology. GARP defines the architecture, rules of operation, state machines and variables for the registration and deregistration of attribute values.

A GARP participation in a switch or an end station consists of a GARP application component, and a GARP Information Declaration (GID) component associated with each port or the switch. The propagation of information between GARP participants for the same application in a bridge is carried out by the GARP Information Propagation (GIP) component. Protocol exchanges take place between GARP participants by means of LLC Type 1 services, using the group MAC address and PDU format defined for the GARP application concerned.

# 1.2.12-1 Configuration

This page allows you to configure the basic GARP Configuration settings for all switch ports.

### Web Interface

To configure the GARP settings via the Web Interface:

- 1. Click Configuration, GARP and Configuration.
- 2. Specify the GARP configuration parameters for the individual ports.
- 3. Click the Apply button to save your changes or the Reset button to revert to previous settings.

- C fi 🗋 192.168.1.1			_				r.	3
ALLOY	ALLOY		, 88886					
AMS-24T6SFP							Auto-Logout OFF . Logout	He
Configuration CPU Load	GAR	P Port Con	figuration				Auto-refresh 🔲 [Refresh]	
Time Account	Port		Timer Value		Application	Attribute Type	GARP Applicant	
▶ IP		Join Timer		Leave All Timer				
► Syslog	1	200	600	10000	GVRP •	VLAN -	normal-participant ·	
► SNMP	2	200	600	10000	GVRP -	VLAN .	normal-participant	
Configuration	3	200	600	10000	GVRP *	VLAN +	normal-participant	
ACL	4	200	600	10000	GVRP -	VLAN -	normal-participant 💌	
Aggregation	5	200	600	10000	GVRP -	VLAN -	normal-participant	
Spanning Tree	6	200	600	10000	CVRP +	VLAN +	normal-participant -	
IGMP Snooping					and the second s		Const.	
MLD Snooping	7	200	600	10000	GVRP +	VLAN -	normal-participant	
► MVR	8	200	600	10000	GVRP •	VLAN 💌	normal-participant	
LLDP     Filtering Data Base	9	200	600	10000	GVRP *	VLAN -	normal-participant 💌	
► VLAN	= 10	200	600	10000	GVRP +	VLAN -	normal-participant +	
- Voice VLAN	11	200	600	10000	GVRP -	VLAN -	normal-participant	
T GARP	12	200	600	10000	GVRP -	VLAN -	normal-participant	
Configuration	13	200	600	10000	GVRP +	VLAN +	and a second	
Statistics • GVRP			1000				normal-participant 💌	
P QoS	14	200	600	10000	GVRP •	VLAN -	normal-participant	
Thermal Protection	15	200	600	10000	GVRP •	VLAN 💌	normal-participant	
► sFlow Agent	16	200	600	10000	GVRP +	VLAN +	normal-participant -	
Loop Protection	17	200	600	10000	GVRP ·	VLAN -	normal-participant -	
Single IP	18	200	600	10000	GVRP -	VLAN -	normal-participant	
Easy Port Mirroring	19	200	600	10000	GVRP +	VLAN -	normal-participant -	
Trap Event Severity	20				GVRP -			
SMTP Configuration		200	600	10000	the second second	VLAN •	normal-participant -	
UPnP	- 21	200	600	10000	GVRP -	VLAN 📼	normal-participant	

Fig. 82 GARP Configuration

Port:	Physical port of the switch.
Timer Values:	To set the GARP Join Timer, Leave Timer and Leave All Timer, the units are set in micro seconds. Join Timer: The default value for the Join Timer is 200ms. Leave Timer: The default value for the Leave Timer is 600ms. Valid values are 600 to 1000ms. Leave All Timer: The default value for the Leave All Timer is 10000ms.
Application:	The only supported application currently is GVRP.
Attribute Type:	The only supported Attribute Type currently is VLAN.
GARP Applicant:	This configuration is used to configure the Applicant state machine behaviour for GARP on a particular port.
	<b>normal-participant:</b> In this mode the Applicant state machine will operate normally in GARP protocol exchanges. <b>non-participant:</b> In this mode the Applicant state machine will not participate in the protocol operation.

*Reset Button:* Used to reset unsaved changes to original configuration.

Apply Button: Used to save the settings configured on this page.

## 1.2.12-2 Statistics

This page allows you to view the GARP Statistics for all switch ports.

#### Web Interface

To view the GARP Statistics via the Web Interface:

- 1. Click Configuration, GARP and Statistics.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

AMS-24T6SFP Configuration CPU Load Time Account IP P Sysiog SNMP Configuration Port AcL Aggregation	GARP Po Port Pee 1 2 3 4 5 6 7	ort Stati		HEREE In the	Auto-Logout OFF 😦 Logou Auto-refresh 🖹 Refresh	I Help
CPU Load         G           Time         I           Account         I           IP         Systeg           SNMP         Configuration           Configuration         Port           ACL         Aggregation	Port Pee 1 2 3 4 5 6	er MAC	Failed Count   		Auto-refresh 🖾 🤼 Refresh	
Account     IP     Port     Configuration     Port     Accu     Aggregation	1 2 3 4 5 6	1 1 1 1 1				
Account IP Systog StMAP Configuration Port ACL Accusion	1 2 3 4 5 6	1 1 1 1 1				
IP     Sysing     SNMP     Configuration     Port     Accurate     Acguration	3 4 5 6	1 1 1 1	-			
► SNMP ▼ Configuration ► Port ► ACL ► Aggregation	3 4 5 6	1 1 1				
► SNMP ▼ Configuration ► Port ► ACL ► Aggregation	4 5 6	-				
<ul> <li>▶ Port</li> <li>▶ ACL</li> <li>▶ Aggregation</li> </ul>	5	-				
<ul> <li>▶ Port</li> <li>▶ ACL</li> <li>▶ Aggregation</li> </ul>	6		-			
► Aggregation						
	8	-	-			
Spanning Tree	9					
► IGMP Snooping	10	-				
MLD Snooping	11					
► MVR	12		-			
► LLDP	13	5				
Filtering Data Base	14	-				
► VLAN	15	-	-			
► Voice VLAN	16	-	-			
* GARP	17		-			
Configuration	18	-	-			
Statistics	19	-	-			
► GVRP	20	-				
P 008	21	77	-			
<ul> <li>Thermal Protection</li> </ul>	22 23	-				
sFlow Agent		+	-			
+ Loop Protection	24 25	-				
Single IP	25	-	-			

Fig. 83 GARP Statistics

- *Peer MAC:* The MAC Address of the connecting switch from which the GARP frame has been received.
- *Failed Count:* The number of GARP frames that have been dropped.
- *Refresh:* Used to manually refresh the information on the page.
- *Auto*-Refresh: Tick the box to enable the information to be automatically refreshed.

# 1.2.13 GVRP

The GARP VLAN Registration Protocol (GVRP) allows network devices to share VLAN information and to use the information to modify existing VLANs or create new VLANs, automatically. This makes it easier to manage VLANs that span more than one switch. Without GVRP, you have to manually configure your switches to ensure that the various parts of the VLANs can communicate with each other across the different switches. With GVRP, which is an application of the Generic Attribute Registration Protocol (GARP), this is done for you automatically.

Here are the guidelines for GVRP:

- GVRP is supported with STP or RSTP or without spanning tree.
- Both ports that constitute a network link between the switch and the other device must be running GVRP.
- You cannot modify or delete dynamic GVRP VLANs.
- You cannot remove dynamic GVRP ports from static or dynamic VLANs.
- To be detected by GVRP, a VLAN must have at least one active node or have at least one port with a valid link to an end node. GVRP cannot detect a VLAN that does not have any active nodes or valid port links.
- Resetting the switch erases all dynamic GVRP VLANs and dynamic GVRP port assignments. The dynamic assignments are relearned by the switch as PDUs arrive on the ports from other switches.
- GVRP has three timers: join timer, leave timer, and leave all timer. The values for these timers must be identically configured on all switches running GVRP. Timers with different values on different switches can result in GVRP compatibility problems.
- You can convert dynamic GVRP VLANs and dynamic GVRP port assignments to static VLANs and static port assignments.

# 1.2.13-1 Configuration

This page allows you to configure the basic GVRP Configuration settings for all switch ports.

### Web Interface

To configure the GVRP settings via the Web Interface:

- 1. Click Configuration, GVRP and Configuration.
- 2. Specify the GVRP Configuration parameters for the required ports.

3. Click the Apply button to save your changes or the Reset button to revert to previous settings.

- C f 🗋 192.168.1.1				会 🕏	1
ALLOY				MEADINT	
AMS-24T6SFP		- 14		Auto-Logout OFF 💌 Logout He	lp
Configuration CPU Load	Glob	al Configur	ation	Auto-refresh 📃 Refresh	1
► Time					
► Account	GVRF	Mode Disat	e ok		
F IP					
► Syslog	Port	Configurati	on		
► SNMP	- III				
Configuration     Port	Port		GVRP rrole		
> ACL	1	Disable -	Disable -		
► Aggregation	2	Disable 💌	Disable -		1
<ul> <li>Spanning Tree</li> </ul>	3	Disable 💌	Disable -		
► IGMP Snooping	4	Disable *	Disable -		
MLD Snooping	B 5	Disable -	Desable -		
► MVR	6	Disable -	Disable -		
► LLDP	7	Disable +	Disable +		
Filtering Data Base	8		Disable -		
VLAN Voice VLAN		Disable 💌			
GARP	9	Disable -	Disable -		
Y GVRP	10	Disable 💌	Desable .		
Configuration	11	Disable -	Disable -		
Statistics	12	Disable 💌	Disable -		
P QoS	13	Disable .	Desable -		
Thermal Protection	14	Disable -	Disable -		
sFlow Agent	15	Disable 💌	Desable -		
► Loop Protection	15	Disable +	Disable -		
Single IP	16	Disable *	Lisable *		1

Fig. 84 GVRP Configuration

GVRP Mode:	Used to enable or disable GVRP globally for the switch.
Port:	Physical port of the switch.
GVRP Mode:	Here you can enable or disable GVRP for a particular port.
GVRP rrole:	This parameter controls if the VLAN registration on the port is restricted or not. Enable - The Restricted VLAN Registration is active for the port row selected. Disable - The Restricted VLAN Registration is de-active for the port row selected.
Refresh:	Used to manually refresh the information on the page.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

# 1.2.13-2 Statistics

This page allows you to view the GVRP Statistics for all switch ports.

### Web Interface

To view the GVRP Statistics via the Web Interface:

- 1. Click Configuration, GVRP and Statistics.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

- C f 🗋 192.168.1.1				会 型
AMS-24T6SFP	Binory Binory Annual Controller			Auto-Logout OFF Cegout Help
Configuration CPU Load	- GVPP P	Port Statist	re.	Auto-refresh 🔲 Refresh Clear
CPU Load	OVRF F	on statist	103	Auto-remesh Clear
Account	Port Ja	oin Tx Count	Leave Tx Count	
F ACCOUNT	1	0	0	
- Syslog	2	0	0	
► SNMP	3	0	0	
* Configuration	4	0	0	
Configuration     Port	- 5	0	0	
► ACL	6	0	0	
	7	0	0	
Aggregation	8	0	0	
Spanning Tree	9	0	D	
► IGMP Snooping	10	0	0	
MLD Snooping	11	0	0	
► MVR	12	0	0	
► LLDP	13	0	0	
Filtering Data Base	14	0	0	
► VLAN	15	0	0	
Voice VLAN	16	0	0	
► GARP	17 18	0	0	
* GVRP	18	0	0	
Configuration	19 20	0	0	
Statistics	20	0	0	
► QoS	21	0	0	
► Thermal Protection	23	0	0	
► sFlow Agent	23	0	0	
► Loop Protection	24	0	0	
► Single IP	- 25	0	0	

Fig. 85 GVRP Statistics

Port:	Physical port of the switch.
Join Tx Count:	Displays the number of Join GVRP requests sent from the port.
Leave Tx Count:	Displays the number of Leave GVRP requests sent from the port.
Refresh:	Used to manually refresh the information on the page.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.

# 1.2.14 QoS

The AMS Series switches support four QoS queues per port with strict or weighted fair queuing scheduling. It supports QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP and UDP/TCP ports and ranges.

High flexibility in the classification of incoming frames to a QoS class. The QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS class assigned to a frame is used throughout the device for providing queuing, scheduling, and congestion control guarantees priority to the frame according to what was configured for that specific QoS class.

The AMS Series switches support advanced memory control mechanisms providing excellent performance of all QoS classes under any traffic scenario, including jumbo frames. A super priority queue with dedicated memory and strict highest priority in the arbitration. The ingress super priority queue allows traffic recognized as CPU traffic to be received and queued for transmission to the CPU even when all the QoS class queues are congested.

## **1.2.14-1 Port Classification**

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

### Web Interface

To configure the QoS Port Classification settings via the Web Interface:

- 1. Click Configuration, QoS and Port Classification.
- 2. Select the appropriate QoS class settings for each switch port.
- 3. Click the Apply button to save your changes or the Reset button to revert to previous settings.

C fi 🗋 192.168.1.1										12 😎 I
ALLOY		ALLOY R Part Monard Digate Balan					::::		TT I I I I I I I I I I I I I I I I I I	
AMS-24T6SFP									Auto-Logout OFF	agout Help
Spanning Tree	1.0									
► IGMP Snooping	~	Qos	Ingress P	ort Class	sificati	on				1
MLD Snooping		Deat	QoS class	DP level	PCP	DEI	Tag Class.	DSCP Based		
► MVR		Port	QOS CIASS	OP level	O.	UEI OF	Tag Class.	DSCP Based		
<ul> <li>LLDP</li> <li>Filtering Data Base</li> </ul>		1	0-	0-	0-	0 -	Disabled	100		
► VLAN				- Andrewski -		Charles Street, St.				
► Voice VLAN		2	0 -	0 -	0 -	0 -	Disabled			
► GARP	1.1	3	0 💌	0 +	0 -	0 💌	Disabled			
► GVRP	- 18	4	0 -	0 -	0 -	0 -	Disabled	E		Ē
▼ Qo5 Port Classification		5	0 🕶	0 -	0 -	0 🖛	Disabled			
Port Policing		6	0 -	0 -	0 -	0 -	Disabled	10		
Port Scheduler		7	0 -	0 -	0-	0 -	Disabled	ET		
Port Shaping		8	0 -	0 -	0 -	0 -	Disabled			
Port Tag Remarking Port DSCP		9	0 -	0 -	0 -	0 -	Disabled	E.		
DSCP-Based QoS		10	0	0 -	0 -	0 -	Desabled			
DSCP Translation			0 -	0 -	Contraction of the local division of the loc	the second second				
DSCP Classification		11		and the second second	0 -	0 -	Disabled			
QoS Control List QCL Status		12	0 -	0 -	0 -	0 -	Disabled	13		
Storm Control		13	0 💌	0 -	0 -	0 -	Disabled	<b></b>		
Thermal Protection		14	0 🕶	0 -	0 •	0 💌	Disabled	19		
► sFlow Agent	100	15	0 💌	0 -	0 💌	0 -	Disabled	1		
Loop Protection		16	0 -	0 -	0 -	0 -	Disabled			
<ul> <li>Single IP</li> <li>Easy Port</li> </ul>		17	0 -	0 -	0-	0-	Disabled	17		
Edsy Port	-		-		-					4

Fig. 86 QoS Port Classification

Port:	Physical port of the switch.
QoS Class:	Controls the default QoS class, i.e., the QoS class for frames not classified in any other way. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.
DP Level:	Every incoming frame is classified to a Drop Precedence Level (DP level), which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP level. This setting controls the default DP level, i.e., the DP level for frames not classified in any other way.
PCP:	Controls the default PCP for untagged frames. PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame.
DEI:	Controls the default DEI for untagged frames. DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.
Tag Class:	Shows the classification mode for tagged frames on this port. <b>Disabled</b> : Use default QoS class and DP level for tagged frames. <b>Enabled</b> : Use mapped versions of PCP and DEI for tagged frames. Click on the mode in order to configure the mode and/or mapping.

DSCP Based:	Click to Enable DSCP Based QoS Ingress Port Classification.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

# 1.2.14-2 Port Policing

This section provides an overview of QoS Ingress Port Policers for all switch ports The Port Policing is useful in constraining traffic flows and marking frames above specific rates. Policing is primarily useful for data flows and voice or video flows because voice and video usually maintains a steady rate of traffic.

### Web Interface

To configure the QoS Port Policing settings via the Web Interface:

- 1. Click Configuration, QoS and Port Policing.
- 2. Enable the ports that to wish to enable policing on.
- 3. Enter the required rates and the units in kbps, Mbps, fps or kfps.
- 4. Tick the check box to enable flow control on required ports.
- 5. Click the Apply button to save your changes or the Reset button to revert to previous settings.

- C f 🗋 192.168.1.1								公 💁
ALLOY		ALLOY Sharehouse	-					
AMS-24T6SFP			-		k k k		and a state of the	a-Logaut OFF 💽 Logaut Hel
► Time					5.0			
► Account		008	ingress	Port Pol	cers			
+ IP	-	Port		Rate	Unit	Flow Control		
<ul> <li>Syslog</li> <li>SNMP</li> </ul>	11	•			0			
Configuration	_	Ť		500	kbps .			
+ Port	_	2		500	kbps -			
MACL		3	EL.	500	kbps .	ad		
► Aggregation		_						
Spanning Tree		4		500	kbps -			
IGMP Snooping     MLD Snooping	E.	5		500	kbps 🔹			
<ul> <li>MUD shooping</li> <li>MVR</li> </ul>		6		500	kbps -			
+ LLDP		7	P1 1	500	kbps -			
► Filtering Data Base		8	n.	500	kbps -			
► VLAN		_						
Voice VLAN		9		500	kbps -			
GARP  GVRP		10		500	kbps -			
Y QoS		11		500	kbps -			
Port Classification		12	PT	500	kbps -	1		
Port Policing		13	17	500	kbps -			
Port Scheduler						-		
Port Shaping		14		500	kbps -	-		
Port Tag Remarking Port DSCP		15		500	kbps -			
DSCP-Based QoS		16	5	500	kbps -			
DSCP Translation		17	FI	500	kbps -	1 🗉		

Fig. 87 QoS Port Policing

Port:	Physical port of the switch.
Mode:	Check the box next to the corresponding port to enable Ingress port policing.
Rate:	Set the Rate that you want to limit the ingress bandwidth to. Default vale is 500.
Unit:	Select the required speed type in units of kbps, Mbps, fps or kfps.
Flow Control:	Check the box to enable Flow Control on the selected port.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

# 1.2.14-3 Port Scheduler

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

### Web Interface

To configure the QoS Port Scheduler settings via the Web Interface:

- 1. Click Configuration, QoS and Port Scheduler.
- 2. Click on the required port to configure the scheduling options.
- 3. You will now be prompted with another screen, here you can select to use Strict Priority or Weighted.
- 4. Configure your Egress bandwidth parameters based on Queue Settings or force the port to a desired speed. If using Weighted a total percentage of a queue can also be set.
- 5. Click the Apply button to save your changes or the Reset button to revert to previous settings.

- C & C 192.168.1.1	1										☆ 克
ALLOY		ALLOY Directions Control Terms									
AMS-24T6SFP			_		-	-	-		1-0-1	Auto-Logout OFF	Logout Help
► Time	· · ·	QoS	Egress Po	rt Sr	hed	uler					
► Account			-9.000.0								
► IP		Port	Mode				ight				
<ul> <li>Syslog</li> </ul>				QO	Q1	Q2		Q4	Q5		
► SNMP	_	1	Weighted	17%	17%	17%	17%	17%	17%		
Configuration		2	Strict Priority Strict Priority						-		
► Port		2	Strict Priority		•		•	-			
► ACL		5	Strict Priority	-	-	12	-		-		
Aggregation		6	Strict Priority	-			-		-		
Spanning Tree		7	Strict Priority	-							
► IGMP Snooping	H	8	Strict Priority								
MLD Snooping		9	Strict Priority				-		-		
		10	Strict Priority		+	-	-				
		11	Strict Priority								-
<ul> <li>Filtering Data Base</li> <li>VLAN</li> </ul>		12	Strict Priority								
> Voice VLAN		13	Strict Priority								
GARP		14	Strict Priority	-	7	-	-				
GARP GVRP		15	Strict Priority								
V QoS		16	Strict Priority		•		•		.*		
Port Classification		17 18	Strict Priority								
Port Policing		10	Strict Priority			-	-				
Port Scheduler		20	Strict Priority				-		-		
Port Shaping		21	Strict Priority								
Port Tag Remarking		22	Strict Priority	-	-	12	÷		-		
Port DSCP		23	Strict Priority		-	-	Ŧ		-		
DSCP-Based QoS		24	Strict Priority						-		
DSCP Translation			Strict Priority								

Fig. 88 Port Scheduling



Fig. 89 Port Scheduling – Strict Priority



Fig. 90 Port Scheduling – Weighted

#### **QoS Egress Port Schedulers**

Port:	Physical port of the switch.
Mode:	Displays the configured Mode type, Strict Priority or Weighted.
Weight (Q0-5):	Shows the current weight for this queue and corresponding port.
QoS Egress Port Schedu	ler and Shapers (Strict Priority)
Scheduler Mode:	Select the required Scheduler Mode for the port, Strict Priority or Weighted.
Queue Shaper Enable:	Tick the box next to the appropriate queue to enable the Queue Shaper.
Queue Shaper Rate:	Enter the required bandwidth rate, maximum values are based on the speed on the port. If running at 1Gb, 1000000 Kbps or 1000Mbps. Default value is 500.
Queue Shaper Unit:	Select whether the shaping rate is measured in kbps or Mbps. Default is kbps.
Queue Shaper Excess:	Enable this if the queue is allowed to use excess bandwidth available on the switch.
Port Shaper Enable:	Tick the box to enable Port shaping on the selected port.

Port Shaper Rate:	Enter the required bandwidth rate, maximum values are based on the speed on the port. If running at 1Gb, 1000000 Kbps or 1000Mbps. Default value is 500.
Port Shaper Unit:	Select whether the shaping rate is measured in kbps or Mbps. Default is kbps.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

## QoS Egress Port Scheduler and Shapers (Weighted)

Scheduler Mode:	Select the required Scheduler Mode for the port, Strict Priority or Weighted.
Queue Shaper Enable:	Tick the box next to the appropriate queue to enable the Queue Shaper.
Queue Shaper Rate:	Enter the required bandwidth rate, maximum values are based on the speed on the port. If running at 1Gb, 1000000 Kbps or 1000Mbps. Default value is 500.
Queue Shaper Unit:	Select whether the shaping rate is measured in kbps or Mbps. Default is kbps.
Queue Shaper Excess:	Enable this if the queue is allowed to use excess bandwidth available on the switch.
Queue Scheduler Weigh	<ul> <li>t: Controls the weight of the queue. This is a percentage of total bandwidth available, valid values 1 to 100.</li> <li>Default is 17.</li> </ul>
Queue Scheduler Percer	t: Shows the weight in percent for this queue.
Port Shaper Enable:	Tick the box to enable Port shaping on the selected port.
Port Shaper Rate:	Enter the required bandwidth rate, maximum values are based on the speed on the port. If running at 1Gb, 1000000 Kbps or 1000Mbps. Default value is 500.
Port Shaper Unit:	Select whether the shaping rate is measured in kbps or Mbps. Default is kbps.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

### 1.2.14-4 Port Shaping

This section provides an overview of QoS Egress Port shaping for all switch ports.

#### Web Interface

To configure the QoS Port Shaping settings via the Web Interface:

- 1. Click Configuration, QoS and Port Shaping.
- 2. Click on the required port to configure the shaping options.
- 3. You will now be prompted with another screen, here you can select to use Strict Priority or Weighted.
- 4. Configure your Egress bandwidth parameters based on Queue Settings or force the port to a desired speed. If using Weighted a total percentage of a queue can also be set.
- 5. Click the Apply button to save your changes or the Reset button to revert to previous settings.

- C 🐔 🗋 192.168.1.1		-		_		_	_	_				_	5	2
ALLOY	VILOY	-			nament inte	r r r	Tracition 1		Alsonith	1				
Taka and	Charles Harman													
AMS-24T6SFP						1000	and the second s			Aut	o-Logout OF	F .	ogout F	fe
										740	o-cogour or			1
► MVR		1. A. C. A.	1.1.1.1											
F LLDP	QoS	Egress	Port Sh	apers										
Filtering Data Base						Shapers								
+ VLAN	Port	00	01	02	03	04	Q5	Q6	07	Port				
Voice VLAN	1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled				
► GARP	2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled				
- GVRP	1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled				
Y QoS	4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled				
Port Classification	5	disabled disabled	disabled disabled	disabled disabled	disabled disabled	disabled disabled	disabled disabled	disabled disabled	disabled disabled	disabled disabled				
Port Policing	0	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled				
Port Scheduler	8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled				
Port Shaping	- 9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled				
Port Tag Remarking	10	500 kbps	500 kbps	disabled	disabled	disabled	disabled	disabled	disabled	10 Mbps				
Port DSCP	11	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled				
DSCP-Based QoS	12	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled				
DSCP Translation	13 14	disabled disabled	disabled disabled	disabled disabled	disabled disabled	disabled disabled	disabled disabled	disabled disabled	disabled disabled	disabled disabled				
DSCP Classification	15	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled				
QoS Control List	16	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled				
QCL Status	17	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled				
Storm Control	18	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled				
<ul> <li>Thermal Protection</li> </ul>	19	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled				
► sFlow Agent	20	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled disabled				
Loop Protection	2 <u>1</u> 22	disabled disabled	disabled disabled	disabled disabled	disabled disabled	disabled disabled	disabled disabled	disabled disabled	disabled disabled	disabled				
► Single IP	23	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled				
Easy Port	24	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled				
Mirroring	25	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled				
Trap Event Seventy	26	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled				
SMTP Configuration														

Fig. 91 Port Shaping

- C ń 🗋 192.168.1.1					ta 🔁
AMS-24T6SFP				Auto-Logout OFF	Logout Hel
<ul> <li>Time</li> <li>Account</li> <li>IP</li> <li>Syslog</li> </ul>	•	QoS Egress Port Scheduler and Sha Scheduler Mode Strict Priority -	apers Port 1		Port 1 💌
Source S	-	Queue Shaper Enable Rate Unit Excess	Port Shaper Enable Rate Unit		
► AGE ► Aggregation ► Spanning Tree ► IGMP Snooping ► MLD Snooping	Ē	00-3 500 https:-	<u> </u>		
► MVR ► LLDP ► Filtering Data Base ► VLAN		500 kbps -			
Voice VLAN GARP GVRP QoS		03 • 6 500 kbps -	R I S00 kbps v		
Port Classification Port Policing Port Scheduler Port Shaping		500 kbps -	C		
Port Snaping Port Tag Remarking Port DSCP DSCP-Based QoS DSCP Translation		06-00 kbps -			

Fig. 92 Port Shaping – Strict Priority

- C f 🗋 192.168.1.1		습 <u>원</u>
AMS-24T6SFP		Auto-Logout OFF Clogout Help
Time     Account	Qo8 Egress Port Scheduler and Shapers Port 1	Port 1 💌
► IP ► Syslog	Scheduler Mode Weighted	
SNMP     Configuration     Port	Queue Shaper Queue Scheduler Enable Rate Unit Excess Weight Percent I	Port Shaper Enable Rate Unit
ACL     Aggregation     Spanning Tree     IGMP Snooping		
MLD Snooping MVR LLDP	01+8 500 kbps 17 17% D	
► Filtering Data Base ► VLAN	22 • 6 Kops - 17 17% W R T	
Voice VLAN     GARP     GVRP	500 kbps - 17 17% R I	*6
Port Classification Port Policing	500 kbps 17 17%	
Port Scheduler Port Shaping Port Tag Remarking	600 kbp: 17 17%	
Port DSCP DSCP-Based QoS DSCP Translation		

Fig. 93 Port Shaping – Weighted

### **QoS Egress Port Shapers**

*Port:* Physical port of the switch.

Mode:	Displays the configured Mode type, Strict Priority or Weighted.

*Weight (Q0-5):* Shows the current weight for this queue and corresponding port.

### **QoS Egress Port Scheduler and Shapers (Strict Priority)**

Scheduler Mode:	Select the required Scheduler Mode for the port, Strict Priority or Weighted.
Queue Shaper Enable:	Tick the box next to the appropriate queue to enable the Queue Shaper.
Queue Shaper Rate:	Enter the required bandwidth rate, maximum values are based on the speed on the port. If running at 1Gb, 1000000 Kbps or 1000Mbps. Default value is 500.
Queue Shaper Unit:	Select whether the shaping rate is measured in kbps or Mbps. Default is kbps.
Queue Shaper Excess:	Enable this if the queue is allowed to use excess bandwidth available on the switch.
Port Shaper Enable:	Tick the box to enable Port shaping on the selected port.
Port Shaper Rate:	Enter the required bandwidth rate, maximum values are based on the speed on the port. If running at 1Gb, 1000000 Kbps or 1000Mbps. Default value is 500.
Port Shaper Unit:	Select whether the shaping rate is measured in kbps or Mbps. Default is kbps.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.
QoS Egress Port Sched	uler and Shapers (Weighted)
Scheduler Mode:	Select the required Scheduler Mode for the port, Strict Priority or Weighted.
Queue Shaper Enable:	Tick the box next to the appropriate queue to enable the Queue Shaper.
Queue Shaper Rate:	Enter the required bandwidth rate, maximum values are based on the speed on the port. If running at 1Gb, 1000000 Kbps or 1000Mbps. Default value is 500.
Queue Shaper Unit:	Select whether the shaping rate is measured in kbps or Mbps. Default is kbps.

*Queue Shaper Excess:* Enable this if the queue is allowed to use excess bandwidth available on the switch.

*Queue Scheduler Weight:* Controls the weight of the queue. This is a percentage of total bandwidth available, valid values 1 to 100. Default is 17.

*Queue Scheduler Percent:* Shows the weight in percent for this queue.

Port Shaper Enable:	Tick the box to enable Port shaping on the selected port.
Port Shaper Rate:	Enter the required bandwidth rate, maximum values are based on the speed on the port. If running at 1Gb, 1000000 Kbps or 1000Mbps. Default value is 500.
Port Shaper Unit:	Select whether the shaping rate is measured in kbps or Mbps. Default is kbps.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

# 1.2.14-5 Port Tag Remarking

This section provides an overview of QoS Egress Port Tag Remarking all switch ports.

#### Web Interface

To configure the QoS Port Tag Remarking settings via the Web Interface:

- 1. Click Configuration, QoS and Port Tag Remarking.
- 2. Click on the port you want to configure.
- 3. Select the required Mode, Classified, Default or Mapped.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Fig. 94 Port Tag Remarking



### Fig. 95 Port Tag Remarking – Classified Mode



Fig. 96 Port Tag Remarking – Default Mode

- C f 🗋 192.168.1.1								_	_			\$
ALLOY		ALLOY Effectives						666		Alternations		
AMS-24T6SFP	10		- 6.41	-		_	and in				Auto-Logout OFF	Logout He
MVR	100											
+ LLDP		QoS Egre	ss Port	Tag	Re	ma	rking	Port 1				Port 1 💌
Filtering Data Base							- 2					
► VLAN		Tag Remar	king Mode	Ma	pped	*						
Voice VLAN     GARP		(QoS class, I	DP level) to	PC	P. D	EI) T	apping					
► GVRP		QoS class	DBland	PC	-0	DE						
* QoS		WOS class	UP level		-		-					
Port Classification				0		0						
Port Policing		0	0	1		0						
Port Scheduler		0	1	1	۲	1						
Port Shaping	100	1	0	0		0						
Port Tag Remarking Port DSCP		1	1	0		1	-					
DSCP-Based QoS		2	0	2	-	0						
DSCP Translation		2	1	2		1						
DSCP Classification					-		the second se					
QoS Control List		3	Q	3		0						
QCL Status Storm Control	E	3	1	3		1	*					
Thermal Protection		4	0	4		0						
► sFlow Agent		4	1	4		1						
Loop Protection		5	0	5		0	-					
► Single IP		5	1	5	F	1						
Easy Port		-		-	-	-	Const.					
Mirroring		6	0	6	-	0	-					
Trap Event Seventy SMTP Configuration		6	1	6		1						
11Dop	+	7	0	7		0	-					

Fig. 97 Port Tag Remarking – Mapped Mode

Port:	Physical port of the switch.
Mode:	Shows the tag remarking mode for this port. Classified: Use classified PCP/DEI values. Default: Use default PCP/DEI values. Mapped: Use mapped versions of QoS class and DP level.

Tag Remarking Mode (Classified): When set to Classified no configuration is necessary.

*Tag Remarking Mode (Default):* When set to Default the Administrator can manually set the PCP and DEI Values.

*Tag Remarking Mode (Mapped):* When set to Mapped the Administrator can map the PCP and DEI values based on the values of the QoS Class and DP Level.

- *Reset Button:* Used to reset unsaved changes to original configuration.
- *Apply Button:* Used to save the settings configured on this page.

## 1.2.14-6 Port DSCP

This section provides an overview of QoS Port DSCP settings for all switch ports.

### Web Interface

To configure the QoS Port DSCP settings via the Web Interface:

- 1. Click Configuration, QoS and Port DSCP.
- 2. Check the tick box next to each corresponding port to enable the DSCP feature.
- 3. Specify the Ingress Classify parameter and whether the Egress packets will be rewritten.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.

AMS-24T6SFP       Auto-Logout OFF • Logout         • NVR         • NVR         • LUDP         • KIRFING Data Base         • VAIN         • OSP         • OSP-Based CoS         DSP-Based CoS         DSP-Classification         DSP-Based CoS         DSP-Based CoS         DSP-Based CoS         DSP-Based CoS         DSP-Based CoS         Disable · D	- C 🐔 🗋 192.168.1.1				_	-		_		\$ 3
Public       QoS Port DSCP Configuration         Filtering Data Base       Filtering Data Base         VLAN       Port         VOIce VLAN       Ingress         CARP       Ingress         CARP       Ingress         Port       Disable         Port       Disable         Port       Disable         Port Scheduler       Disable         Port Scheduler       Disable         Port Scheduler       Disable         Port Scheduler       Disable         Port DSCP       Disable         DSCP-Dissed CoS       7         DSCP-Dissed CoS       10         Disable       Disable         Cos Control List       10         Control       11         Disable       Disable         Fiberwal protection       12         Disable       Disable         Pistroler Protection       14 </th <th>AMS-24T6SFP</th> <th></th> <th>ALCY D're Menael Sair Trail</th> <th></th> <th>• 8</th> <th>Ģ</th> <th></th> <th><del>CH</del></th> <th>i in in the second s</th> <th>Logout He</th>	AMS-24T6SFP		ALCY D're Menael Sair Trail		• 8	Ģ		<del>CH</del>	i in in the second s	Logout He
VLN     Port     Ingress     Egress       Volce VLAN     GaRP     Classify     Rewrite       GARP <ul> <li>Garba</li> <li>Girable</li> <li>Disable</li> <lidisable< li="">         &lt;</lidisable<></ul>	F LLDP	-	QoS	Port DSC	P Conf	igur	ation			
Voice VLAN     Port     Translate     Classify     Rewrite       CARP <ul> <li>CVRP</li> <li>Disable</li> <lidisable< li=""></lidisable<></ul>				Ing	ress		Eare	88		
CVRP       1       Disable       Disable          Y QoS       2       Disable       Disable          Port Dolicing       3       Disable       Disable          Port Stassification       3       Disable       Disable          Port Scheduler       4       Disable       Disable          Port Scheduler       6       Disable       Disable          Port Scheduler       6       Disable           Port Scheduler       6       Disable           DSCP Translation       8       Disable        Disable          DSCP Translation       8       Disable        Disable          QCI, Status       10       Disable        Disable          Storm Control       11       Disable        Disable          Flow Agent       13       Disable        Disable          Single IP       14       Disable        Disable			Port			ify				
• QoS     I     Disable     Disable       Port Classification     2     Disable     Disable       Port Scheduler     3     Disable     Disable       Port Scheduler     4     Disable     Disable       Port Scheduler     4     Disable     Disable       Port Tag Remarking     5     Disable     Disable       Port Tag Remarking     6     Disable     Disable       Port DSCP     0     Disable     Disable       DSCP Translation     8     Disable     Disable       DSCP Classification     9     Disable     Disable       OSC Control List     10     Disable     Disable       QCL Status     11     Disable     Disable       Storm Control     12     Disable     Disable       + Termail Protection     12     Disable     +       > Loop Protection     14     Disable     +	► GARP				0	-	0			
Port Classification     2     Disable     Circable       Port Policing     3     Disable     Disable     +       Port Scheduler     4     Disable     +     Disable     +       Port Tag Remarking     5     Disable     +     Disable     +       Port DiscReduler     6     Disable     +     Disable     +       Port DiscReduler     6     Disable     +     Disable     +       Port DiscReduler     6     Disable     +     Disable     +       DSCP Tarsistion     8     Disable     +     Disable     +       DSCP Classification     9     Disable     +     Disable     +       DSCP Classification     9     Disable     +     Disable     +       Disable     Disable     +     Disable     +     Disable     +       Thermal Protection     11     Disable     +     Disable     +       Stom Control     11     Disable     +     Disable     +       Stom Control     12     Disable     +     +     +       Stom Control     13     Disable     +     Disable     +       Stop Protection     14     Disable     +     Disable			1	1	Disable	-	Disable	-		
Port Policing 3 Disable • Disable • Port Scheduler 4 Disable • Disable • Port Scheduler 5 Disable • Disable • Port Tag Remarking 5 Disable • Disable • Port Tag Remarking 6 Disable • Disable • DSCP Flassed QoS 7 Disable • Disable • DSCP Classification 8 Disable • Disable • DSCP Classification 9 Disable • QCL Status 10 Disable • Disable • Thremal Protection 12 Disable • Storm Control = Stow Agent 13 Disable • Disable • Single P			2					- Internet		
Port Scheduler     4     Disable     •       Port Shaping     5     Disable     •       Port Tag Remarking     6     Disable     •       Port DSCP     6     Disable     •       Port DSCP     7     Disable     •       DSCP Translation     8     Disable     •       DSCP Classification     9     Disable     •       Disable     •     Disable     •       QoS Control List     10     Disable     •       Storm Control     11     Disable     •       Thermal Protection     12     Disable     •       P Flow Agent     13     Disable     •       > Loop Protection     14     Disable     •					1.000	The second second		-		
Port Bapping     5     Disable     •       Port DSCP     6     Disable     •       DSCP-Flassed QoS     7     Disable     •       DSCP Fransfation     8     Disable     •       DSCP Classification     9     Disable     •       DSCP Classification     9     Disable     •       DSCP Classification     10     Disable     •       Disable     •     Disable     •       CLS status     10     Disable     •       Storm Control     11     Disable     •       Thermal Protection     12     Disable     •       > Flow Agent     13     Disable     •       > Single IP     Disable     •						And a local division of the				
Port Tag Remarking     0     Disable     Insable       Port DSCP     Disable     Disable     Port Disable       DSCP-Based QoS     7     Disable     Disable     Port Disable       DSCP-Dased QoS     7     Disable     Port Disable     Port Disable       DSCP Classification     8     Disable     Port Disable     Port Disable       QoS Control Ust     10     Disable     Disable     Port Disable       Stom Control     11     Disable     Poisable     Poisable       Thermal Protection     12     Disable     Disable     Poisable       > Single IP     13     Disable     Poisable     Poisable			the second second			-				
Port DSCP     6     Disable     V     Disable     *       DSCP-Rased GoS     7     Dicable     -     Dicable     -       DSCP Translation     8     Disable     -     Dicable     +       DSCP Classification     9     Dicable     +     Dicable     +       QoS Control List     10     Dicable     +     Dicable     +       QCL Status     11     Dicable     +     Dicable     +       Storm Control     12     Dicable     +     Dicable     +       > Fremal Protection     12     Dicable     +     Dicable     +       > Loop Protection     14     Dicable     +     Dicable     +		100	-			and a second sec				
DSCP Translation     8     Disable     •       DSCP Classification     9     Deable     •       Qas Control List     10     Disable     •       QCL Status     10     Disable     •       Stom Control     11     Disable     •       Thermal Protection     12     Disable     •       > Flow Agent     13     Disable     •       > Single IP     14     Disable     •						-				
DSCP Classification     9     Disable     •       QoS Control List     10     Disable     •       QCL Status     11     Disable     •       Storm Control     11     Disable     •       Thermal Protection     12     Disable     •       Flow Agent     13     Disable     •       Storp Protection     14     Disable     •	DSCP-Based QoS		7	1000	Disable	-	Disable	-		
Gos Control List     s     Disable     Disable       GCL Status     10     Disable     Disable     +       Stom Control     11     Disable     >     Disable     +       Thermal Protection     12     Disable     +     Disable     +       Stom Control     13     Disable     +     Disable     +       Single IP     14     Disable     +     -			8		Disable	*	Disable	*		
QCL Status     10     Disable •     Disable •       Storm Control     11     Disable •     Disable •       Fnemal Protection     12     Disable •     Disable •       > aFlow Agent     13     Disable •     Disable •       > Loop Protection     14     Disable •     Disable •			9		Disable	-	Desable			
Stom Control     11     Disable     •       • Thermal Protection     12     Disable     •       • SFlow Agent     13     Disable     •       • Loop Protection     14     Disable     •       • Single IP     14     Disable     •			10		Disable		Disable	•		
Thermal Protection     12     Disable     ■		E	11		Disable	-	Disable	*		
▶ sFlow Agent 13 Disable ★ Disable ★ ▶ Loop Protection 14 Disable ★ Disable ★ Single IP		11	12		Disable	-	Disable	-		
Loop Protection     Single IP     Id     Disable     Disable     Disable						- Internal I				
Single IP						Contraction of the		100.0		
Easy Port 10 Uisable * Disable *								- Andrew - A		
						-				
Mirroring 16 Disable  Trap Event Seventy 17 Disable Disable			1000			the second second		- Andrew -		
Trap Event Seventy     17     Disable         SMTP Configuration     18     Disable			10000000			and it	Disable			

Fig. 98 Port DSCP Settings

Port:	Physical port of the switch.
Ingress Translate:	To enable ingress translation of the DSCP value enable this feature.
Classify:	Classification values available for the port are as follows: <b>Disable</b> : No Ingress DSCP Classification. <b>DSCP=0</b> : Classify if incoming (or translated if enabled) DSCP is 0. <b>Selected</b> : Classify only selected DSCP values for which classification is

	enabled as specified in DSCP Translation window for the specific DSCP. All: Classify all DSCP values.
Egress Rewrite:	<ul> <li>DSCP Values can be rewritten based on the below parameters:</li> <li>Disable: No Egress rewrite.</li> <li>Enable: Rewrite enable without remapping the DSCP value.</li> <li>Remap DP Unaware: Frame with DSCP from analyser is remapped and remarked with the remapped DSCP value. The mapped DSCP value is always taken from the DSCP Translation table.</li> <li>Remap DP Aware: Frame with DSCP from analyser is remapped and remarked with the remapped DSCP value. Depending on the frame's DP level, the remapped DSCP value is either taken from the DSCP Translation table or the Egress Remap DP0 or DP1 field.</li> </ul>
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

# 1.2.14-7 DSCP-based QoS

This section is used to configure DSCP-based QoS settings for all switch ports.

### Web Interface

To configure the DSCP-based QoS settings via the Web Interface:

- 1. Click Configuration, QoS and DSCP-based QoS.
- 2. Specify whether the DSCP value is trusted, and set the corresponding QoS value and DP level used for ingress processing.
- 3. Click the Apply button to save your changes or the Reset button to revert to previous settings.

C n 🗋 192.168.1.1		_					Q 🕏
ALLOV E	LLOY Par Manarel	7	12000	at an an i a		401-2-2007	
	Contraction of the local distribution of the	1.17			*****		
MS-24T6SFP							Auto-Logout 10 min • Logout Ho
Syslog	SCP-R	ased	QoS Ingre	ss Class	ication		
SNMP					loudon		
Configuration	DSCP	Trust	QoS Class	DPL			
ACL			0.	0.			
	0 (BE)	-	0 -	0 -			
<ul> <li>Spanning Tree</li> </ul>	O (DE)			a dead			
IGMP Snooping	1	2	0 -	0 -			
	2		0 -	0 -			
MVR				and the second sec			
LLDP	3	1	0 🖛	0 💌			
Filtering Data Base	4		0 -	0 -			
VLAN =	5	0	0 -	0 -			
VOICE VERIN			Landson and				
GARP	6		0 🕶	0 💌			
T QoS	7		0 -	0 -			
Cont Clinical Statistics							
Port Policing	8 (CS1)		0 -	0 -			
Port Scheduler	9		0 -	0 -			
Port Shaping	10 (AF11)	0	0 -	0 -			
Port Tag Remarking							
	11		0 🕶	0 🕶			
DSCP-Based QoS DSCP Translation	12 (AF 12)		0 -	0 -			
DSCP Translation							
QoS Control List	13		0 -	0 -			
QCL Status +	14 (AF13)	0	0 -	0 -			

Fig. 99 DSCP-based QoS

#### Parameter Description

DSCP: DSCP value in ingress packets. Range is 0 – 63.

Trust:Controls whether a specific DSCP value is trusted. Only frames with trustedDSCP values are mapped to a specific QoS class and drop level (DPL). Frameswith untrusted DSCP values are treated as non-IP frames.

QoS Class:QoS value to which the corresponding DSCP value is classified for ingress<br/>processing.<br/>Range: 0-7.<br/>Default value is 0.

DPL:	Drop Precedence Level to which the corresponding DSCP value is classified
	for ingress processing.
	Range: 0-1, where 1 is the higher drop priority;
	Default value is 0.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

### 1.2.14-8 DSCP Translation

This section is used to configure DSCP translation for ingress traffic or DSCP re-mapping for egress traffic.

#### Web Interface

To configure the DSCP Translation settings via the Web Interface:

- 1. Click Configuration, QoS and DSCP Translation.
- 2. Set the required ingress translation and egress re-mapping parameters.
- 3. Click the Apply button to save your changes or the Reset button to revert to previous settings.

C ń 🗋 192.168.1.1												2
ALLOY	ALLOY		lan.	10000			-		481-017	ane 1		
ALL OF	ALLOY District Manageri District Manageri	I								i l		
AMS-24T6SFP	_									Auto-	Logout OFF	Logout H
Syslog	DSCP T	ranslatio	m									
► SNMP		anorane										
Configuration > Port	DSCP		gres		-		ress					
ACL		Translat		Classify	Remap		Remap	-				
<ul> <li>Aggregation</li> </ul>			•		0		0					
Spanning Tree	0 (BE)	.0 (BE)	•		0 (BE)		0 (BE)					
IGMP Snooping	1	1	•		1		1					
MLD Snooping	2	2	+	17	2		2					
MVR.	3	3	•	E	3		3					
LLDP	4		-		4		4	-				
Filtering Data Base			-			- Land						
► VLAN	E 5		٠		5		5					
Voice VLAN	6		*		6		6					
► GARP	7	7	-		7		1					
► GVRP	8 (CS1)	8 (CS1)	•	10	8 (CS1)		8 (CS1)	1.				
Qos     Port Classification	9	9	+	1	9		9					
Port Policing	10 (AF11)	10 (AF11)	-		10 (AF1)		10 (AF1	1				
Port Scheduler	11				11	-	11					
Port Shaping		12 (AF 12)	-		12 (AF1)	1000	12 (AF1	10001				
Port Tag Remarking	12 (AF12)		-					and the second se				
Port DSCP	13		•		13		13	-				
DSCP-Based QoS	14 (AF13)	14 (AF13)	•	2	14 (AF1)	i) -	14 (AF1	3) •				
DSCP Translation	15	15	•	1	15		15					
DSCP Classification	16 (CS2)	16 (CS2)	-	Ē	16 (CS2)	-	16 (CS2	) 🗐				
QoS Control List QCL Status	17	17	•		17		17					

Fig. 100 DSCP Translation

DSCP:	DSCP value. Range is 0 – 63.
Ingress Translate:	Enables ingress translation of DSCP values based on the specified classification method.
Ingress Classify:	Enable Classification at ingress side as defined in the QoS Port DSCP Configuration table.

Egress Remap DPO:	Re-maps DP0 field to selected DSCP value. DP0 indicates a drop precedence with a low priority.
Egress Remap DP1:	Re-maps DP1 field to selected DSCP value. DP1 indicates a drop precedence with a high priority.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

## 1.2.14-9 DSCP Classification

This section is used to map DSCP values to a QoS class and drop precedence level.

### Web Interface

To configure the DSCP Classification settings via the Web Interface:

- 1. Click Configuration, QoS and DSCP Classification.
- 2. Map the DSCP values to a corresponding QoS class and drop precedence level.
- 3. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Fig. 101 DSCP Classification

QoS Class/DPL:	Shows the mapping options for QoS class values and DP (drop precedence) levels.
DSCP:	DSCP value. Range is 0 – 63.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

# 1.2.14-10 QoS Control List

Use the QoS Control List Configuration page to configure Quality of Service policies for handling ingress packets based on Ethernet type, VLAN ID, TCP/UDP port, DSCP, ToS, or VLAN priority tag.

Once a QCE is mapped to a port, traffic matching the first entry in the QoS Control List is assigned to the QoS class, drop precedence level, and DSCP value defined by that entry. Traffic not matching any of the QCEs are classified to the default QoS Class for the port.

### Web Interface

To configure the QoS Control List settings via the Web Interface:

- 1. Click Configuration, QoS and QoS Control List.
- 2. Click the 🕀 button to add a new QCE, or use the other QCE modification buttons to specify the editing action (i.e., edit, delete, or moving the relative position of entry in the list).
- 3. When editing an entry on the QCE Configuration page, specify the relevant criteria to be matched, and the response to a match.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Fig. 102 QoS Control List



Fig. 103 Adding a QoS Control List Entry

QCE:	Quality Control Entry Index.
Port:	Physical port of the switch.
Frame Type:	Indicates the type of frame to look for in incoming frames. Possible frame types are: Any, Ethernet, LLC, SNAP, IPv4, and IPv6.
SMAC:	The OUI field of the source MAC address, i.e. the first three octets (bytes) of the MAC address.
DMAC:	The type of destination MAC address. Possible values are: Any, Broadcast, Multicast, and Unicast.
VID:	VLAN ID. Valid Range 1 – 4095
PCP:	PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame.
DEI:	DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.
Action:	Indicates the classification action taken on ingress frames, if the configured parameters are matched in the frame's content. If a frame matches the QCE, the following actions will be taken: <b>Class (Classified QoS Class)</b> – If a frame matches the QCE, it will be put in the 213

queue corresponding to the specified QoS class.

**DPL** – The drop precedence level will be set to the specified value.

**DSCP** – The DSCP value will be set the specified value.

Ð	Inserts a new QCE before the current row.
e	Edits the QCE.
Ô	Moves the QCE up the list.
$\odot$	Moves the QCE down the list.
8	Deletes the QCE.
Ð	The lowest plus sign adds a new entry at the bottom of the QCE listings

Fig. 104 Functions of QCE Control Buttons

QCE Configuration:	Port Members – The ports assigned to this entry.
Tag:	VLAN tag type. Options: Any, Tag, Untag; Default: Any
VID:	VLAN identifier. Options: Any, Specific (1-4095), Range. Default: Any
PCP:	Priority Code Point (User Priority). Options: a specific value of 0, 1, 2, 3, 4, 5, 6, 7, a range of 0-1, 2-3, 4-5, 6-7, 0-3, 4-7, or Any. Default: Any
DEI:	Drop Eligible Indicator. Options: 0, 1 or Any Default: Any
SMAC:	The OUI field of the source MAC address. Enter the first three octets (bytes) of the MAC address, or Any.
DMAC:	The type of destination MAC address. (Options: Any, BC (Broadcast), MC (Multicast), UC (Unicast).

### *Frame Type:* The supported Frame Types are listed below:

Any – Allow all types of frames.

**Ethernet** – This option can only be used to filter Ethernet II formatted packets. Options: Any, Specific – 600-ffff hex; Default: ffff Note that 800 (IPv4) and 86DD (IPv6) are excluded. A detailed listing of Ethernet protocol types can be found in RFC1060. A few of the more common types include 0800 (IP), 0806(ARP), 8137 (IPX).

LLC – Link Logical Control includes the following settings: SSAP Address – Source Service Access Point address. (Options: Any, Specific (0x00-0xff); Default: 0xff) DSAP Address – Destination Service Access Point address. (Options: Any, Specific (0x00-0xff); Default: 0xff) Control – Control field may contain command, response, or sequence information depending on whether the LLC frame type is Unnumbered, Supervisory, or Information. (Options: Any, Specific (0x00-0xff); Default: 0xff)

**SNAP** – SubNetwork Access Protocol can be distinguished by an OUI and a Protocol ID. (Options for PID: Any, Specific (0x00-0xffff); Default: Any) If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP. If the OUI is that of a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of the OUI field is 00-00-00, then value of the PID will be etherType (0x0600-0xffff), and if value of the OUI is other than 00-00-00, then valid value of the PID will be any value from 0x0000 to 0xffff.

IPv4 – IPv4 frame type includes the following settings: *Protocol* – IP protocol number. (Options: Any, UDP, TCP, or Other (0-255)) *Source IP* – Source IP address. (Options: Any, Specific)
To configure a specific source IP address, enter both the address and mask format. The address and mask must be in the format x.y.z.w where x, y, z, and where 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.

*IP Fragment* – Indicates whether or not fragmented packets are accepted. (Options: Any, Yes, No; Default: Any)Datagrams may be fragmented to ensure they can pass through a network device which uses a maximum transfer unit smaller than the original packet's size.
	DSCP – Diffserv Code Point value. (Options: Any, specific value of 0-63, BE, CS1-CS7, EF or AF11-AF43, or Range; Default: Any)
	IPv6 – IPv6 frame type includes the same settings as those used for IPv4, except for the Source IP. When configuring a specific IPv6source address, enter the least significant 32 bits (a.b.c.d) using the same type of mask as that used for an IPv4 address. Sport – Source TCP/UDP port. (Any, Specific/Range: 0-65535) Dport – Destination TCP/UDP port. (Any, Specific/Range: 0-65535)
Class (Classified QoS Cl	ass): If a frame matches the QCE, it will be put in the queue corresponding to
	the specified QoS class, or placed in a queue based on basic classification
	rules.
	Options: 0-7, Default (use basic classification)
	Default setting: 0
DPL:	The drop precedence level will be set to the specified value or left unchanged.
	Options: 0-1, Default
	Default setting: Default
DSCP:	The DSCP value will be set to the specified value or left unchanged.
	Options: 0-63, BE, CS1-CS7, Default (not changed)
	Default setting: Default)
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

## 1.2.14-11 QCL Status

Displays the current QCL (QoS Control List) entries configured on the switch.

## Web Interface

To view the QCL via the Web Interface:

- 1. Click Configuration, QoS and QCL Status.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

C 🐔 🗋 192.168.1.1								ŝ	2
ALLOY	et for Hanaat Daar Texto								
MS-24T6SFP							Auto-Logout OFF	E Logout	Hel
Aggregation	H					-			
Spanning Tree	QoS Control	List Status	5		Combined	· Auto-refresh	Resolve Conflict	Refresh	
IGMP Snooping MLD Snooping	to the same of		-	Action	1 million and				
MVR	User QCE#	Frame Type	Port Class	DPL DSCP	Conflict				
LLDP	No entries								
Filtering Data Base									
VLAN									
Voice VLAN	14								
GARP									
GVRP									
Qos									
Port Classification									
Port Policing									
Port Scheduler									
Port Shaping	-								
Port Tag Remarking Port DSCP									
DSCP-Based QoS									
DSCP-Based Gos DSCP Translation									
DSCP Classification									
QoS Control List									
QCL Status									
Storm Control									
Thermal Protection									
sFlow Agent									
Loop Protection									
<ul> <li>Single IP</li> </ul>									

Fig. 105 QoS Control List Status

User:	Displays the QCL user type.
QCE#:	Displays the QCE Index number.
Frame Type:	Displays the frame type configured for that entry.
Port:	Displays the list of ports that the QCE applies to.
Action:	Displays the Action values configured for the QCE entry.
Conflict:	Displays any conflict that have occurred with the QCE entry.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed. 217

*Refresh:* Used to manually refresh the information on the page.

*Resolve Conflict:* Click to resolve any current QCE conflicts that have occurred.

# 1.2.14-12 Storm Control

Use the Storm Control Configuration page to set limits on broadcast, multicast and unknown unicast traffic to control traffic storms which may occur when a network device is malfunctioning, the network is not properly configured, or application programs are not well designed or properly configured. Traffic storms caused by any of these problems can severely degrade performance or bring your network to a complete halt.

You can protect your network from traffic storms by setting a threshold for broadcast, multicast, or unknown unicast traffic. Any packets exceeding the specified threshold will then be dropped. Note that the limit specified on this page applies to each port.

#### Web Interface

To configure the Storm Control settings via the Web Interface:

- 1. Click Configuration, QoS and Storm Control.
- 2. Enable storm control for unknown unicast, broadcast, or multicast traffic by marking the Status box next to the required frame type.
- 3. Select the control rate for the selected traffic type.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.

C fi 🗋 192.168.1.1		ेद्ध <b>क्</b> र
MS-24T6SFP		
W3-24103FF		Auto-Logout OFF · Logout Help
Aggregation		
Spanning Tree	Storm Control Configuration	
IGMP Snooping	Frame Type Enable Rate (pps)	
MLD Snooping	Unicast 1 -	
LLDP		
Filtering Data Base		
VLAN	Broadcast 🔲 1 💌	
Voice VLAN	The second second	
GARP	Apply Reset	
GVRP		
QoS		
Port Classification		
Port Policing		
Port Scheduler		
Port Shaping		
Port Tag Remarking	5	
Port DSCP		
DSCP-Based QoS		
DSCP Translation DSCP Classification		
QoS Control List		
QCL Status		
Storm Control		
Thermal Protection		
sFlow Agent		
Loop Protection		

Fig. 106 Storm Control

Frame Type:	Specifies broadcast, multicast or unknown unicast traffic.
Status:	Enables or Disables Storm Control.
Rate (pps):	The threshold above which packets are dropped. This limit can be set by specifying a value in pps, or by selecting one of the options in Kpps (i.e., marked with the suffix "K"). Options: n pps where n = 1, 2, 4, 8, 16, 32, 64, 128, 256, 512; or 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024 Kpps; Default: 2 pps
	Due to an ASIC limitation, the enforced rate limits are slightly less than the listed options. For example: 1 Kpps translates into an enforced threshold of 1002.1 pps.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

# 1.2.15 s-Flow Agent

The AMS Series switches support s-Flow network monitoring. sFlow is a sampling technology that meets the key requirements for a network traffic monitoring solution:

- sFlow provides a network-wide view of usage and active routes. It is a scalable technique for measuring network traffic, collecting, storing, and analyzing traffic data. This enables tens of thousands of interfaces to be monitored from a single location.
- sFlow is scalable, enabling it to monitor links of speeds up to 10Gb/s and beyond without impacting the performance of core internet routers and switches, and without adding significant network load.
- sFlow is a low cost solution. It has been implemented on a wide range of devices, from simple L2 workgroup switches to high-end core routers, without requiring additional memory and CPU.
- sFlow is an industry standard with a growing number of vendors delivering products with sFlow support.

sFlow is a multi-vendor sampling technology embedded within switches and routers. It provides the ability to continuously monitor application level traffic flows at wire speed on all interfaces simultaneously.

The sFlow Agent is a software process that runs as part of the network management software within a device. It combines interface counters and flow samples into sFlow datagrams that are sent across the network to an sFlow Collector. Packet sampling is typically performed by the switching/routing ASICs, providing wire-speed performance. The state of the forwarding/routing table entries associated with each sampled packet is also recorded.

The sFlow Agent does very little processing. It simply packages data into sFlow Datagrams that are immediately sent on the network. Immediate forwarding of data minimizes memory and CPU requirements associated with the sFlow Agent.

# 1.2.15-1 Collector

This section allows you to configure the s-Flow Agent Collector settings for the switch.

## Web Interface

To configure the s-Flow Agent Collector settings via the Web Interface:

- 1. Click Configuration, s-Flow Agent and Collector.
- 2. Configure the appropriate s-Flow Agent Collector settings.

3. Click the Apply button to save your changes or the Reset button to revert to previous settings.

- C 🐔 🗋 192.168.1.1				술 👮
ALLOY				ALCARDATION ]
ALLOY	ALLOY II Part Manual Come Taxon		98 <b>888888</b> (11) 11	
AMS-24T6SFP			and the second division of the second divisio	Auto-Logout 10 min - Logout Hel
				Adid-Logola To min 🔄 Logoda The
► SNMP	-		10	
▼ Configuration	SFIOW Receiv	er Configurati	on	
► Port	The second second	Configured	Current	
► ACL	Receiver Id	1	1	
► Aggregation	IP Type	IPV4 ·	1Pv4	
Spanning Tree	IP Address	0.0.0	0.0.0.0	
► IGMP Snooping	Port	6343		
MLD Snooping	0.000	1	6343	
F MVR	Time Out	0	0	
Filtering Data Base	Datagram Size	1400	1400	
> VLAN				
P VOICE VLAN	Apply Reset			
► GARP				
► GVRP				
► QoS				
▼ sFlow Agent				
Collector				
Sampler				
Loop Protection				
► Single IP				
Easy Port				
Mirroring Trap Event Severity				
SMTP Configuration				
UPnP				
► Security				
Maintenance				

Fig. 107 s-Flow Agent Collector Settings

Receiver ID:	The "Receiver ID" input field allows the user to input the receiver ID. Currently one ID is supported as one collector is supported.
IP Туре:	Here you can select to whether the Collector has an IPv4 or IPv6 Address.
IP Address:	Enter the IP Address of the s-Flow Agent Collector. The switch will send all s- Flow information to the collector.
Port:	Enter the port that the collector uses to listen to s-Flow requests. Port Range is 1 – 655365. Default is 6343.
Time Out:	This is the duration during which the collector receives samples, once the duration has expired the sampler stops sending the samples. Valid values are within the range of 0-2147483647. Default is 0.
Datagram Size:	The maximum UDP datagram size to send out sFlow samples to the receiver. The value accepted is within the range of 200-1500 bytes. Default is 1400 bytes.

*Reset Button:* Used to reset unsaved changes to original configuration.

Apply Button: Used to save the settings configured on this page.

# 1.2.15-2 Sampler

This section is used to configure the s-Flow sampling rate that is sent to the receiver. An average of 1 out of N packets/operations is randomly sampled. This type of sampling does not provide a 100% accurate result, but it does provide a result with quantifiable accuracy

### Web Interface

To configure the s-Flow Agent Sampling settings via the Web Interface:

- 1. Click Configuration, s-Flow Agent and Sampler.
- 2. Click the 🖲 button to edit the s-Flow sampling parameters.
- 3. Select whether the samples will taken from RX, TX or all packets.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.

						\$ C
Directoreases				ALCORATE A	Auto-Logout [d	OFF 💽 Logout He
sFlow Sam	pler Configur	ration				
-	1. 1. 1. 1. 1. 1. <u>1</u> . 1.		-			
sFlow Ports	sFlow Instance	Sampler Trees		May Hele Size		
1	1					0
2	1				0	ĕ
3	1				0	0
1	4				0	ě
5	1	11111			0	ĕ
6	1				0	ĕ
7	1				0	ě
8	1				0	ĕ
	1				0	ĕ
10	1	None	0	128	0	õ
11	1	None	0	128	0	0
12	1	None	0	128	0	ě
13	1	None	0	128	0	O
14	1	None	0	128	0	e
15	1	None	0	126	0	O
16	1	None	0	128	0	C
17	1	None	0	128	0	©
18	1	None	0	128	0	000000000000000000000000000000000000000
19	1	Nane	0	128	0	0
20	1	None	0	128	0	0
21	1	None	0	128	0	0
22	1	None	0	120	0	0
23	1	None	0	128	0	O
	sFlow Sam sFlow Ports 1 2 3 4 5 6 7 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22	sFlow Sampler Configur           sFlow Ports         sFlow Instance           1         1           2         1           3         1           4         1           5         1           6         1           7         1           8         1           9         1           10         1           11         1           12         1           13         1           14         1           15         1           16         1           17         1           18         1           19         1           21         1           22         1	SFlow Sampler Configuration           sFlow Ports         sFlow Instance         Sampler Type           1         1         None           2         1         None           3         1         None           4         1         None           5         1         None           6         1         None           7         1         Nane           8         1         None           10         1         None           11         1         None           12         1         None           13         1         None           14         1         None           15         1         None           16         1         None           19         1         None           20         1         None	SFlow Sampler Configuration           sFlow Ports         sFlow Instance         Sampler Type         Sampling Rate           1         1         None         0           2         1         None         0           3         1         None         0           3         1         None         0           5         1         None         0           6         1         None         0           7         1         None         0           6         1         None         0           7         1         None         0           10         1         None         0           11         1         None         0           12         1         None         0           13         1         None         0           14         1         None         0           15         1         None         0           16         1         None         0           17         1         None         0           18         1         None         0           19         1         None </td <td>Flow Sampler Configuration           sFlow Ports         sFlow Instance         Sampler Type         Sampling Rate         Max Hdr Size           1         1         None         0         128           3         1         None         0         128           3         1         None         0         128           5         1         None         0         128           6         1         None         0         128           7         1         None         0         128           6         1         None         0         128           7         1         None         0         128           8         1         None         0         128           9         1         None         0         128           10         1         None         0         128           11         1         None         0         128           12         1         None         0         128           13         1         None         0         128           14         1         None         0         128</td> <td>Flow Sampler Configuration         Sampler Type         Flow Sampling Type         Sampling Rate         Mark Hdr Size         Counter Sampling Polling Interval           1         1         None         0         128         0           3         1         None         0         128         0           5         1         None         0         128         0           5         1         None         0         128         0           6         1         None         0         128         0           7         1         None         0         128         0           6         1         None         0         128         0           7         1         None         0         128         0           7         1         None         0         128         0           10         1         None         0         128         0           11         1         None         0         128         0           12         1         None         0         128         0           13         1         None         0         128         0</td>	Flow Sampler Configuration           sFlow Ports         sFlow Instance         Sampler Type         Sampling Rate         Max Hdr Size           1         1         None         0         128           3         1         None         0         128           3         1         None         0         128           5         1         None         0         128           6         1         None         0         128           7         1         None         0         128           6         1         None         0         128           7         1         None         0         128           8         1         None         0         128           9         1         None         0         128           10         1         None         0         128           11         1         None         0         128           12         1         None         0         128           13         1         None         0         128           14         1         None         0         128	Flow Sampler Configuration         Sampler Type         Flow Sampling Type         Sampling Rate         Mark Hdr Size         Counter Sampling Polling Interval           1         1         None         0         128         0           3         1         None         0         128         0           5         1         None         0         128         0           5         1         None         0         128         0           6         1         None         0         128         0           7         1         None         0         128         0           6         1         None         0         128         0           7         1         None         0         128         0           7         1         None         0         128         0           10         1         None         0         128         0           11         1         None         0         128         0           12         1         None         0         128         0           13         1         None         0         128         0

Fig. 108 s-Flow Agent Sampler Settings



Fig. 108 s-Flow Agent Sampler Port Settings

s-Flow Ports:	Displays the ports that s-Flow is configured.
s-Flow Instance:	Configured sFlow instance for the port number.
Sampler Type:	Sampler types available are None, RX, TX and All. Default is None.
Sampling Rate:	Configured sampling rates of the port.
Max Hdr Size:	Configured size of the header of the sampled frame.
Polling Interval:	Configured polling interval for the counter sampling.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.

# 1.2.16 Loop Protection

The AMS Series switches support a Loop protection mechanism. Loop Protection can be used in environments that have devices that do not support the spanning tree protocol. If the switch receives a packet containing its own MAC address the port will be locked.

# 1.2.16-1 Configuration

This section allows you to configure the Loop Protection settings for the switch.

### Web Interface

To configure the Loop Protection settings via the Web Interface:

- 1. Click Configuration, Loop Protection and Configuration.
- 2. Select the required Action to take when a loop is detected and select whether to enable or disable TX Mode.
- 3. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Fig. 109 Loop Protection Configuration

#### **Parameter Description**

Enable Loop Protection: Used to enable or disable Loop protection on the switch.

Transmission Time:	The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds.
Shutdown Time:	The period (in seconds) for which a port will be kept disabled in the event of a loop is detection (and the port action is to shut 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).
Port:	Physical port of the switch.
Enable:	Used to enable or disable Loop Protection on each individual port.
Action:	Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port, Shutdown Port and Log or Log Only.
Tx Mode:	Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

## 1.2.16-2 Status

This section displays the Loop Protection status of individual ports.

## Web Interface

To view the Loop Protection status via the Web Interface:

- 1. Click Configuration, Loop Protection and Status.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

C n 🗋 192.168.1.1								資
ALLOY	ALLOY Bhan Branch							1
And and a second se	Duran Bridd	-						and the first state
AMS-24T6SFP								Auto-Logout 10 min · Logout Help
• IP	14							
Syslog	Loop	Protect	ion Statu	IS				Auto-refresh Refresh
► SNMP	Port	Action	Transmit	Lasar	Status	1	Time of Last Loop	
* Configuration	Port	Shutdown	Enabled	Loops 0	Down	Loop	time of Last Loop	
> Port	2	Shutdown	Enabled	0	Down		-	
+ ACL	3	Shutdown	Enabled	ő	Down			
► Aggregation	4	Shutdown	Enabled	0	Down		-	
► Spanning Tree	5	Shutdown	Enabled	0	Down			
► IGMP Snooping	6	Shutdown	Enabled	0	Down		-	
MLD Snooping	7	Shutdown	Enabled	0	Up	-	-	
► MVR	8	Shutdown	Enabled	0	Down			
► LLDP	9	Shutdown	Enabled	0	Down			
Filtering Data Base	10	Shutdown	Enabled	0	Down			
► VLAN	11	Shutdown	Enabled	0	Down	-	-	
VOICE VLAN	12	Shutdown	Enabled	0	Down	-	~	
> GARP	13	Shutdown	Enabled	0	Down		-	
+ GVRP	- 14	Shutdown	Enabled	0	Down			
► QoS	15	Shutdown	Enabled	0	Down	19	1.00	
► sFlow Agent	16	Shutdown	Enabled	0	Down		~	
V Loop Protection	17	Shutdown	Enabled	0	Down		*	
Configuration	18	Shutdown	Enabled	0	Down			
Status	19	Shutdown	Enabled	0	Down			
► Single IP	20	Shutdown	Enabled Enabled	0	Down Down			
Easy Port	21	Shutdown	Enabled Enabled	0	Down		~	
Mirroring	22 23	Shutdown	Enabled	0	Down	-	-	
Trap Event Severity	23	Shutdown	Enabled	0	Down			
SMTP Configuration	24	Shutdown	Enabled	0	Down			
UPnP	25	Shutdown	Enabled		Down	-		

#### Parameter Description

Fig. 110 Loop Protection Status

Port:	Physical port of the switch.
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.
Time of Last Loop:	The time of the last loop event detected.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page. 227

# 1.2.17 Single IP

The AMS Series switches support Single IP Management.

Single IP Management (SIM), is a simple and useful method to optimize network utilities and management, it is designed to manage a group of switches as a single entity, called a SIM group. Implementing the SIM feature will have the following advantages for users

- Simplify management of small workgroups or wiring closets while scaling networks to handle increased bandwidth demand.
- Reduce the number of IP addresses needed on the network.
- Virtual stacking structure Eliminate any specialized cables for stacking and remove the distance barriers that typically limit topology options when using other stacking technology.

# 1.2.17-1 Configuration

This section describes how to configure the Single IP Management function.

## Web Interface

To configure the Single IP Management settings via the Web Interface:

- 1. Click Configuration, Single IP and Configuration.
- 2. Set the required Mode for the switch and enter the Group Name.
- 3. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Fig. 111 Single IP Configuration

Mode:	Is used to disable the SIP function or set the device as a Master or Slave.
	Possible modes are:
	Disable: Disable operation of Single IP Management.
	Master: Enable Single IP Management and run as a Master Switch. Running
	as the master switch the user will connect to the Master switches IP Address
	and can then control the Slave switches in the same SIP group.
	Slave: Enable Single IP Management and run as a Slave Switch. The user will
	connect to the management of this switch via the Master Switches IP
	Address.
Group Name:	The specific group name of the Single IP Management Group. All switches
	that belong to this group will be controlled by the Master Switch of the
	group.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

## 1.2.17-2 Information

This section displays the slave devices and allows the administrator access to these switches.

### Web Interface

To view and configure the slave switches of the Single IP Management group via the Web Interface:

- 1. Click Configuration, Single IP and Information.
- 2. Click on the index number of the relevant switch you would like to connect to.
- 3. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 4. Click Refresh to manually refresh the information.

APS-4814545FP ×	A REAL PROPERTY OF THE REAL PR	· · · · · · · · · · · · · · · · · · ·
ALLOY		
APS-48T4S4SFP		Auto-Logout 10 min - Logout Halp
System     System Information     Information     Configuration	Single IP Information Index Model Name MAC Address	Auto-refresh 🖾 (Refresh)
CPU Load Time Account IP	T Vec-401424214, 00404640741488	
<ul> <li>Syslog</li> <li>SNMP</li> <li>Configuration</li> </ul>		
Port     ACL     Aggregation		
Spanning Tree     IGMP Snooping     MLD Snooping     MVR		
<ul> <li>LLDP</li> <li>PoE</li> <li>Filtering Data Base</li> </ul>		
► VLAN ► Voice VLAN ► GARP		
► GVRP ► QoS ► sFlow Agent		
Loop Protection	+	

Fig. 112 Single IP Information

Index:	The ID of the active Slave Switch. The parameter lets you know how many slave devices are connected to the SIP group.
Model Name:	Displays the model name of the slave switch.
MAC Address:	Displays the MAC Address of the slave switch.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.



**NOTE:** When you click the index link you will be redirected to the web interface of the slave device.

# 1.2.18 Easy Port

The AMS Series switches support a feature called Easy Port, which provides a convenient way to save and share common configurations. You can use it to enable features and settings based on the location of a switch in the network and for mass configuration deployments across the network. Predefined ports settings can be applied to particular ports for installations of IP Phones, Wireless Access Points and IP Cameras.

### Web Interface

To configure the Easy Port settings via the Web Interface:

- 1. Click Configuration and Easy Port.
- 2. Use the check boxes to enable the Easy Port function on the required ports.
- 3. Select the Role of the ports using the drop down box provided.
- 4. Specific parameters can be changed based on your requirements.
- 5. Click the Apply button to save your changes or the Reset button to revert to previous settings.

- C 🐔 🗋 192.168.1.1																\$
AMS-24T6SFP					Ņ.			1	Aut	o-Loo	tuor	OFF		Logo	ut	felp
												No.				
F IP F Syslog	Easy Port Configuration	1														
► SNMP				Ron	t Memb	ore										
* Configuration	1 2 3 4 5 6	7 8 9	10 11				16	17	18	19	20	21	22	23	24	25
► Port		0000	TUT			107	0	D	1	-	10	I	T	100	1	-
► ACL																
<ul> <li>Aggregation</li> </ul>	Role IP-Phone -															
► Spanning Tree	and the second se	-	_													
► IGMP Snooping	Access VLAN	1														
MLD Snooping     MVR	VLAN Mode	Hybrid •														
► LLDP	Voice VLAN	1000														
Filtering Data Base	Traffic Class	7(High) -														
► VLAN	Port Security	Enable -														
► Voice VLAN	Port Security Action	Trap	-													
► GARP																
► GVRP	Port Security Limit	1														
► QoS	Spanning Tree Admin Edge	Enable ·														
► sFlow Agent	Spanning Tree BPDU Guard	Enable 💌														
Loop Protection     Single IP	Apply Reset															
Configuration Information	Apply Reset															
Easy Port																
Mirroring																
Trap Event Seventy	1															
SMTP Configuration																

Fig. 113 Easy Port Configuration

#### **Parameter Description**

Port Members:

A row of check boxes for each port is displayed. To include a port in an Easy Port, check the box as  $\checkmark$ . Remove or exclude the port from the VLAN, make

sure the box is unchecked. By default, no ports are members.

Role:The port role is based on the type of devices to be connected to the switch<br/>ports. Scroll to select the type of device that will connect to the port.<br/>Options are IP-Phone, IP-CAM and WIFI-AP.

Access VLAN: Used to set the Access VLAN ID. Allowed range is 1 to 4095.

- VLAN Mode:Scroll to select the Port Egress Rule. The allowed values are Hybrid, Trunk or<br/>Access. This parameter affects VLAN egress processing. If Trunk is selected, a<br/>VLAN tag with the classified VLAN ID is inserted in frames transmitted on the<br/>port. This mode is normally used for ports connected to VLAN aware device.<br/>If Hybrid (the default value) is selected, if the classified VLAN ID of a frame<br/>transmitted on the port is different from the Port VLAN ID, a VLAN tag with<br/>the classified VLAN ID is inserted in the frame. If Access is selected, untag all<br/>frames transmitted on the port.
- Voice VLAN: Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal any other configured port PVID. A conflict will occur if the VLAN ID is the same as the management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.
- Traffic Class:Scroll to select the traffic class for the data stream priority. The available<br/>values from 0 (Low) to 7 (High). If you want voice to have a high priority then<br/>you can set the value to 7.
- Port Security:Scroll to enable or disable the Port Security function on the Port. If you turn<br/>on the function then you need to set Port Security limit to allow how many<br/>device can access the port (via MAC address).
- Port Security Action: If 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 is 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 is 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.
- Port Security limit:The maximum number of MAC addresses that can be secured. This number<br/>cannot exceed 1024. If the limit is exceeded, the corresponding action is<br/>taken. The switch is "born" with a total number of MAC addresses from<br/>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.

Spanning Tree Admin Edge: Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized).

Spanning Tree BPDU Guard: If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not effect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

- *Reset Button:* Used to reset unsaved changes to original configuration.
- Apply Button: Used to save the settings configured on this page.

# 1.2.19 Mirroring

The AMS Series switches support traffic mirroring to capture and analyze real time traffic.

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Mirror Configuration is to monitor the traffic of the network. For example, we assume that Port A and Port B are Monitoring Port and Monitored Port respectively, thus, the traffic received by Port B will be copied to Port A for monitoring.

#### Web Interface

To configure the Port Mirroring settings via the Web Interface:

- 1. Click Configuration and Mirroring.
- 2. Select the port that you wish to mirror on. This port will be used to collect the data.
- 3. Select the ports and mode that you wish to monitor. All traffic from this port will be sent to the port selected above.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Fig. 114 Port Mirroring

Port to Mirror on:	Port to mirror 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 mirroring.
Port:	Physical port of the switch.
Mode:	Used to select the Mirror Mode. <b>Rx only:</b> Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored. <b>Tx only:</b> Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored. <b>Disabled:</b> Neither frames transmitted nor frames received are mirrored. <b>Enabled:</b> Frames received and frames transmitted are mirrored on the mirror port. <b>NOTE:</b> For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames on the mirror port. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

# 1.2.20 Trap Event Severity

The AMS Series switches support trap events that can alert the administrator if a particular event occurs. This section is used to customize the severity levels of the trap events. Administrators can manually configure each event to have a Severity level of Emerg, Alert, Crit, Error, Warning, Notice, Info and Debug.

### Web Interface

To configure the Trap Event Severity levels via the Web Interface:

- 1. Click Configuration and Trap Event Severity.
- 2. Change the Severity Level of each of the Trap Events.
- 3. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Fig. 115 Trap Event Severity levels

#### **Parameter Description**

*Group Name:* The name identifying the severity group.

Severity Level:Scroll to select a severity level for each group. The following level types are<br/>supported:<br/><0> Emergency: System is unusable.<br/><1> Alert: Action must be taken immediately.<br/><2> Critical: Critical conditions.

	<3> Error: Error conditions.
	<4> Warning: Warning conditions.
	<5> Notice: Normal but significant conditions.
	<6> Information: Information messages.
	<7> Debug: Debug-level messages.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

# 1.2.21 SMTP Configuration

The AMS Series switches support trap events that can alert the administrator if a particular event occurs. This section is used to configure the mail server settings that will be used to send the emails. Email Addresses can also be configured here, these will be the addresses the events will be sent to.

## Web Interface

To configure the SMTP Configuration settings via the Web Interface:

- 1. Click Configuration and SMTP Configuration.
- 2. Enter the appropriate parameters as required.
- 3. Click the Apply button to save your changes or the Reset button to revert to previous settings.

AMS-24T6SEP ×		-1-1-1-	
C ń 🗋 192.168.1.1			(a)
ALLOY F	NLOY		- wingeran
	the Broad		ninin ninin
AMS-24T6SFP			Auto-Logout OFF - Logout Help
• IP	MTP Configu	ration	
- sysiog	Swire comigu	rauon	
► SNMP	Mail Server		
Configuration     Port	User Name		
Front	Password		
a Announdation			
Spanning Tree	Severity Level	Info 💌	
► IGMP Snooping	Sender		
	Return Path		
► MVR	Email Address 1		
LLDP     Filtering Data Base	Email Address 2		
Filtering Data base	Email Address 3		
A Marian MR MAR			
► GARP	Email Address 4		
F GVRP	Email Address 5		
	Email Address 6		
► sFlow Agent			
Loop Protection     Single IP	Apply Reset		
Easy Port			
Mirroring			
Trap Event Severity			
SMTP Configuration			
UPnP			
Security			
Maintenance -			

Fig. 116 SMTP Configuration

Mail Server:	Specify the IP Address of the mail server used to send/relay the emails.
Username:	Specify the username for the mail server. (If required)
Password:	Specify the password for the mail server. (If required)
Sender:	Enter an email address for which the emails will be sent from.
Return-Path:	Set the mail Return-Path as sender mail address.

- *Email Address 1 6:* Enter up to 6 email address to receive the trap events.
- *Reset Button:* Used to reset unsaved changes to original configuration.
- *Apply Button:* Used to save the settings configured on this page.

# 1.2.22 UPnP

The AMS Series switches support UPnP. UPnP is an acronym for Universal Plug and Play. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components.

#### Web Interface

To configure the UPnP settings via the Web Interface:

- 1. Click Configuration and UPnP.
- 2. Select to enable or disable UPnP.
- 3. Configure the required parameters.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Fig. 117 UPnP Configuration

#### **Parameter Description**

Mode:

Indicates the UPnP operation mode. Possible modes are: **Enabled:** Enable UPnP mode operation. **Disabled:** Disable UPnP mode operation. When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled.

- TTL: The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 255.
- Advertising Duration: The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.
- *Reset Button:* Used to reset unsaved changes to original configuration.
- *Apply Button:* Used to save the settings configured on this page.

# **1.3 Security**

This chapter describes the Security configuration options available in the AMS Series of switches. Features such as IP Source Guard, Port Security, HTTPS, DHCP Snooping, DHCP Relay and many more can be configured from this section.

# 1.3.1 IP Source Guard

The AMS Series switches support IP Source Guard. IP Source Guard can be used to help secure your switch from IP based spoofing attacks.

# 1.3.1-1 Configuration

This section is used to configure the IP Source Guard settings for the AMS switch.

## Web Interface

To configure the IP Source Guard settings of the switch via the Web Interface:

- 1. Click Security, IP Source Guard and Configuration.
- 2. Select to enable or disable the IP Source Guard feature.
- 3. Select to enable or disable this function on each individual port.
- 4. Select the amount of Dynamic Clients allowed to be learnt by the port.
- 5. Click the Apply button to save your changes or the Reset button to revert to previous settings.

AMS-24T6SEP ×							
C ń 🗋 192.168.1.1							Q 1
ALLOY AMS-24T6SFP	ALLON BLACK BLACK	9	<b>, 199</b>			to-Logout OFF	Logout Help
► System						io-cogour orr	instant and
+ Configuration	IP So	urce Gua	rd Configur	ation			
▼ Security	Mode	Disabled	-				
V IP Source Guard Configuration	1000 C						
Static Table	Transl	ate dynamic to	static				
Dynamic Table							
<ul> <li>ARP Inspection</li> <li>DHCP Snooping</li> </ul>	Port	Mode Co	nfiguration				
DHCP Relay			-				
► NAS	Port	Mode	Max Dynamic				
AAA     Port Security		Disabled -					
<ul> <li>Access Management</li> </ul>		Disabled •	Unlimited				
SSH	3	Long Long	Unlimited				
HTTPS Auth Method	4		Unlimited				
► Maintenance	5						
		Disabled -	Unlimited	<b>T</b>			
	7	Disabled +	Unlimited				
	8	Disabled •	Unlimited				
	9	Disabled +	Unlimited				
	10	Disabled •	Unlimited				
	11	Disabled •	Unimited				
		autority a [10]		100			

Fig. 118 IP Source Guard Configuration

Mode:	Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.
Port:	Physical port of the switch.
Mode:	Select to enable or disable the IP Source Guard function on the select port. The global IP Source Guard Mode must also be enabled, when enabling each individual port.
Max. Dynamic Clients:	Specify the maximum number of dynamic clients that can be learnt on any given port. 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, only IP Packets that have been entered into the static table will be forwarded.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

# 1.3.1-2 Static Table

This section is used to enter Static IP addresses into the AMS switch.

## Web Interface

To enter Static IP Addresses into the Static Table via the Web Interface:

- 1. Click Security, IP Source Guard and Static Table.
- 2. Click on Add New Entry.
- 3. Specify the Port, VLAN ID, IP Address and MAC Address.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.

ALLOY		
AMS-24T6SFP		Auto-Logout OFF . Logout Hal
System     Configuration	Static IP Source Guard Table	
Security VIP Source Guard	Delete Port VLAN ID IP Address MAC address	
Configuration	Delete 1 •	
Static Table Dynamic Table	Add new entry	
ARP Inspection	Apply Reset	
<ul> <li>DHCP Snooping</li> <li>DHCP Relay</li> </ul>	Abbia Liveser	
► NAS		
► AAA		
<ul> <li>Port Security</li> <li>Access Management</li> </ul>		
SSH		
HTTPS		
Auth Method Maintenance		
- Hannestanios	-	

Fig. 119 Static Table Configuration

Delete:	Check the tick box next to the required entry and press the Apply button.
Port:	Physical port of the switch.
VLAN ID:	The VLAN ID of the static entry.
IP Address:	The IP Address of the static entry.
MAC Address:	The MAC Address of the static entry.

- Add New Entry: Click to add a new static entry.
- *Reset Button:* Used to reset unsaved changes to original configuration.
- Apply Button: Used to save the settings configured on this page.

## 1.3.1-3 Dynamic Table

This section is used to view the dynamic IP Source Guard entries.

#### Web Interface

To view the Dynamic IP Addresses via the Web Interface:

- 1. Click Security, IP Source Guard and Dynamic Table.
- 2. To filter the entries you can select the Start from Port, VLAN ID and or IP Address.
- 3. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 4. Click Refresh to manually refresh the information.



Fig. 120 Dynamic Table

Physical port of the switch.
VLAN ID of the IP traffic that's permitted.
IP Address of the dynamic entry.
MAC Address of the dynamic entry.
Tick the box to enable the information to be automatically refreshed.
Used to manually refresh the information on the page.

<<, >>: The arrow keys are used to navigate between the pages, displaying the current VLAN's configured on the switch.

# 1.3.2 ARP Inspection

The AMS Series switches supports ARP Inspection. This allows the switch to intercept and examine all ARP request and response packets in a subnet and discard those packets with invalid IP to MAC address bindings.

# 1.3.2-1 Configuration

This section is used to configure the ARP Inspection settings for the AMS switch.

### Web Interface

To configure the ARP Inspection settings of the switch via the Web Interface:

- 1. Click Security, ARP Inspection and Configuration.
- 2. Select to enable or disable the ARP Inspection feature.
- 3. Select to enable or disable this function on each individual port.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Fig. 121 ARP Inspection Configuration

#### **Parameter Description**

*Mode:* Enable or Disable the Global ARP Inspection.

*Port:* Physical port of the switch.

Mode:	Select to enable or disable the ARP Inspection function on the select port. The global ARP Inspection Mode must also be enabled, when enabling each individual port.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

# 1.3.2-2 Static Table

This section is used to enter Static ARP entries into the AMS switch.

## Web Interface

To enter Static ARP entries into the Static Table via the Web Interface:

- 1. Click Security, ARP Inspection and Static Table.
- 2. Click on Add New Entry.
- 3. Specify the Port, VLAN ID, IP Address and MAC Address.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.

ALLOY		9710V
AMS-24T6SFP		Auto-Logout OFF . Logout Help
System Configuration	Static ARP Inspection Table	
Security	Delete Port VLAN ID MAC Address IP Address	
IP Source Guard     ARP Inspection		
Configuration	Add new entry	
Static Table	Apply Reset	
Dynamic Table	A subject of the second	
<ul> <li>DHCP Snooping</li> <li>DHCP Relay</li> </ul>		
> NAS		
- AAA		
► Port Security		
<ul> <li>Access Management SSH</li> </ul>		
HTTPS		
Auth Method		
Maintenance		

Fig. 122 Static Table Configuration

Delete:	Check the tick box next to the required entry and press the Apply button.
Port:	Physical port of the switch.
VLAN ID:	The VLAN ID of the static entry.
IP Address:	The IP Address of the static entry.
MAC Address:	The MAC Address of the static entry.
- Add New Entry: Click to add a new static entry.
- *Reset Button:* Used to reset unsaved changes to original configuration.
- Apply Button: Used to save the settings configured on this page.

# 1.3.2-3 Dynamic Table

This section is used to view the dynamic ARP Inspection entries.

#### Web Interface

To view the Dynamic ARP entries via the Web Interface:

- 1. Click Security, ARP Inspection and Dynamic Table.
- 2. To filter the entries you can select the Start from Port, VLAN ID and or IP Address.
- 3. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 4. Click Refresh to manually refresh the information.



Fig. 123 Dynamic Table

Port:	Physical port of the switch.
VLAN ID:	VLAN ID of the IP traffic that's permitted.
IP Address:	IP Address of the dynamic entry.
Mac Address:	MAC Address of the dynamic entry.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.

<<, >>: The arrow keys are used to navigate between the pages, displaying the current VLAN's configured on the switch.

# 1.3.3 DHCP Snooping

The AMS Series switches supports DHCP Snooping. The section describes how to configure the DHCP Snooping parameters of the switch. DHCP Snooping can prevent attackers from adding their own DHCP servers on the network.

# 1.3.3-1 Configuration

This section is used to configure the DHCP Snooping settings for the AMS switch.

#### Web Interface

To configure the DHCP Snooping settings of the switch via the Web Interface:

- 1. Click Security, DHCP Snooping and Configuration.
- 2. Select to enable or disable DHCP Snooping on the switch.
- 3. Select either trusted or untrusted for each port.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Fig. 124 DHCP Snooping Configuration

#### **Parameter Description**

Snooping Mode:Indicates the DHCP snooping mode operation. Possible modes are:Enabled:Enable DHCP snooping mode operation. When DHCP snooping<br/>mode operation is enabled, the DHCP request messages will be forwarded

	to trusted ports and only allow reply packets from trusted ports. <b>Disabled:</b> Disable DHCP snooping mode operation.
Port:	Physical port of the switch.
Mode:	Indicates the DHCP snooping port mode. Possible port modes are: <b>Trusted:</b> Configures the port as trusted source of the DHCP messages. <b>Untrusted:</b> Configures the port as untrusted source of the DHCP messages.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

## 1.3.3-2 Statistics

This section is used to view the DHCP Snooping Statistics for the AMS switch.

## Web Interface

To view the DHCP Snooping Statistics of the switch via the Web Interface:

- 1. Click Security, DHCP Snooping and Statistics.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

AMS-24T6SFP			Auto-Logout OFF 💌 Logout
<ul> <li>System</li> <li>Configuration</li> </ul>	DHCP Snooping Port S	tatistics Port 1	Port 1 💌 Auto-refresh 🗐 Refresh Glear
<ul> <li>T Security</li> <li>IP Source Guard</li> <li>ARP Inspection</li> <li>ARP Inspection</li> <li>ORCOMPARTMENT</li> <li>Configuration</li> <li>Statistics</li> <li>DHCP Relay</li> <li>NAS</li> <li>AAA</li> <li>Port Security</li> <li>Access Management</li> <li>SSH</li> <li>HTTPS</li> <li>Auth Method</li> <li>Maintenance</li> </ul>	Receive Packets Rx Discover Rx Offer Rx Request Rx Decline Rx ACK RX IAK RX Release Rx Inform Rx Lease Unarsigned Rx Lease Unarsigned Rx Lease Active	Transmit Packets 6 Tx Difecver 7 Tx Digrev 1 Tx Request 1 Tx Request 1 Tx Request 0 Tx NAK 0 Tx NAK 0 Tx NAK 0 Tx Lease Oursy 1 Tx Lease Unassigned 0 Tx Lease Active	

Fig. 125 DHCP Snooping Statistics

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.

AMS User Manual

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 Unassig	gned: The number of lease unassigned (option 53 with value 11) packets received and transmitted.
Rx and Tx Lease Unknow	<i>wn:</i> 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.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.

# 1.3.4 DHCP Replay

The AMS Series switches supports the DHCP Relay function. DHCP Relays are used to forward DHCP requests to other DHCP Server on the same or on another subnet. This section is used to configure the DHCP Relay parameters.

# 1.3.4-1 Configuration

This section is used to configure the DHCP Relay settings for the AMS switch.

## Web Interface

To configure the DHCP Relay settings of the switch via the Web Interface:

- 1. Click Security, DHCP Relay and Configuration.
- 2. Select to enable or disable the DHCP Relay function.
- 3. Enter the IP Address of the Relay Server IP Address.
- 4. Select to enable or disable the Relay Information Mode setting.
- 5. Select the appropriate Relay Information Policy.
- 6. Click the Apply button to save your changes or the Reset button to revert to previous settings.

ALLOY	-	\$
MS-24T6SFP System		Auto-Logout OFF
Configuration	DHCP Relay Configuration	
Security	Relay Mode Disabled	
IP Source Guard     ARP Inspection	Relay Server 0.0.0.0	
DHCP Snooping		
DHCP Relay		
Configuration	Relay Information Policy Replace	
Statistics	Apply Reset	
AAA	and the second s	
Port Security		
Access Management		
SSH		
HTTPS		
Auth Method Maintenance		
Maintenance		

Fig. 126 DHCP Relay Configuration

Relay Mode:	Indicates the DHCP relay mode operation. Possible modes are: <b>Enabled:</b> Enable DHCP relay mode. When the DHCP relay is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. <b>Disabled:</b> Disable the DHCP relay.
Relay Server:	Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain.
Relay Information Moa	<i>le:</i> Indicates the DHCP relay information mode option operation. Possible modes are:
	<ul> <li>Enabled: Enable DHCP relay information mode. When DHCP relay information mode is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to a DHCP server and removes it from a DHCP message when transferring to a DHCP client. It only works when DHCP relay operation mode is enabled.</li> <li>Disabled: Disable DHCP relay information mode.</li> </ul>
Relay Information Polic	<ul> <li><i>cy:</i> Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if an agent receives a DHCP message that already contains relay agent information it will enforce the policy. And it only works under DHCP if relay information operation mode is enabled. Possible policies are:</li> <li><b>Replace:</b> Replace the original relay information when a DHCP message that already contains it is received.</li> <li><b>Keep:</b> Keep the original relay information when a DHCP message that already contains it is received.</li> <li><b>Drop:</b> Drop the package when a DHCP message that already contains relay information is received.</li> </ul>
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

## 1.3.4-2 Statistics

This section is used to view the DHCP Relay Statistics for the AMS switch.

#### Web Interface

To view the DHCP Relay Statistics via the Web Interface:

- 1. Click Security, DHCP Relay and Statistics.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

<ul> <li>System</li> <li>Configuration</li> <li>Security</li> </ul>	DHCP Re Server Stati		stics				Auto	refresh 🕅 🛛 Ref	fresh Clear
IP Source Guard     ARP Inspection     DHCP Snooping     THCP Relay	Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Rece Miss Remot	ng	Receive Bad Circuit ID	Receive Ba Remote ID
Configuration Statistics	0	0	0	Q		0	0	0	
► NAS	Client Statis								
► AAA	Transmit to Client	Transmit Error	Receive from Client		Replace ent Option Ad	Keep gent Option A	Drop gent Opti	on	
Port Security     Access Management	0		0	0	0	0		0	
SSH									
HTTPS									
Auth Method Maintenance	- C								
Maniteriarice									

Fig. 127 DHCP Relay Statistics

#### Parameter Description

*Transmit to Server:* The number of packets that are relayed from client to server.

*Transmit Error:* The number of packets that resulted in errors while being sent to clients.

*Receive from Server:* The number of packets received from server.

Receive Missing Agent Option: The number of packets received without agent information options.

Receive Missing Circuit ID: The number of packets received with the Circuit ID option missing.

Receive Missing Remote ID: The number of packets received with the Remote ID option missing.

AMS User Manual

*Receive Bad Circuit ID:* The number of packets whose Circuit ID option did not match known circuit ID.

*Receive Bad Remote ID:* The number of packets whose Remote ID option did not match known Remote ID.

## **Client Statistics**

Transmit to Client:	The number of relayed packets from server to client.
Transmit Error:	The number of packets that resulted in error while being sent to servers.
Receive from Client:	The number of received packets from server.
Receive Agent Option:	The number of received packets with relay agent information option.
Replace Agent Option:	The number of packets which were replaced with relay agent information option.
Keep Agent Option:	The number of packets whose relay agent information was retained.
Drop Agent Option:	The number of packets that were dropped which were received with relay agent information.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.

# 1.3.5 NAS

The AMS Series switches supports a NAS (Network Access Server) function which allows users connection to a variety of resources, including the internet. Particular settings can be applied to this user based on authentication to a RADIUS Server. Functions such as 802.1x and Mac based Authentication can be used to authenticate users onto the network allowing them access to these shared resources.

# 1.3.5-1 Configuration

This section is used to configure the NAS settings for the AMS switch.

## Web Interface

To configure the NAS settings of the switch via the Web Interface:

- 1. Click Security, NAS and Configuration.
- 2. Enable and configure the system wide parameters for the NAS server.
- 3. Configure the required settings for each of the ports that will utilize the NAS function.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.

C f [ 192.168.1.1										ť	2
					-						-
ALLOY	ALLOY El Pert Manual		-		-	THEFT	Arcal	1072			
	Married Street							÷			
AMS-24T6SFP	6					1.0.0.0		Auto	Logout OFF	Logout H	elp
									collour [ out ] [m	Intelligible intelligible	
System	Netw	ork Access S	erver	Configu	rati	on				Refresh	
Configuration     Security	Network Access Server Co			connigu	- un	U.I.				Feareist	
F IP Source Guard	System	Configuration									
► ARP Inspection	Mode			Disab	led						
DHCP Snooping	Reau	thentication Enal	bled								
DHCP Relay	Reaut	thentication Perio	od	3600		seconds					
▼ NAS Configuration	EAPO	L Timeout		30		seconds					
Switch Status	Aging Period			300		seconds					
Port Status	Hold	Time		10	-	seconds					
► AAA	RADIUS-Assigned QoS Enabled				-	34201102					
Port Security     Access Management		JS-Assigned VLA									
SSH	Gues	t VLAN Enabled									
HTTPS	Gues	t VLAN ID		1							
Auth Method	Max.	Reauth. Count		2							
<ul> <li>Maintenance</li> </ul>	Allow	Guest VLAN if EA	APOL S	een .							
	Port C	onfiguration									
	1000			RADIUS		RADIUS-	Guest	I Sectore and			
	Port	Port Admin State		Assigned		Assigned	VLAN	Port State	Rest	tart	
	-	0	-	QoS Enabl	ed	VLAN Enabled	Enabled				
			-					Globally			£1
	1	Force Authorized	Ŧ					Disabled	Reauthenticate	Reinitialize	Ŀ.
	2	Force Authorized						Globally Disabled	Reauthenticate	Reinitialize	
			1000					Globalls			83

Fig. 128 Network Access Server Configuration

#### **Parameter Description**

Mode:	Indicates if NAS is globally enabled or disabled on the switch. If globally
	disabled, all ports are allowed forwarding of frames.

Reauthentication Enabled: 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: 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 1 to 3600 seconds.

EAPOL Timeout:Determines the time for retransmission of Request Identity EAPOL frames.Valid values are in the range 1 to 255 seconds. This has no effect for MAC-<br/>based ports.

Aging Period:This setting applies to the following modes, i.e. modes using the PortSecurity functionality to secure MAC addresses:

- Single 802.1X
- Multi 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 PortSecurity functionality to secure MAC addresses:

Single 802.1XMulti 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 request times out (according to the timeout specified on the "Configuration $\rightarrow$ Security $\rightarrow$ AAA" page) - 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.

RADIUS-Assigned QoS Enabled: RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description)

The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

RADIUS-Assigned VLAN Enabled: RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUSassigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description).

The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determine whether RADIUS-

assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

*Guest VLAN Enabled:* A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.

The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

- Guest VLAN ID:This is the value that a port's Port VLAN ID is set to if a port is moved into<br/>the Guest VLAN. It is only changeable if the Guest VLAN option is globally<br/>enabled.<br/>Valid values are in the range [1; 4095].
- Max. Reauth. Count: The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 255].
- Allow Guest VLAN if EAPOL Seen: The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port.

The value can only be changed if the Guest VLAN option is globally enabled.

- *Port Configuration:* The table has one row for each port on the selected switch and a number of columns, which are:
- *Port:* Physical port of the switch.
- Admin State:If NAS is globally enabled, this selection controls the port's authentication<br/>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.

Port-based 802.1X: 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 authenticator 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 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, 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 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 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.

Single 802.1X: In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

**Multi 802.1X:** In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Multi 802.1X variant.

Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

In Multi 802.1X it is not possible to use the multicast BPDU MAC address as

destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.

The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

**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", 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 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 advantage of MAC-based authentication over 802.1X-based authentication is 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. RADIUS-Assigned QoS Enabled: When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e.

- Port-based 802.1X
- Single 802.1X

RADIUS attributes used in identifying a QoS Class:

Refer to the written documentation for a description of the RADIUS attributes needed in order to successfully identify a QoS Class. The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.

Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '3', which translates into the desired QoS Class in the range [0; 3].

RADIUS-Assigned VLAN Enabled: When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.

If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e.

- Port-based 802.1X
- Single 802.1X

	For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.
	<ul> <li>RADIUS attributes used in identifying a VLAN ID:</li> <li>RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:</li> <li>The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.</li> <li>The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):</li> <li>Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).</li> <li>Value of Tunnel-Type must be set to "VLAN" (ordinal 13).</li> <li>Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].</li> </ul>
Guest VLAN Enabled:	<ul> <li>When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below.</li> <li>This option is only available for EAPOL-based modes, i.e.:</li> <li>Port-based 802.1X</li> <li>Single 802.1X</li> <li>Multi 802.1X</li> <li>For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.</li> </ul>
	Guest VLAN Operation: When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down

	or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.
	Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.
	While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.
Port State:	The current state of the port. It can undertake one of the following values: <b>Globally Disabled:</b> NAS is globally disabled. <b>Link Down:</b> NAS is globally enabled, but there is no link on the port. <b>Authorized:</b> The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized. <b>Unauthorized:</b> The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server. <b>X Auth/Y Unauth:</b> The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.
Restart:	Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL- based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect. <b>Reauthenticate:</b> 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.
	<b>Reinitialize:</b> 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.
Refresh:	Used to manually refresh the information on the page.

*Reset Button:* Used to reset unsaved changes to original configuration.

Apply Button: Used to save the settings configured on this page.

## 1.3.5-2 Switch Status

This section is used to view the NAS Status Information on the AMS switch.

## Web Interface

To view the NAS information via the Web Interface:

- 1. Click Security, NAS and Switch Status.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

ALLOT/		_		_	_		_	
ALLOY	ALLOY Therefore	-	000000	14444	- 26		41072	
AMS-24T6SFP		- 644	UNANAA	dra an	olon y		Autol	ogout OFF - Logout Help
							Auto-t	ugua orr in cogoar her
<ul> <li>System</li> <li>Configuration</li> </ul>	Netwo	ork Access S	erver Switch	h Status				Auto-refresh
V Security	-							
F IP Source Guard	Port	Admin State	Port State Globally Disabled	Last Source	Last ID	QoS Class	Port VLAN ID	
► ARP Inspection	1 2	Force Authorized						
DHCP Snooping		Force Authorized						
> DHCP Relay	4	Force Authorized						
TNAS	5	Force Authorized						
Configuration	6	Force Authorized						
Switch Status	I	Force Authorized						
Port Status	8 9	Force Authorized						
- AAA		Force Authorized						
F Port Security	11	Force Authorized						
Access Management		Force Authorized						
SSH SSH		Force Authorized	Globally Disabled					
HTTPS	14	Force Authorized						
	15	Force Authorized						
Auth Method	16	Force Authorized						
Maintenance	17 18	Force Authorized						
		Force Authorized						
		Force Authorized						
	21	Force Authorized	Globally Disabled					
		Force Authorized						
		Force Authorized						
		Force Authonzed Force Authonzed						
		Force Authorized						
	20	- orde Particuized	contrary provided					

Fig. 129 Network Access Server Status

Port:	Physical port of the switch. Click on the port number to view details for statistics.
Admin State:	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
Port State:	The current state of the port. Refer to NAS Port State 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.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.

## 1.3.5-3 Port Status

This section is used to view the Port Status of the NAS function on the AMS switch.

## Web Interface

To view the Port related NAS information via the Web Interface:

- 1. Click Security, NAS and Port Status.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

AMS-24T6SFP  System Configuration NAS S		Auto-Logout OFF 💌 Logout Het
	Statistics Port 1	Port 1 💌 Auto-refresh 📃 Refresh
Security Port St	ate	
IP Source Guard     ARP Inspection     Admin	State Force Authorized	
DHCP Snooping Port S		
► DHCP Relay		
* NAS		
Configuration		
Switch Status		
Port Status		
AAA     Port Security		
Access Management		
SSH		
HTTPS		
Auth Method		
Maintenance		

Fig. 130 Network Access Server Port Status

Admin State:	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
Port State:	The current state of the port. Refer to NAS Port State for a description of the individual states.
Port:	Select the required port from the drop down box at the top of the screen.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.

# 1.3.6 AAA

The AMS Series switches supports AAA (Authentication, Authorization, Accounting) to provide access control to your network. The AAA server can be a TACACS+ or RADIUS server to create and manage objects that contain settings for using AAA servers.

# 1.3.6-1 Configuration

This section is used to configure the AAA settings for the AMS switch.

## Web Interface

To configure a Common Configuration of AAA in the web interface:

- 1. Click Security, AAA and Configuration.
- 2. Set Timeout (Default is 15 seconds).
- 3. Set Dead Time (Default is 300 seconds).

To configure a TACACS+ Authorization and Accounting Configuration of AAA in the web interface:

- 1. Click Security, AAA and Configuration.
- 2. Select "Enabled" in the Authorization.
- 3. Select "Enabled" in the Failback to Local Authorization.
- 4. Select "Enabled" in the Account.

To configure a RADIUS Authentication Server Configuration of AAA in the web interface:

- 1. Check "Enabled".
- 2. Specify IP address or Hostname for Radius Server.
- 3. Specify Authentication Port for Radius Server (Default is 1812).
- 4. Specify the Secret with Radius Server.

To configure a RADIUS Accounting Server Configuration of AAA in the web interface:

- 1. Check "Enabled".
- 2. Specify IP address or Hostname for Radius Server.
- 3. Specify Authentication Port for Radius Server (Default is 1813).
- 4. Specify the Secret with Radius Server.

To configure a TACACS+ Authentication Server Configuration of AAA in the web interface:

- 1. Check "Enabled".
- 2. Specify IP address or Hostname for TACACS+ Server.
- 3. Specify Authentication Port for TACACS+ Server (Default is 49).
- 4. Specify the Secret with TACACS+ Server.

- C # 192.168.1.1					57
12 2.0.12225					
ALLOV	ALLOY			ALCOLUMNY .	
	Charles Annual Sectors		*****		
AMS-24T6SFP				Auto-Logout OFF	Logout Help
► System					
Configuration	Authentica	tion Server Configura	ation		Í
V Security	Common Serv	er Configuration			
FIP Source Guard		C. C			
ARP Inspection     DHCP Snooping	Timeout	15 seconds			
<ul> <li>DHCP Relay</li> </ul>	Dead Time	300 seconds			
► NAS	TACACS+ Aut	norization and Accounting C	onfiguration		
* AAA		states and a set a set of a			
Configuration	Authorization		and the second sec		
RADIUS Overview RADIUS Details	Fallback to L	ocal Authorization Disable			
Port Security	Accounting	Disable	d 💌		
Access Management	PADILIS Autho	ntication Server Configurat	ion		
SSH		and a surface of the			
HTTPS	# Enabled	IP Address/Hostname	Port	Secret	
Auth Method	1 💷		1812		
Maintenance	2		1812		
	3		1812		
	4		1012		
	5 🗔		1812		
		inting Server Configuration			
	# Enabled	IP Address/Hostname	Port	Secret	
	1 2 3		1813		
			1813		

Fig. 131 AAA Configuration

Timeout:	The Timeout, which can be set to a number between 3 and 3600 seconds, is
	the maximum time to wait for a reply from a server.
	If the server does not reply within this timeframe, we will consider it to be
	dead and continue with the next enabled server (if any).
	RADIUS servers are using the UDP protocol, which is unreliable by design. In
	order to cope with lost frames, the timeout interval is divided into 3
	subintervals of equal length. If a reply is not received within the subinterval,
	the request is transmitted again. This algorithm causes the RADIUS server to
	be queried up to 3 times before it is considered to be dead.
Dead Time:	The Dead Time, which can be set to a number between 0 and 3600 seconds,
	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 Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

TACACS+ Authorization and Accounting Configuration

Authorisation: Every command will be authorized by the TACACS+ server when enabled. The authorization table on the TACACS+ server is able to configure which command can be passed successfully. For example, TACACS+ server is set to accept STP command but deny VLAN command. The server will block any commands related to VLAN's entered by the user, but it will allow STP commands to be configured when entered by the user

Fallback to Local Auth:Enable to allow the user who typed wrong account or password to login<br/>successfully when the user account is on the local authorization list of the<br/>local switch. For example, when user entered the wrong account or<br/>password, TACACS+ server will refer to the account information on the local<br/>end of switch. If the account is recorded on the local switch, the user will be<br/>authorized to login with the privilege level set on the local switch.

Accounting: Enable to record all commands entered by a specific user. All the log data will be recorded on the server when enabled. For instance, login time, log out time, IGMP setting, VLAN setting, etc.

**RADIUS** Authentication Server Configuration

#:	The RADIUS Authentication Server number for which the configuration below applies.	
Enabled:	Enable the RADIUS Authentication Server by checking this box.	
IP Address/Hostname:	The IP address or hostname of the RADIUS Authentication Server. IP address is expressed in dotted decimal notation.	
Port:	The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server.	
Secret:	The secret - up to 29 characters long - shared between the RADIUS Authentication Server and the switch.	
RADIUS Accounting Server Configuration		
#:	The RADIUS Accounting Server number for which the configuration below applies.	
Enabled:	Enable the RADIUS Accounting Server by checking this box.	

IP Address/Hostname:	The IP address or hostname of the RADIUS Accounting Server. IP address is expressed in dotted decimal notation.
Port:	The UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server.
Secret:	The secret - up to 29 characters long - shared between the RADIUS Accounting Server and the switch.
TACACS+ Authenticatio	n Server Configuration
#:	The TACACS+ Authentication Server number for which the configuration below applies.
Enabled:	Enable the TACACS+ Authentication Server by checking this box.
IP Address/Hostname:	The IP address or hostname of the TACACS+ Authentication Server. IP address is expressed in dotted decimal notation.
Port:	The TCP port to use on the TACACS+ Authentication Server. If the port is set to 0 (zero), the default port (49) is used on the TACACS+ Authentication Server.
Secret:	The secret - up to 29 characters long - shared between the TACACS+ Authentication Server and the switch.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

# 1.3.6-2 RADIUS Overview

This section is used show you an overview of the status of the RADIUS Authentication and Accounting servers.

### Web Interface

To view the RADIUS Server overview in the web interface:

- 1. Click Security, AAA and RADIUS Overview.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.



Fig. 132 RADIUS Overview

#### Parameter Description

RADIUS Authentication Servers Status Overview

#:	The RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address:	The IP address and UDP port number (in <ip address="">:<udp port=""> notation) of this server.</udp></ip>
State:	The current state of the server. This field takes one of the following values: Disabled: The 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 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.

**RADIUS Accounting Servers Status Overview** 

#:	The RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address:	The IP address and UDP port number (in <ip address="">:<udp port=""> notation) of this server.</udp></ip>
State:	The current state of the server. This field takes one of the following values: Disabled: The server is disabled.
	<b>Not Ready:</b> The server is enabled, but IP communication is not yet up and running.
	<b>Ready:</b> The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
	<b>Dead (X seconds left):</b> 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.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.

# 1.3.6-3 RADIUS Details

This section shows you detailed information of the RADIUS Accounting and Authentication Statistics.

### Web Interface

To view the RADIUS Detailed Information in the web interface:

- 1. Click Security, AAA and RADIUS Details.
- 2. Specify the Server you wish to view statistics for.
- 3. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 4. Click Refresh to manually refresh the information.

ALLOV		the set		ette petterni	
AMS-24T6SFP					Auto-Logout OFF 💌 Logout Help
► System	RADIUS Authentication St	atisti	ins	Essue	r#1 + Auto-refresh 🗌 Refresh Clear
<ul> <li>Configuration</li> </ul>	RADIOS Addientication St	ausu	0.5	Delve	Auto-refresh L Refresh Glear
* Security	Receive Packets		Transmit Packets		
IP Source Guard	Access Accepts	0	Access Requests	.0.	
ARP Inspection	Access Rejects		Access Retransmissions	0	
DHCP Snooping	Access Challenges	0		0	
DHCP Relay	Malformed Access Responses		Timeouts	0	
► NAS	Bad Authenticators	0			
* AAA	Unknown Types	0			
Configuration	Packets Dropped	0			
RADIUS Overview	Concernant of the second se	Othe	er Info		
RADIUS Defails	IP Address		0	0 0 0 1812	
	State			Disabled	
► Port Security	Round Trip Time			0 ms	
Access Management     SSH	RADIUS Accounting Statis	stics	for Server #1		
HITPS	Receive Packets		Transmit Packets		
Auth Method	Responses	0	Requests	0	
<ul> <li>Maintenance</li> </ul>	Malformed Responses	Q		0	
	Bad Authenticators		Pending Requests	U	
	Unknown Types		Timeouts	۵	
	Packets Dropped	Û			
	and server	Othe	er Info		
	IP Address		0	0.0.0 1813	
	State Round-Trip Time			Disabled	
	Round- Inp Lime			0 mis	

Fig. 133 RADIUS Detailed Statistics

#### **Parameter Description**

**RADIUS** Authentication Statistics

*Packet Counters:* RADIUS authentication server packet counter. There are seven receive and four transmit counters.

Direction	Name	RFC4668 Name	Description
Rx		Acconts	The number of RADIUS Access-Accept packets (valid or invalid) received from the

			server.
Rx	Access Rejects	radiusAuthClientExtAccessR ejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	Access Challenges	radiusAuthClientExtAccessC hallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	Malformed Access Responses	radiusAuthClientExtMalfor medAccessResponses	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 Authenticato rs	radius Auth Client Ext Bad Aut henticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx	Unknown Types	radiusAuthClientExtUnkno wnTypes	The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.
Rx	Packets Dropped	radiusAuthClientExtPackets Dropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Тх	Access Requests	radius Auth Client Ext Access R equests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Тх	Access Retransmissi ons	radiusAuthClientExtAccessR etransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Тх	Pending Requests	radiusAuthClientExtPendin gRequests	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, Access- Reject, Access-Challenge, timeout, or retransmission.
Tx	Timeouts	radius Auth Client Ext Timeou ts	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.

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

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 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 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	radiusAuthClientExtRoundT ripTime	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.

## **RADIUS Accounting Statistics**

Packet Counters:RADIUS authentication server packet counter. There are five receive and<br/>four transmit counters.

Direction	Name	RFC4670 Name	Description
Rx	Responses	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	Malformed Responses	radiusAccClientExtMalformed Responses	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	radiusAcctClientExtBadAuthe nticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	Unknown Types	radiusAccClientExtUnknownT ypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	Packets Dropped	radius Acc Client Ext Packets Dro pped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Тх	Requests	radius Acc Client Ext Requests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Тх	Retransmissions	radius Acc Client Ext Retransmis	The number of RADIUS packets

## AMS User Manual

		sions	retransmitted to the RADIUS accounting server.
Тх	Pending Requests	radiusAccClientExtPendingRe quests	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.
Тх	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.

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

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.

*Auto*-Refresh: Tick the box to enable the information to be automatically refreshed.

*Refresh:* Used to manually refresh the information on the page.

## 1.3.7 Port Security

The AMS Series switches supports a Port Security function allowing the administrator to specify the amount MAC Addresses allowed to be accessed by an individual port.

## 1.3.7-1 Limit Control

This section is used to configure the amount of MAC Addresses allowed to by the port and you can also specify the action taken once this configured threshold has been reached

## Web Interface

To configure the Port Security limitations via the web interface:

- 1. Click Security, Port Security and Limit Control.
- 2. Specify the appropriate system settings for your configuration.
- 3. Enable per port settings based on your requirements.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.

C n 🗋 192.168.1.1									ជ
AMS-24T6SFP	ALLON State Manager State Team	9.	-		<b></b>			Auto-Logout OFF	Logout Help
System     Configuration	Port S	Security	Limit Cor	trol Cont	figuratio	n			Refresh
* Security	System	Configura	tion						
IP Source Guard     ARP Inspection     DHCP Snooping	Mode		Disabled	×					
► DHCP Relay ► NAS		Enabled Period	3600 s	econds					
- AAA	Port Co	onfiguratio	n						
Port Security     Limit Control	Port	Mode	Limit	Act		State	Re-open		
Switch Status		0	-	0	-				
Port Status • Access Management	1	Disabled	- 4	None	+	Disabled	Reapen		
SSH	2	Disabled	- 4	Mane	1	Disabled	Reopen		
HTTPS	з	Desabled	- 4	Nane		Disabled	Reopen		
Auth Method	4	Desabled	- 4	None	-	Disabled	Reopen		
r maintenance	5	Desabled	- 4	None	-	Disabled	Reapen		
	6	Disabled	- 4	None	17	Disabled	Reopen		
	7	Disabled	- 4	None	1	Disabled	Reopen		
	8	Disabled		None	[-]	Disabled	Reopen		
	9	Disabled		None	[+]	Disabled	Reopen		
	10	Disabled		None	[-]	Disabled	Reopen		
	11	Disabled	-			Disabled	Reopen		

Fig. 134 Port Security Limit Control

### **Parameter Description**

Mode:

Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

AMS User Manual

Aging Enabled:If checked, secured MAC addresses are subject to aging as discussed under<br/>Aging Period.

Aging Period:If Aging Enabled is checked, then the aging period is controlled with this<br/>input. If other modules are using the underlying port security for securing<br/>MAC addresses, they may have other requirements to the aging period. The<br/>underlying port security will use the shorter requested aging period of all<br/>modules that use the functionality.<br/>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

Port:	Physical port of the switch.
Mode:	Controls whether Limit Control is enabled 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 Limit is reached, the switch can take one of the following actions: <b>None:</b> Do not allow more than Limit MAC addresses on the port, but take no further action.

	<b>Trap:</b> If Limit + 1 MAC addresses is 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 is exceeded.
	<ul> <li>Shutdown: If Limit + 1 MAC addresses is 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:</li> <li>Reboot the switch.</li> <li>Disable and re-enable Limit Control on the port or the switch.</li> <li>Click the Reopen button.</li> </ul>
	<b>Trap &amp; Shutdown:</b> If Limit + 1 MAC addresses is 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: <b>Disabled:</b> Limit Control is either globally disabled or disabled on the port.
	<b>Ready:</b> The limit is not yet reached. This can be shown for all actions.
	<b>Limit Reached:</b> Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap.
	<b>Shutdown:</b> 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 shut down 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 Shut down in the Action section.
i	<b>NOTE: T</b> hat clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost
Refresh:	Used to manually refresh the information on the page.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

## 1.3.7-2 Switch Status

This section shows the Port Security status. Port Security is a module with no direct configuration. 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. The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

### Web Interface

To view the Port Security Switch Status via the web interface:

- 1. Click Security, Port Security and Switch Status.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

- C f 192168.1.1						\$
		-				(2)
ALLOY	ALLOY				-	MEANWY
and the second	El Part Manage		- 6			
AMS-24T6SFP		_				Auto-Logout OFF 🖃 Logout Hel
► System	an 11					
► Configuration	Port	Secur	ty Swite	ch Statu:	s	Auto-refresh 📉 Refresh
▼ Security	User	lodule L	egend			
F IP Source Guard						
► ARP Inspection	Limit C		Name A	bbr		
DHCP Snooping	802.1)		L			
DHCP Relay NAS		Snooping				
> AAA	Voice	VLAN	V			
V Port Security	Port S	atus				
Limit Control						
Switch Status	Port	Users	State	MAC Co Current		
Port Status			Desabled	Current	Limit	
► Access Management	2		Disabled			
SSH	3		Disabled	-	-2	
HTTPS	4		Disabled			
Auth Method	2		Disabled Disabled	2	-	
► Maintenance	2		Disabled			
	8		Disabled			
	9		Disabled	-		
	10		Disabled		14	
	11 12		Disabled Disabled			
	13	~~~~	Disabled			
	14	warm to	Disabled		T	
	15		Disabled			
	16		Disabled	-		
	17		Disabled		4	
	18 19		Disabled Disabled		-	

Fig. 135 Port Security Switch Status

### **Parameter Description**

User Module Legend

*User Module Name:* The full name of a module that may request Port Security services.

AMS User Manual

Abbr:	A one-letter abbreviation of the user module. This is used in the Users column in the port status table.
Port Status	
Port:	The port number for which the status applies. Click the port number to see the status for this particular port.
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:
	<b>Disabled:</b> No user modules are currently using the Port Security service.
	<b>Ready:</b> The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.
	<b>Limit Reached:</b> The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.
	<b>Shutdown:</b> 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 reopened on the Limit Control configuration Web-page.
MAC Count:	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 (-). Indicates the number of currently learned MAC addresses (forwarding as well as blocked) on the port. If no user modules are enabled on the port, a dash (-) will be shown.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.

## 1.3.7-3 Port Status

This section shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. 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.

### Web Interface

To view the Port Security Switch Status via the web interface:

- 1. Click Security, Port Security and Port Status.
- 2. Select the port from the drop down box you would like to view the status of.
- 3. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 4. Click Refresh to manually refresh the information.



Fig. 136 Port Security Port Status

MAC Address and VLAN	ID: The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learnt, 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.
<i>Time of Addition:</i>	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.
Auto-Refresh:	Tick the box to enable the information to be automatically refreshed.
Refresh:	Used to manually refresh the information on the page.

## 1.3.8 Access Management

The AMS Series switches supports a number of methods for configuring the switch. This section is used to allow/deny specific IP Addresses from accessing HTTP/HTTPS, SNMP or Telnet/SSH access.

## 1.3.8-1 Configuration

This section is used to configure the Access Management function of the AMS Series switch.

## Web Interface

To configure the Access Management settings via the web interface:

- 1. Click Security, Access Management and Configuration.
- 2. Click Add New Entry.
- 3. Specify the start and end IP Address and select the type of access allowed.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Fig. 137 Access Management Configuration

### **Parameter Description**

Mode:Indicates the access management mode operation. Possible modes are:Enabled: Enable access management mode operation.Disabled: Disable access management mode operation.

Delete:	Check to delete the entry. It will be deleted during the next save.
Start IP Address:	Indicates the start IP address for the access management entry.
End IP Address:	Indicates the end IP address for the access management entry.
HTTP/HTTPS:	Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.
SNMP:	Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.
TELNET/SSH:	Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

## 1.3.8-2 Statistics

This section is used to view the statistics of the Access Management function of the AMS Series switch.

### Web Interface

To view the Access Management statistics via the web interface:

- 1. Click Security, Access Management and Statistics.
- 2. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
- 3. Click Refresh to manually refresh the information.

			kakaka kakaka		
AMS-24T6SFP	-				Auto-Logout OFF 🖃 Logout
System Configuration	Access M	lanagement Sta	atistics		Auto-refresh 🔲 Refresh Clear
Security > IP Source Guard		<b>Received Packets</b>		Discarded Packets	
ARP Inspection	HTTP	0	0	0	
DHCP Snooping	SNMP	0		0	
> DHCP Relay	TELNET	0	0		
► NAS	SSH	0	Ó	0	
► AAA					
Port Security					
Access Management Configuration Statistics					
SSH					
HTTPS					
Auth Method					
Maintenance	8				

Fig. 138 Access Management Statistics

Interface:	The interface type through which the remote host can access the switch.
Received Packets:	Number of received packets from the interface when access management mode is enabled.
Allowed Packets:	Number of allowed packets from the interface when access management mode is enabled.
Discarded Packets:	Number of discarded packets from the interface when access management mode is enabled.

*Auto*-Refresh: Tick the box to enable the information to be automatically refreshed.

*Refresh:* Used to manually refresh the information on the page.

## 1.3.9 SSH

The AMS Series switches supports SSH access to the management interface. SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication.

## Web Interface

To enable/disable SSH via the web interface:

- 1. Click Security and SSH.
- 2. Select to enable or disable SSH.
- 3. Click the Apply button to save your changes or the Reset button to revert to previous settings.

AMS-24T6SEP ×	Contraction of the second s	
- C n 🗋 192.168.1.1		ĝ
ALLOY AMS-24T6SFP		Auto-Logout OFF V Logout Help
System     Configuration	SSH Configuration	
Security	Mode Enabled -	
<ul> <li>IP Source Guard</li> <li>ARP Inspection</li> </ul>		
<ul> <li>DHCP Snooping</li> </ul>	Apply Reset	
> DHCP Relay		
NA5		
AAA     Port Security		
► Access Management		
SSH		
HTTPS Auth Method		
Maintenance		

Fig. 139 SSH Configuration

Mode:	Indicates the SSH mode operation. Possible modes are: <b>Enabled:</b> Enable SSH mode operation. <b>Disabled:</b> Disable SSH mode operation.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

## 1.3.10 HTTPS

The AMS Series switches supports HTTPS access to the management interface. HTTPS is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication via the browser.

### Web Interface

To enable/disable HTTPS via the web interface:

- 1. Click Security and HTTPS.
- 2. Select to enable or disable HTTPS.
- 3. Select to enable Automatic Redirect of HTTP to HTTPS
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.

E) AMS-20165FP ×		
		Auto-Logout OFF  Logout Help
<ul> <li>System</li> <li>Configuration</li> <li>Security</li> <li>IP Source Guard</li> <li>ARP Inspection</li> <li>DHCP Snooping</li> <li>DHCP Relay</li> <li>NAS</li> <li>AAA</li> <li>Port Security</li> <li>Access Management SSH</li> <li>HTTPS Auth Method</li> <li>Maintenance</li> </ul>	HTTPS Configuration	

Fig. 140 HTTPS Configuration

Mode:	Indicates the HTTPS mode operation. Possible modes are:
	Enabled: Enable HTTPS mode operation.
	Disabled: Disable HTTPS mode operation.
Automatic Redirect:	Indicates the HTTPS redirect mode operation. Automatically redirect web browser to HTTPS when HTTPS mode is enabled. Possible modes are:

**Enabled:** Enable HTTPS redirect mode operation. **Disabled:** Disable HTTPS redirect mode operation.

*Reset Button:* Used to reset unsaved changes to original configuration.

Apply Button: Used to save the settings configured on this page.

## 1.3.11 Auth Method

The AMS Series switches support different ways of authenticating a user when logging into the management of the switch. Authentication can be done locally, via TACACS+ or via RADIUS.

### Web Interface

To configure the Authentication Method via the web interface:

- 1. Click Security and Auth Method.
- 2. Select the Authentication method for console, telent, ssh and web access.
- 3. Select to enable Fallback.
- 4. Click the Apply button to save your changes or the Reset button to revert to previous settings.

ALLOY	-			 -		
ALLOY	ALLON March Research		122 233			
AMS-24T6SFP	_			Auto-L	ogout OFF 💌 Logou	it Help
System Configuration	Auther	ntication Method Co	onfiguration			
Security > IP Source Guard	Client	Authentication Method	Fallback			
ARP Inspection	console	local	-			
<ul> <li>DHCP Snooping</li> </ul>	teinet	local 💌				
DHCP Relay NAS	ssh	local				
AAA	web	local 🔹				
Port Security     Access Management     SSH     HTTPS     Auth Method     Maintenance	Apply	Rush				

Fig. 141 Authentication Method Configuration

### Parameter Description

*Client:* The management client for which the configuration below applies.

Authentication Method: Authentication Method can be set to one of the following values:
 None: authentication is disabled and login is not possible.
 Local: use the local user database on the switch for authentication.
 Radius: use a remote RADIUS server for authentication.
 Tacacs+: use a remote TACACS+ server for authentication.

<i>Fallback:</i> Enable fallback to local authentication by checking this box.	
	If none of the configured authentication servers are alive, the local user
	database is used for authentication.
	This is only possible if the Authentication Method is set to a value other than
	'none' or 'local'.
Reset Button:	Used to reset unsaved changes to original configuration.
Apply Button:	Used to save the settings configured on this page.

## **1.4 Maintenance**

This chapter describes all of the switch Maintenance configuration tasks to enhance the performance of the switch, including Restart Device, Firmware upgrade, Save/Restore, Import/Export, and Diagnostics.

## 1.4.1 Restart Device

This section explains how to restart the device.

### Web Interface

To restart the switch via the Web Interface:

- 1. Click Maintenance and Restart Device.
- 2. Click Yes to restart the device.

AMS-20165FP 8		
← → C ♠ 🕒 192.168.1.1		☆ =
AMS-24T6SFP		Auto-Logout OFF 🕞 Logout Help
<ul> <li>System</li> <li>Configuration</li> </ul>	Restart Device	
Security     Maintenance     Restart Device     Firmware     Save/Restore	Are you sure you want to perform a Restart?	
Export/Import     Diagnostics	Yes No	

Fig. 142 Restart Device

### **Parameter Description**

*Restart Device:* You can restart the switch on this page. After restart, the switch will boot normally.

Yes: Click "Yes" to restart the device.

No: Click to undo any restart action.

## 1.4.2 Firmware

This section is used to upgrade the firmware in the AMS Series switches. Firmware updates are provided periodically to provide bug fixes and features enhancements. The AMS Series switches support Dual Firmware Images, allowing the administrator to upload two firmware images into the switch. This allows you to easily roll back to a previous version, if you have issues with a new firmware that you have loaded.

## 1.4.2-1 Firmware Upgrade

This section is used to upgrade the firmware in the AMS switch.

### Web Interface

To upgrade the firmware in the switch via the Web Interface:

- 1. Click Maintenance, Firmware and Firmware Upgrade.
- 2. Click browse to select your firmware files and click upload to apply the new firmware.



Fig. 143 Firmware Upgrade

### **Parameter Description**

*Browse:* Click the "Browse" button to select the firmware file to upload.

*Upload:* Click the "Upload" button to upload the firmware into the switch.



WARNING: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time or the switch may fail to function afterwards.

## 1.4.2-2 Firmware Selection

This section is used to switch between the latest uploaded firmware image and the previously uploaded firmware image. This page displays both firmware file details including the version number.

### Web Interface

To select the required firmware to be used in the switch via the Web Interface:

- 1. Click Maintenance, Firmware and Firmware Selection.
- 2. Click on the Activate Alternate Image button to switch to the old firmware version.



Fig. 144 Firmware Selection

Image:	The flash index name of the firmware image. The name of primary (preferred) image is managed, the alternate image is named managed.bk.
Version:	The version of the firmware image.
Date:	The date of the firmware image.
Activate Alternate Imag	e: Click this button to switch to the Alternate firmware version.
Cancel:	Cancel the firmware selection process.



## NOTE:

- 1. In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.
- 2. If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.
- 3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

## 1.4.3 Save/Restore

This section is used to backup, restore, and save the configuration in the switch.

## 1.4.3-1 Factory Defaults

This section is used to reset the switch back to its factory default settings.

## Web Interface

To Factory Default the switch via the Web Interface:

- 1. Click Maintenance, Save/Restore and Factory Defaults.
- 2. Select to set the IP Address back to Factory Default, or leave it as previously configured.
- 3. Press Yes to set the switch to Factory Default Settings, press No to cancel the request.

AMS-24165FP ×		2100 B
AMS-24T6SFP		Auto-Logout OFF 💌 Logout Help
System     Configuration     Security	Factory Defaults	
Maintenance     Restart Device     Firmware     Save/Restore	Are you sure you want to reset the configuration to Factory Defaults?	
Factory Defaults Save Start Save User Restore User Export/Import	Restore Default Configuration without changing current IP address Yes No	
Diagnostics		
	A	

Fig. 145 Factory Defaults

### Parameter Description

*Restore Default Configuration without changing current IP Address:* Check this box if you do not want to reset the IP Address to factory default.

*Yes:* Press Yes button to factory default the switch.

*No:* Press No to cancel the request.

## 1.4.3-2 Save Start

This section describes how to save the Switch Start configuration. Any current configuration files will be saved as XML format. This must be performed after configuration of the switch. If the Start configuration is not saved after the switch has been powered off it will revert back to previous settings.

## Web Interface

To Save the Startup Configuration in the switch via the Web Interface:

- 1. Click Maintenance, Save/Restore and Save Start.
- 2. Press Save.



Fig. 146 Save Start Up Configuration

### **Parameter Description**

Save:

Save Start Up Configuration.

#### NOTE:

This must be performed after configuration of the switch. If the Start configuration is not saved after the switch has been powered off it will revert back to previous settings.

## 1.4.3-3 Save User

This section describes how to save the Switch User configuration. Any current configuration files will be saved as XML format.

## Web Interface

To Save the User Configuration in the switch via the Web Interface:

- 1. Click Maintenance, Save/Restore and Save User.
- 2. Press Save.

AMS-24T6SEP ×	CONTRACTOR OF THE OWNER.	joke <mark>2</mark>
- C n 🗋 192.168.1.1		습 :
ALLOY		
AMS-24T6SFP	and the second se	Auto-Logout OFF 💌 Logout Help
System     Configuration	Save as Backup Configuration	
Security     Maintenance     Restart Device     Firmware     Save/Restore	Are you sure to save the current setting as Backup Configuration?	
Factory Defaults Save Start Save User Restore User	Save	
Export/Import     Diagnostics		

Fig. 147 Save User Configuration

### Parameter Description

Save:

Save Start Up Configuration.

## 1.4.3-4 Restore User

This section describes how to restore user's information back to the switch. Any current configuration files will be restored via XML format. *Web Interface* 

To Restore the User Configuration in the switch via the Web Interface:

- 1. Click Maintenance, Save/Restore and Restore User.
- 2. Press Save.

	ALLOY El Portbassed		trever interver
AMS-24T6SFP			Auto-Logout OFF 💽 Logout Hel
System Configuration	Restore	Backup Configuration	
Security Maintenance Restart Device		Are you sure to restore the Backup Configuration?	
<ul> <li>Firmware</li> <li>Save/Restore</li> </ul>	-		
Factory Defaults Save Start	Save		
Save User			
Restore User Export/Import			
► Diagnostics			

Fig. 148 Restore User Configuration

### **Parameter Description**

Save: Save Start Up Configuration.

## 1.4.4 Export/Import

This section describes how to export and import the Switch configuration. Any current configuration files will be exported as XML format.

## **1.4.4-1 Export Configuration**

This section is used to Save / Export the currently running configuration file of the switch.

## Web Interface

To Save the configuration file of the switch via the Web Interface:

- 1. Click Maintenance, Export/Import and Export Configuration.
- 2. Click Save to save the configuration file in XML format.

AM5-24165FP ×	and the second se	. Ø ×
← → C fi 🗋 192.168.1.1		û ≡
AMS-24T68FP		Auto-Logout OFF . Logout Help
System     Gonfiguration     Security     Maintenance     Reslart Device     Firmware     Save/Restore     Export/import     Export/import     Export/config     Import Config     Import Config     Diagnostics	Configuration Save	

Fig. 149 Export Configuration File

#### Parameter Description

Save:

Press the save button to save the configuration file to your computer.

## **1.4.4-2 Import Configuration**

This section is used to Import a saved configuration file into the switch.

## Web Interface

To Import a configuration file into the switch via the Web Interface:

- 1. Click Maintenance, Export/Import and Import Configuration.
- 2. Click Choose File to browse for the previously saved configuration file.
- 3. Click upload to load the file into the switch.

C # 192.168.1.1		жалият
AMS-24T6SFP		Auto-Logout OFF 💽 Logout Help
System Configuration	Configuration Upload	
Security Maintenance Restart Device	Choose File No file chosen Upload	
<ul> <li>Firmware</li> <li>Save/Restore</li> </ul>		
<ul> <li>Export/Import</li> <li>Export Config</li> <li>Import Config</li> </ul>		
<ul> <li>Diagnostics</li> </ul>		

Fig. 150 Import Configuration File

Choose File:	Press the "Choose File" Button to browse for the saved configuration file.
Upload:	Press upload to apply the configuration file to the switch.

## 1.4.5 Diagnostics

This section provides a set of basic system diagnosis. It lets users know whether the system is healthy or needs to be fixed. Users can also check network connectivity issues with the Ping command. The basic system check includes ICMP Ping, ICMPv6, and VeriPHY Cable Diagnostics.

## 1.4.5-1 Ping

This section is used to test network connectivity issues using the Ping command.

## Web Interface

To test network connectivity using the switch via the Web Interface:

- 1. Click Maintenance, Diagnostics and Ping.
- 2. Enter the IP Address of the device you are trying to communicate with.
- 3. Set the ping Data Length, Ping Count and Ping Interval.
- 4. Click the Start button to commence the test.

🗢 C ni 🗋 192.168.1.1			ŵ
ALLOY AMS-24T6SFP	Phile Phile Wood Sevent States		Auto-Logout OFF - Logout Help
			Auto-Logout OFF 💽 Logout Help
System Configuration	ICMP Ping		
Security Maintenance	IP Address	0000	
Restart Device	Ping Length	56	
Firmware	Ping Count	5	
Save/Restore Export/Import	Ping Interval	1	
<ul> <li>Diagnostics</li> <li>Ping</li> <li>Ping6</li> </ul>	Start		
VenPHY			
Veneny			
Veniery			
Venieny			
Veninity			
Venery			
Veniny			
Venery			

Fig. 151 Ping Command

IP Address:	The destination IP Address you want to ping it.
Ping Length:	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
Ping Count:	The count of the ICMP packet. Values range from 1 time to 60 times.
Ping Interval:	The interval of the ICMP packet. Values range from 0 second to 30 seconds.

## 1.4.5-2 Ping6

This section is used to test network connectivity issues using the Ping IPv6 command.

## Web Interface

To test IPv6 network connectivity using the switch via the Web Interface:

- 1. Click Maintenance, Diagnostics and Ping.
- 2. Enter the IP Address of the device you are trying to communicate with.
- 3. Set the ping Data Length, Ping Count and Ping Interval.
- 4. Click the Start button to commence the test.

C n 🗋 192.168.1.1				â
ALLOY	ALLON a real formation disput formation			
MS-24T6SFP			Auto-Logout OFF 💌 Logout	Hel
System Configuration	ICMPv6 Pin	g		
Security	IP Address	0.0.0.0.0.0		
Maintenance Restart Device	Ping Length	56		
Firmware	Ping Count	5		
<ul> <li>Save/Restore</li> <li>Export/Import</li> </ul>	Ping Interval	1		
Diagnostics	and the second second	<u>.</u>		
Ping	Start			
Ping6				
VenPHY				

Fig. 152 Ping IPv6 Command

IP Address:	The destination IP Address you want to ping it.
Ping Length:	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
Ping Count:	The count of the ICMP packet. Values range from 1 time to 60 times.
Ping Interval:	The interval of the ICMP packet. Values range from 0 second to 30 seconds.

## 1.4.5-3 VeriPHY

This section is used for running the VeriPHY Cable Diagnostics. Press to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 -140 meters.10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

## Web Interface

To perform a VeriPHY Cable Diagnostic test via the Web Interface:

- 1. Specify the port in which you wish to perform a test.
- 2. Click Start to perform the test.

C 🐔 🗋 192.168.1.1											
LION		_									
ILLOY	ALLON II Part Manual		_ =			1011	I.	ALC: NO	armore .		
	Prover Second		- 📰 🗷			ių er		ψψ I			
24T6SFP	-									D-Logout OFF	- Logout
m	1 I										
iguration	Verif	PHY Ca	ble Diag	nostics	5						
rity	Port	Al 🔻									
tenance art Device	1 011	1 44 121									
mware	Start										
ve/Restore											
port/Import	Cable Status										
ignostics ng	Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D		
ng6	1										
MPHY	2		-	-			*		-		
	4		-	-	-	-			-		
	5		-		-	-	-		-		
	6	-	+	-	-	-	-	1 1	-		
	7		-						-		
	8	**	+	-	-	-			-		
	9							-	-		
	10			*			-	-	-		
	11			-				-	-		
	12		-	-	-	+	-	-	-		
	13	-	+	-	-						
	-14		-		-	-			-		
	15		-	-				1.000	-		
	16	-	-		-	-			-		
	17	-	+	-	-	-	-	-	-		
	18	-	-		-	-	-		-		
	19			*					-		
	20										

Fig. 153 VeriPHY Cable Diagnostic Test

### **Parameter Description**

*Port:* The physical port of the switch.

Cable Status:Port: Port number.Pair: The status of the cable pair.Length: The length (in meters) of the cable pair.

# 2. Specifications

AMS Series Model	10T2SFP	24T6SFP	48T4SFP	24T4S4SFP	48T4S4SFP	4T24S4SFP			
Interface		<u> </u>	<u> </u>		<u> </u>				
Total Ports, comprising	10x GbE         26x GbE         48x GbE         28x GbE         52x GbE         28x								
UTP (10/100/1000Mbps)	8	20	44	20	44	4			
UTP/(100M/1G) SFP	2	4	4	4	4	4			
SFP (100M/1G)	-	2	-	-	-	20			
SFP+ (1G/10G)	-	-	-	4	4	4			
General									
Jumbo Frames			9Kb on (	Gigabit Interfa	ces				
MAC Table	8K	32K	32К	32К	32К				
Performance									
Switching Capacity	14.88 mpps	38.69 mpps	71.42 mpps	95.23 mpps	130.94 mpps	95.23 mpps			
Forwarding Rate	20Gbps	52Gbps	96Gbps	128Gbps	136Gbps	128Gbps			
Layer 2+ Switching	<u> </u>	<u> </u>	<u> </u>						
Spanning Tree		Spanning T	ree Protoc	ols supported:	STP, RSTP, MS	ГР			
LACP Trunking	5 groups, 10 ports per group	12 groups, 8 ports per group	24 groups, 12 ports per group	14 groups, 8 ports per group	24 groups, 12 ports per group	14 groups, 12 ports per group			
VLAN	4K VLAN's: Port based VLAN's; 802.1Q; MAC Based VLAN's; Management VLAN; Private VLAN								
Voice VLAN	Voice			assigned to a v opropriate leve	•	/LAN and			
GVRP			S	Supported					
DHCP Relay	F	Relay of DH	CP traffic to	DHCP server	in different VL	AN.			

	Works with DHCP Option 82
IGMP Snooping	V1, V2 and v3 . Supports 1024 Multicast Groups
IGMP Querier	Supported
IGMP Proxy	Supported
MLD Snooping	v1 and v2
Security	
SSH	v1 and v2 are supported
SSL	Supported
IEEE 802.1x	IEEE802.1x: RADIUS authentication, authorisation and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions. Supports IGMP-RADIUS based 802.1x Dynamic VLAN assignment
Layer 2 isolation	PVE (Private VLAN Edge, aka protected ports) for L2 isolation between clients in the same VLAN. Supports multiple uplinks.
Port Security	Locks MAC Addresses to ports, and limits the number of learned MAC addresses
IP Source Guard	Supports illegal IP address from accessing to specific port in the switch.
RADIUS/ TACACS+	Supports RADIUS and TACACS+ authentication. Switch as a client.
Storm control	Broadcast, multicast, or unicast storm on a port.
ACLs	Supports up to 256 entries
	Drop or rate limitation based on source and destination MAC, VLAN ID or IP address, protocol, port, differentiated services code point (DSCP) / IP precedence, TCP/ UDP source and destination ports, 802.1p priority, Ethernet type, Internet Control Message Protocol (ICMP) packets, IGMP packets, TCP flag.
Port Security	Locks MAC Addresses to ports, and limits the number of learned MAC addresses
Quality of Service	
H/W Priority Queue	Supports 8 hardware priority queues
Scheduling	Strict priority and weighted round-robin (WRR). Queue assignment

	based on DSCP and class of service (802.1p/ CoS)
Classification	Port based; 802.1p VLAN priority based; IPv4/IPv6 precedence/ type of service (ToS) / DSCP based; Differentiated Services (DiffServ); classification and re-marking ACLs, trusted QoS
Rate Limiting	Ingress policer; egress shaping and rate control; per VLAN, per port and flow based
IPv6 applications	Web/SSL, Telnet/SSH, Ping, Simple Network Time Protocol (SNTP), Trivial File Transfer Protocol (TFTP), SNMP, RADIUS, Syslog
Management	
Web GUI interface	HTTP/ HTTPS
Dual Image	Dual image provides independent primary and secondary OS files for backup while upgrading.
SNMP	SNMP v1, 2c and 3
RMON	RMON (Remote Monitoring) groups 1,2,3,9
IPv4 and IPv6	Dual protocol stack supported
Firmware Upgrade	Web browser upgrade (HTTP/ HTTPS) and TFTP Upgrade through console port also supported.
Port mirroring	Up to 8 source ports can be mirrored to single destination port
s-Flow	Monitoring for high speed switched networks supported
UPnP	Universal Plug and Play supported
Green Ethernet	
Link detection	Compliant with IEEE802.3az Energy Efficient Ethernet. Automatically turns off power on Gigabit Ethernet RJ-45 port when detecting link down or client idle. Active mode is resumed without loss of any packets when the switch detects link up.
Cable length detection	Adjusts the signal strength based on the cable length. Reduces the power consumption for shorter cables.
Discovery	
LLDP	IEEE802.1AB - Link Layer Detection Protocol with LLDP-MED extensions
Carrier Ethernet Protocols	and Features (AMS-4T24S4SFP Only)

IEEE 802.3ah Ethernet OAM	Simple li	Simple link fault management (LFM) for Ethernet as defined in IEEE 802.3ah (MAC Layer OAM)								
IEEE 802.1ag Ethernet CFM	IEEE 802	IEEE 802.1ag Ethernet CFM function that provides connectivity fault management								
Syn-E and IEEE1588v2		Both IEEE 1588v2 and ITU-T Sync-E Ethernet synchronization protocols, and can emulate link OAM and service OAM protocols (by request).								
ITU-T Y.1731	Both IEEE 1588v2 and ITU-T Sync-E Ethernet synchronization protocols, and can emulate link OAM and service OAM protocols.									
ITU-T G.8032		ITU-T service OAM standard Y.1731 divides a network into maintenance domains in the form of hierarchy levels (to be released in v1.20 firmware)								
MEF E-tree			er MPLS (including E-LINE, E-LAN and E E). Available on release of v1.20 firmw	=						
Environmental Specificati	ons									
Dimensions (WxHxD, mm)	280 x 44 x 166	442 x 44 x 300	442 x 44 x 385	442 x 44 x 300						
Case	Desktop	1RU ra	ckmount (mounting kit included), all m	etal case						
Weight	1.382Kg	3.84Kg	5Kg	3.84Kg						
Temperature		0° to 4	0° operating; -20° to 70° storage							
Humidity	10% to 90% , relative, non-condensing									
Power Supply	100-240VAC 50-60Hz, internal , universal 100-240VAC 50-60Hz, internal , universal 240V 50-60 intern univer ; -48V dua pow input									
Certification		CE Mark	, FCC Part 15 (CFR47) Class A, C-Tick							