

ALL8944WMP



Full L2 Management PoE Switch

24x 10/100/1000 Gigabit + 2 Gigabit SFP Port

User Manual

FCC Warning

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. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. 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.

CE Mark Warning

This is a Class-A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

FCC Warning2	
Table of Contents	
Products Overview	
Content9	
Hardware Description	
User Log In10)
Configuration11	
System11	
Information11	
IP12	•
IPv613	}
NTP15	;
Log16	;
Power Reduction	}
LED18	}
EEE2	1
Ports2	3
Security	5
Switch25	;
Users	;
Privilege Levels	3
Auth Method27	7
SSH29	9
HTTPS)
Access Management	2
SNMP	1
System	
Communities	,
Users	}
Groups40)
Views4	1
Access4	2
RMON4	4
Statistics4	4
History4	5
Alarm4	6
Event4	В
Network4	9

Limit Control	49
NAS	53
ACL	62
Ports	62
Rate Limiters	64
Access Control List	65
DHCP	77
Snooping	77
Relay	78
IP Source Guard	82
Configuration	82
Static Table	83
ARP Inspection	84
Configuration	84
Static Table	86
Aggregation	90
Static	90
LACP	91
Spanning Tree	92
Bridge Settings	92
MSTI Mapping	95
MSTI Priorities	96
CIST Ports	
MSTI Ports	
MVR	101
PMC	102
IGMP Snooping	
VLAN Configuration	104
Port Group Filtering	
MLD Snooping	107
VLAN Configuration	108
Port Group Filtering	110
LLDP	111
LLDP	
LLDP-MED Configuration	114
PoE	
Ports	
MAC Table	

VLANs	127
VLAN Membership	127
Ports	129
Private VLANs	131
PVLAN Membership	131
Port Isolation	133
VCL	134
MAC-based VLAN	134
Protocol-based VLAN	135
Protocol to Group	135
Group to VLAN	138
Voice VLAN	139
Configuration	139
OUI	142
QoS	143
Port Classification	143
Port Policing	145
Port Scheduler	146
Port Shaping	147
Port Tag Remarking	148
Port DSCP	149
DSCP-Based QoS	152
DSCP Translation	154
DSCP Classification	156
QoS Control List	157
Storm Control	160
Mirroring	161
UPnP	162
sFlow	165

Monitor

System	
Information	
CPU Load	170
Log	171
Detailed Log	
Ports	173
State	

Traffic Overview	174
QoS Statistics	175
QCL Status	176
Detailed Statistics	178
Security	181
Access Management Statistics	181
Network	
Port Security	
Switch	
Port	
NAS	186
Port	
ACL Status	195
DHCP	
Snooping Statistics	197
Relay Statistics	199
ARP Inspection	
IP Source Guard	
AAA	205
RADIUS Overview	
Switch	214
RMON	214
Statistics	214
History	216
Alarm	218
Event	219
LACP	220
System Status	220
Port Status	221
Port Statistics	223
Spanning Tree	224
Bridge Status	224
Port Status	225
Port Statistics	226
MVR	
Statistics	227
MVR Channel Groups	228
IPMC	

IGMP Snooping229
Status
Groups Information231
IPv4 SFM Information232
MLD Snooping
Status234
Groups Information
IPv6 SFM Information236
LLDP
Neighbours238
LLDP-MED Neighbours
EEE
Port Statistics
PoE
MAC Table
VLANs
VLAN Membership
VLAN Port255
VCL
MAC-based VLAN

Diagnostics

Ping	
Ping6	
VeriPHY	

Maintenance

Restart Device	
Factory Defaults	
Software	
Upload	
Image Select	
Configuration	

Products Overview

This switch provides 24 10/100/1000Mbps RJ-45 ports and can support 2 Gigabit SFP to uplink. This Full Layer 2 management switch includes auto-MDI/MDIX crossover detection function. 24 of those ports are all built with PoE functionality, providing the ultimate choice in network flexibility. With this added PoE feature, this switch is an ideal solution for building wireless, IP surveillance, and VoIP networks.

It also provides port-based and 802.1Q tag VLAN function to provide better traffic management, reduces latency, improve security and save bandwidth. This is also a cost-saving feature as it reduces the need to add additional hardware to the network.

Specifications

IEEE 802.3 10BaseT IEEE 802.3u 100BaseTX IEEE 802.ab 1000BaseT IEEE 802.3z 1000BaseSX/LX IEEE 802.3x Full-duplex and Flow Control IEEE 802.3ad Link Aggregation IEEE 802.1d Spanning tree protocol IEEE 802.1w Rapid Spanning tree protocol

IEEE 802.1Q VLAN IEEE 802.1p Class of Service IGMP Snooping v1 /v2c/v3 Jumbo Frame Support 9 K MVR

Mechanical

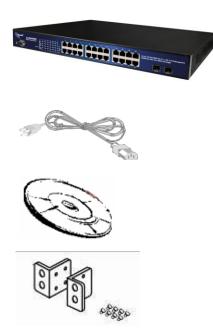
Performance

- MAC Address : 8K
- Buffer Memory :48MB
- Switching Capacity : 52Gbps
- Forwarding Rate : 38.7Mpps

Package Contents

Before you start to install this switch, please verify your package that contains the following items:

- One Network Switch
- One Power Cord
- One User Manual CD
- One pair Rack-mount kit + 8 Screws



Hardware Description

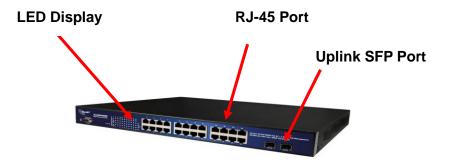
This section mainly describes the hardware of Full L2 Management PoE Switch and gives a physical and functional overview on the certain switch.

Physical Dimensions / Weight

45 x 440 x 220 mm (H x W xD) / 3.0kg

Front Panel

The front panel of the L2 management switch consists of 24 10/100/1000 Base-TX RJ-45 ports and 2 gigabit uplink SFP ports. The LED Indicators are also located on the front panel.



LED Indicators

The LED Indicators present real-time information of systematic operation status. The following table provides description of LED status and their meaning.

LED	Status	Description	No. of LEDs
Power	On	Power on	Power
10/100M	On	Link 10/100Mbps	24(1~24)
	Flashing	Data Activating	24(1~24)
Link/ ACT/1000M	On	Link	24(1~24)
	Flashing	Data Activating	24(1~24)
	On	linked to Power Device	25~26
SFP	Flashing	Data Activating	25~26
	Off	No Device is Connected	25~26

Rear Panel

The 3-pronged power plug is placed at the rear panel of the switch right side shown as below.



Hardware Installation

Set the switch on a large flat space with a power socket close by. The flat space should be clean, smooth, level and sturdy. Make sure there is enough clearance around the switch to allow attachment of cables, power cord and allow air circulation. The last, use twisted pair cable to connect this switch to your PC then user could start to operate the switch.

User Login Default IP-Address: 192.168.2.1 Username: admin Password: admin

System Information Configuration:

RUNT'		ALL8944WMP - Gigabit PoE Switch	6 3
Configuration System Information Information Information Information Information Information Information Information Ports Socurity Aggregation Loop Protection Spanning Tree MVR IPMC LLDP PoE MAC Table VLANs Private VLANs VCL Voice VLAN OoS Mirroring UPnP SFlow Monitor	System Information Configurati System Contact System Name System Location System Timezone Offset (minutes) Save Reset	on 	

System Contact

The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

System Name

An administratively assigned name for this managed node. By convention, this is the node's 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 this node(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.

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.

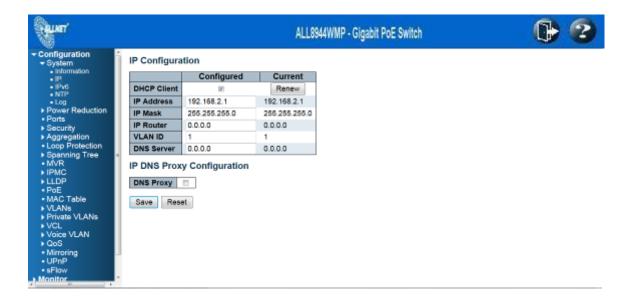
Buttons

Save: Click to save changes

Reset: Click to undo any changes made locally and revert to previously saved values

IP Configuration:

Configure the switch-managed IP information on this page.



The Configured column is used to view or change the IP configuration.

The Current column is used to show the active IP configuration.

DHCP Client

Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

IP Address

Provide the IP address of this switch in dotted decimal notation.

IP Mask

Provide the IP mask of this switch dotted decimal notation.

IP Router

Provide the IP address of the router in dotted decimal notation.

SNTP

Provide the IP address of the SNTP Server in dotted decimal notation.

DNS Server

Provide the IP address of the DNS Server in dotted decimal notation.

VLAN ID

Provide the managed VLAND ID. The allowed range is 1 to 4095.

DNS Proxy

When DNS proxy is enabled, DUT will relay DNS requests to the current configured DNS server on DUT, and reply as a DNS resolver to the client device on the network.

Buttons

Save: Click to save changes

Reset: Click to undo any changes made locally and revert to previously saved values

Renew: Click to renew DHCP. This button is only available if DHCP is enabled.

IPv6 Configuration:

Configure the switch-managed IPv6 information on this page:

The **Configured** column is used to view or change the IPv6 configuration.

The Current column is used to show the active IPv6 configuration.

Auto Configuration

Enable IPv6 auto-configuration by checking this box. If fails, the configured IPv6 address is zero. The router may delay responding to a router solicitation for a few seconds, the total time needed to complete auto-configuration can be significantly longer.

Address

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

Prefix

Provide the IPv6 Prefix of this switch. The allowed range is 1 to 128.

Router

Provide the IPv6 gateway address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example,

'fe80::215:c5ff:fe03:4dc7'.

The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. . For example, '::192.1.2.34'.

Provide the IPv6 SNTP Server address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. . For example, '::192.1.2.34'.

Buttons

Save: Click to save changes

Reset: Click to undo any changes made locally and revert to previously saved values Renew: Click to renew IPv6 AUTOCONF. This button is only available if IPv6 AUTOCONF is enabled.

NTP Configuration:

Indicates the NTP mode operation:

RELINET'		ALL8944WMP - Gigabit PoE Switch	1 2
Configuration System Information Information Information Information Information Information Information Ports Security Aggregation Loop Protection Spanning Tree MVR ILDP PoE MAC Table VLANs VCL VLANs VCL VLANs VCL Voice VLAN CoS Mirroring UPnP sFlow Monitor V	NTP Configuration Mode Disabled Server 1		

Mode

The Possible modes are:

Enable NTP mode operation. When NTP mode operation is enabled, the agent forwards NTP messages

between the clients and the server when they are not on the same subnet domain.

Disable NTP mode operation.

Gener'	ALL8944WMP - Gigabit PoE Switch	1 2
Configuration System Information Prote Security Aggregation Loop Protection Spanning Tree MVR IPMC LLDP PoE MAC Table VLANs VCL VLANs VCL VLAN OoS Mirroring UPPP sFlow Monitor Aggregation Loop Protection Spanning Tree MAC Table VLANs VCL VLAN OoS Mirroring UPPP sFlow		

Server

Provide the NTP IPv4 or IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example,

'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Buttons

Save: Click to save changes

Reset: Click to undo any changes made locally and revert to previously saved values

System Log Configuration:

Relation of the second		ALL8944WMP - Gigabit PoE Switch	2
Configuration System Information IP IP IP IP Log Power Reduction Ports Security Aggregation Loop Protection Spanning Tree MVR IPMC LLDP PoE MAC Table VLANs VCL VLANs VCL VLANs VCL VLANs VCL VLANs VCL VLANs VCL Voice VLAN CoS Mirroring UPnP sFlow Monitor V	System Log Configuration		

Server Mode

Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are:

Enable server mode operation.

Disable server mode operation.

-RUNET'		ALL8944WMP - Gigabit PoE Switch	2
Configuration System Information IP IP46 NTP Log Power Reduction Ports Security Aggregation Loop Protection Spanning Tree MVR IPMC LLDP PoE MAC Table VLANs VCL VLANs VCL Voice VLAN QoS Mirroring UPnP sFlow Monitor	System Log Configuration		

Server Address

Indicates the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a host name.

Syslog Level

Indicates what kind of message will send to syslog server. Possible modes are:

Info: Send information, warnings and errors.

Warning: Send warnings and errors.

Error: Send errors.

Remun'		ALL8944WMP - Gigabit PoE Switch	1
Information IP IP IP IP Se NTP Log Power Reduction	stem Log Configuration		

Buttons

Save: Click to save changes

Reset: Click to undo any changes made locally and revert to previously saved value.

LED Power Reduction Configuration

Status LED

The system status LED shows whether the system is running. The LED is green when system is running and no errors are detected. If errors has been detected the status LED will indicate this by blinking red.

Front Ethernet Port LEDs

The front Ethernet ports have a dual color LEDs per port. The port LEDs is placed in a block (1-high for SFPs, 2-high for RJ45s) to the left of the ports.

A pushbutton and a 4-high tower of LEDs is placed next to the front ethernet port LEDs. The pushbutton selects between four different port LED modes, indicated by the 4-high LED mode tower. After 30 seconds the LED mode falls back to mode A.

The port LED modes are named A through D and shows the following:

Port LED Indication mode A:

Green (1000Mbit): Solid=Link, Blink=Activity Orange (10/100Mbit): Solid=Link, Blink=Activity

Port LED Indication mode B:

Green : Solid=Half Duplex, Blink: Collisions Orange: Solid=Half Duplex, Blink: Collisions

Port LED Indication mode C:

Green: Solid=Link, Blink=Activity Orange: Solid= Port disabled by management, Blink= Errors received

LEDs Intensity

The LEDs power consumption can be reduced by lowering the LEDs intensity. LEDs intensity could for example be lowered during night time, or they could be turn completely off. It is possible to configure 24 different hours of the day, at where the LEDs intensity should be set.

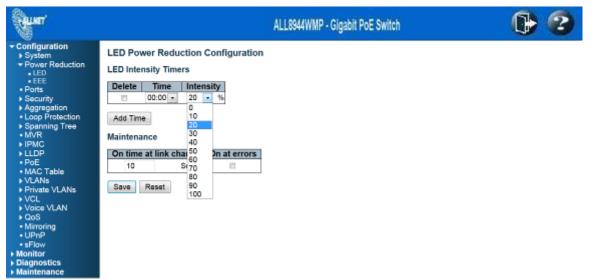
Time

The time at which the LEDs intensity shall be set.



Intensity

The LEDs intensity (100% = Full power, 0% = LED off):



Maintenance Time

When a network administrator does maintenance of the switch (e.g. adding or moving users) he might want to have full LED intensity during the maintenance period. Therefore it is possible to specify that the LEDs shall use full intensity a specific period of time. **Maintenance Time** is the number of seconds that the LEDs will have full intensity after either a port has changed link state, or the LED pushbutton has been pushed.

ALINT'		ALL8944WMP - Gigabit PoE Switch	2
Configuration System System Power Reduction LED EEE Ports Security Aggregation Loop Protection Spanning Tree MVR IPMC LDP PoE MAC Table VLANs VCL Voice VLAN Voic Voice VLAN QoS Mirroring UPPP SFlow Monitor Diagnostics Maintenance	LED Power Reduction Configuration LED Intensity Timers Delete Time Intensity 00:00 × 20 × % Add Time Maintenance On time at link change On at errors 10 Sec. Save Reset		

Buttons

Save: Click to save changes

Reset: Click to undo any changes made locally and revert to previously saved values

EEE Configuration:

	Configurat	tion									
						nt C				1	
	Enabled	1	2	3	4	5	6	7	8		
1				2		10	10		10		
1							10		10		
2						13	13		13		
3		13		8		8	10	8	10		
4				10		10	10		13		
5		13	5	23	8	23	13	-	13		
6				10		10	10		10		
7	10	11	23	23	-	13	13	23	13		
8		11		21		2	21	11	21		
9		10		-	8	1		23	10		
10			10		10			10	_		
11			10	10	8	10		10	10		
12						0			_		
13			8	10	8	8			10		
13			2					8			
15				1	8			8	10		
						2					
17	1000		2			2		-			
18											
19			2	2		2		8			
20						2					
21			5		8	5		8			
22			2			10	B		B		
23	6						5	2	5		
24					8	13	13	2	13		
25											
26											

This page allows the user to inspect and configure the current EEE port settings:

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 gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange information about the devices wakeup time using the LLDP protocol.

For maximizing the power saving, the circuit isn't started at once transmit data are ready for a port, but is instead queued until 3000 bytes of data are ready to be transmitted. For not introducing a large delay in case that data less then 3000 bytes shall be transmitted, data are always transmitted after 48 us, giving a maximum latency of 48 us + 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.

Port

The switch port number of the logical EEE port.

EEE Enabled

Controls whether EEE is enabled for this switch port.

EEE Urgent Queues

Queues set will activate transmision of frames as soon as any data is available. Otherwise the queue will postpone the transmision until 3000 bytes are ready to be transmitted.

Thermal Protection Configuration

This page allows the user to inspect and configure the current setting for controlling thermal protection. Thermal protection is used to protect the chip from getting overheated.

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

Temperature settings for priority groups

The temperature at which the ports with the corresponding priority will be turned off. Temperatures between 0 and 255 C are supported.

Port priorities

The priority the port belongs to. 4 priorities are supported.

Port Configuration:

This page displays current port configurations. Ports can also be configured here.

HUNET'						ALL8944W	MP - Gigat	bit PoE Switch				2
Configuration System Power Reduction	Port 0	Config	uration								Refresh	
Power Reduction Ports				Speed			Flow Con	trol	Maximum	Excessive	Power	
Security Aggregation	Port	Link	Current	Config	ured	Current Rx	Current Tx	Configured	Frame Size	Collision Mode	Contro	
Loop Protection				0					9600	• •	0	
Spanning Tree	1	٠	Down	Auto		×	×		9600	Discard ·	Disabled	
MVR IPMC	2		Down	Auto		x	x		9600	Discard -	Disabled	
LLDP	3		Down	Auto	×	x	x	10	9600	Discard -	Disabled	×
PoE	4		Down	Auto	•	x	x		9600	Discard -	Disabled	
MAC Table VLANs	5		Down	Auto	-	x	x		9600	Discard -	Disabled	-
Private VLANs	6		Down	Auto	-	x	×	8	9600	Discard -	Disabled	-
VCL	7		Down	Auto		x	x		9600	Discard -	Disabled	
 Voice VLAN QoS 	8	ě	Down	Auto	-	x	×		9600	Discard -	Disabled	-
 Mirroring 	9		Down	Auto		x	x		9600	Discard -	Disabled	
UPnP	10		Down	Auto	•	x	x		9600	Discard -	Disabled	-
sFlow Monitor	11		Down	Auto		x	x		9600	Discard ·	Disabled	
Diagnostics	12	×.	Down	Auto		x	x		9600	Discard +	Disabled	
Maintenance	13		Down	Auto		x	×		9600	Discard Restart	Disabled	
	14		100fdx	Auto		x	x		9600	Discard -	Disabled	
		-							0000	Discost	Principal and	

Port

This is the logical port number for this row.

Link

The current link state is displayed graphically. Green indicates the link is up and red that it is down.

Current Link Speed

Provides the current link speed of the port.

Configured Link Speed

Select any available link speed for the given switch port.

Auto Speed: selects the highest speed that is compatible with a link partner.

Disabled: disables the switch port operation.

Fiber Speed

Configure speed for fiber port.

Note: Port speed for the Copper ports will automatically be set to Auto when dual media is selected.

Disable SFPs (Copper port only).

SFP-Auto automatically determines the speed at the SFP.

Note: There is no standardized way to do SFP auto detect, so here it is done by reading the SFP rom. Due to

the missing standardized way of doing SFP auto detect some SFPs might not be detectable.

1000-X force SFP speed to 1000-X.

100-FX force SFP speed to 100-FX.

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 the switch port, including FCS.

Excessive Collision Mode

Configure port transmit collision behavior.

Discard: Discard frame after 16 collisions (default).

Restart: Restart backoff algorithm after 16 collisions.

Power Control

The Usage column shows the current percentage of the power consumption per port. The Configured column

allows for changing the power savings mode parameters per port.

Disabled: All power savings mechanisms disabled.

ActiPHY: Link down power savings enabled.

PerfectReach: Link up power savings enabled.

Enabled: Both link up and link down power savings enabled.

Buttons

Save: Click to save changes

Reset: Click to undo any changes made locally and revert to previously saved values

Refresh: Click to refresh the page. Any changes made locally will be undone.

Security / Switch / Users Configuration:

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.

This page configures a user:

RELINET'		ALL8944WMP - Gigabit PoE Switch	1 🔁 🕄
 Configuration System Power Reduction Ports Security Settch Users Nutwidge Lovets Auth Method SSH HTTPS Access Management SNMP RMON Network AAA Aggregation Loop Protection Spanning Tree MWR IPMC LLDP PoE MAC Table VLANs VCINS 	Users Configuration User Name Privilege Level admin 15 Add New User		

User Name

The name identify the user. This is also a link to Add User & Edit User

User Name

A string identifying the user name that this entry should belong to. The allowed string length is **1** to **32**. The valid user name is a combination of letters, numbers and underscores.

Password

The password of the user. The allowed string length is 0 to 32.

Privilege Level

The privilege level of the user. The allowed range is **1** to **15**. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

Add new user: Click to add a new user.

Privilege Levels Configuration:

This page provides an overview of the privilege levels.

·			Gigabit PoE Switch	
Privilege Level	Configuration			
		Privilege		
Group Name	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5 💌	10 🔽	5 🔽	10 🔽
S Debug	15 -	15 -	15 -	15 -
Diagnostics	5 -	10 -	5 -	10 -
EEE	5 -	10 -	5 -	10 -
IP	5 -	10 -	5 -	10 -
IPMC_LIB	5 -	10 -	5 -	10 -
IPMC Snooping	5 -	10 -	5 -	10 -
LACP	5 -	10 -	5 -	10 -
LLDP	5 -	10 -	5 -	10 -
LLDP_MED	5 -	10 -	5 -	10 -
Loop Protect	5 -	10 -	5 -	10 -
MAC Table	5 -	10 -	5 -	10 -
MVR	5 -	10 -	5 -	10 -
Maintenance	15 -	15 -	15 -	15 -
Mirroring	5 -	10 •	5 -	10 -
POE	5 -	10 -	5 -	10 -
Port Security	5 -	10 •	5 -	10 -
Ports	5 -	10 -	1 -	10 -
Private VLANs	5 -	10 -	5 -	10 -
QoS	5 -	10 -	5 -	10 -
SFlow	5 -	10 -	5 -	10 -
SNMP	5 -	10 -	5 -	10 -
Security	5 -	10 -	5 -	10 -
Spanning_Tree	5 -	10 -	5 -	10 -
System	5 -	10 -	1 -	10 -
Timer	5 -	10 -	5 -	10 -
UPnP	5 -	10 -	5 -	10 -
VCL	5 -	10 -	5 -	10 -
VCL VLANs	5 -	10 -	5 -	10 -
VLANS Voice_VLAN	5 -	10 -	5 -	10 -

Group Name

The name identifying the privilege group. In most cases, a privilege level group consists of a single module

(e.g. LACP, RSTP or QoS), but a few of them contains more than one.

The following description defines these privilege level groups in details:

System: Contact, Name, Location, Timezone, Log.

Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection and IP source guard.

IP: Everything except 'ping'.

Port: Everything except 'VeriPHY'.

Diagnostics: 'ping' and 'VeriPHY'.

Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance. Debug: Only present in CLI.

Privilege Levels

Every group has an authorization Privilege level for the following sub groups: configuration read-only,

configuration/execute read-write, status/statistics read-only, status/statistics read-write (e.g. for clearing of statistics).

User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

Buttons

Save: Click to save changes

Reset: Click to undo any changes made locally and revert to previously saved values

Auth Method

This page allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces.

The table has one row for each client type and a number of columns, which are:

RUNET'			AL	L8944WMP - Gigabit PoE Switch	6 📀
 Configuration System 	Authent	ication Method Configu	iration		
 Power Reduction Ports 	Client	Authentication Method	Fallback		
 Ports Security 	console	local *			
 Switch 	teinet	local +			
Users Privilege Levels	ssh	local ·			
 Auth Method 	web	local ×			
SSH HTTPS Access Management SMMP RMON RMON Network AAA Aggregation Loop Protection Spanning Tree M/R IPMC LLDP PoE MAC Table VLANs Private VLANs VLANs	- Save	Reset			

Client

The management client for which the configuration below applies.

RELACT			ALL	8944WMP - Gigabit PoE Switch	•	2
Configuration System	Authent	ication Method Configu	ration			
 Power Reduction Ports 	Client	Authentication Method	Fallback			
 Ports Security 	console	local				
- Switch	teinet	none				
Users	ssh	local				
Privilege Levels Auth Method	web	RADIUS TACACS+				
 SSH 		IAUAUS+				
• HTTPS =	Save	Reset				
Access Management						
► SNMP						
RMON						
 Notwork AAA 						
► Aggregation						
 Loop Protection 						
 Spanning Tree 						
• MVR						
► IPMC						
LLDP PoE						
MAC Table						
► VLANs						
Private VLANs						
► VCL -						
C 11 F						

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.

Fallback

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'.

Buttons

Save: Click to save changes

Reset: Click to undo any changes made locally and revert to previously saved values

Security /Switch / SSH Configuration

Configure SSH on this page.

Guna,		ALL8944WMP - Gigabit PoE Switch	1
Configuration System Power Reduction Ports Security Swatch Users Phylioge Levels Auth Method SSH Access Management SMMP RMON Network AAA Aggregation Loop Protection Spanning Tree MMCR ILDP PoE MAC Table VLANs VCL	SSH Configuration Mode Enabled • Save Reset		

Quert'		ALL8944WMP - Gigabit PoE Switch	1
Configuration System Power Reduction Ports Security Security Setto Add Security Setto StH Horize Setto Seto Setto Seto Setto Se	SSH Configuration		

Mode

Indicates the SSH mode operation. Possible modes are:

Enable: Enable SSH mode operation.

Disabled: Disable SSH mode operation.

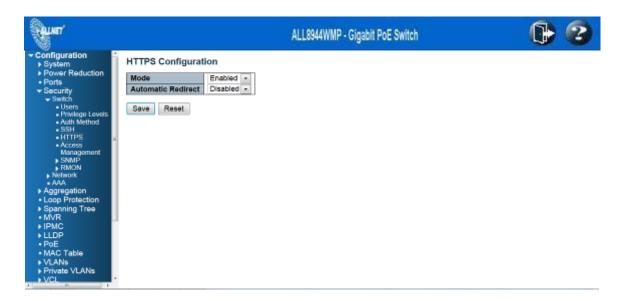
Buttons

Save: Click to save changes

Reset: Click to undo any changes made locally and revert to previously saved values

HTTPS Configuration

Configure HTTPS on this page:



Mode

Indicates the HTTPS mode operation. Possible modes are:

Enable: 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:

Enable: Enable HTTPS redirect mode operation.Disabled: Disable HTTPS redirect mode operation.

Buttons

Save: Click to save changes

Reset: Click to undo any changes made locally and revert to previously saved values

Access Management Configuration

Configure access management table on this page. The maximum entry number is **16.** If the application's type match any one of the access management entries, it will allow access to the switch.



Mode

Indicates the access management mode operation. Possible modes are:

Enable: 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.



Buttons

Add new entry: Click to add a new group entry

Save: Click to save changes

Reset: Click to undo any changes made locally and revert to previously saved values

SNMP –System

Configure SNMP on this page:

1	ALL8944WMP - Gigabit PoE Switch	
tem SNMP System	Configuration	
Mode Mode	Enabled +	
Version	SNMP v2c ·	
Read Communit	y public	
Users Privlege Levels Write Communit	y private	
	2	
Auth Method SSH HTTPS Access Management SNMP Trap Co Tran Mode	-	
SSH HTTPS Access Management SNMP SSNMP System Communities Trap Mode	nfiguration -	
SSH HTTPS Access Management SNMP SNMP SSNMP SSNMP Communities Ubers Ubers Strap Mode Trap Mode Trap Version	Disabled - SNMP v1 -	
SSM Intrps Access Management SSMMP System Communities Dess Groups Yews Trap Community	Disabled SNMP v1 public	
SSIM IntTPS Access Management SSNMP	Disabled • SNMP v1 • Address	
SSH I Engine to STACCess Management SNMP Trap Co System Communities Communiti	I IPV6 Address	
SSH SSH SSH SSNMP	nfiguration Disabled - SNMP v1 - v public Address :: tion Failure Enabled ×	
SSH Interport Access Management System - Communities SNMP Trap Co System - Communities Trap Mode Trap Version - Groups Trap Community - Access Trap Destination RMON - Communities Trap Destination RMON - Communities Trap Destination - Trap Authentica - Protection Trap Link-up an - Protection T	nfiguration Disabled SNMP v1 public Address IPv6 Address Control Internation Enabled Control Internation Control Internatio Control Internatio Control Internation Co	
SSH SSH SSH SSNMP	nfiguration Disabled SNMP v1 public Address Constrained Disabled Constrained	

Mode

Indicates the SNMP mode operation. Possible modes are:

Enable: Enable SNMP mode operation.

Disabled: Disable SNMP mode operation.

Version

Indicates the SNMP supported version. Possible versions are:

SNMPv1: Set SNMP supported version 1.

SNMPv2c: Set SNMP supported version 2c.

SNMPv3: Set SNMP supported version 3.

Read Community

Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.

The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Write Community

Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.

The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular

range of source addresses can be used to restrict source subnet.

Engine ID

Indicates the SNMPv3 engine ID. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

SNMP Trap Configuration

Configure SNMP trap on this page.

Trap Mode

Indicates the SNMP trap mode operation. Possible modes are:

Enable: Enable SNMP trap mode operation.

Disabled: Disable SNMP trap mode operation.

Trap Version

Indicates the SNMP trap supported version. Possible versions are:

SNMPv1: Set SNMP trap supported version 1.

SNMPv2c:Set SNMP trap supported version 2c.

SNMPv3: Set SNMP trap supported version 3.

Trap Community

Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126.

Trap Destination Address

Indicates the SNMP trap destination address.

Trap Destination IPv6 Address

Provide the trap destination IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Trap Authentication Failure

Indicates that the SNMP entity is permitted to generate authentication failure traps. Possible modes are: **Enable:** SNMP trap authentication failure.

Disabled: Disable SNMP trap authentication failure.

Trap Link-up and Link-down

Indicates the SNMP trap link-up and link-down mode operation. Possible modes are:

Enable: Enable SNMP trap link-up and link-down mode operation.

Disabled: Disable SNMP trap link-up and link-down mode operation.

Trap Inform Mode

Indicates the SNMP trap inform mode operation. Possible modes are:

Enable: Enable SNMP trap inform mode operation.

Disabled: Disable SNMP trap inform mode operation.

Trap Inform Timeout (seconds)

Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.

Trap Inform Retry Times

Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.

Trap Probe Security Engine ID

Indicates the SNMP trap probe security engine ID mode of operation. Possible values are:

Enable: Enable SNMP trap probe security engine ID mode of operation.

Disabled: Disable SNMP trap probe security engine ID mode of operation.

Trap Security Engine ID

Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.

Trap Security Name

Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

Buttons

Save: Click to save changes

Reset: Click to undo any changes made locally and revert to previously saved values

SNMPv3 Community Configuration

Configure SNMPv3 community table on this page:

The entry index key is Community.

-BLAET'			ALL8944WMP - Gigabi	t PoE Switch
 Device Reduction 		unity Configuration		
Ports	Delete Commu		Source Mask	
 Security 	= p	ublic 0.0.0.0	0.0.0.0	
 Switch Users 	pr	ivate 0.0.0.0	0.0.0.0	
Auth Method SSH HTTPS Access Management System Communities Users Groups Views Access RMON Matwork AAA Aggregation Jop Protection Bpanning Tree A/R PMC DD V	Add New Entry	Save Reset		

Delete

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

Community

Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.

Source IP

Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.

Source Mask

Indicates the SNMP access source address mask.

Buttons

Add new community: Click to add a new community entry

Save: Click to save changes

Reset: Click to undo any changes made locally and revert to previously saved values

SNMPv3 User Configuration

Configure SNMPv3 user table on this page. The entry index keys are Engine ID and User Name.

- ALINET			ALL8944WMP -	Gigabit PoE Switch	i		
Configuration System Power Reduction	MPv3 User Configuratio		6				
	elete Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
- Switch	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None
 SSH HTTPS Access Management Skystem Communites Usars Groups Views Access Rotoss RMON Naturack Aggregation Loop Protection Spanning Tree MVR IMPC 							

Delete

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

Engine ID

An octet string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usm User Engine ID and usm User Name are the entry's keys. In a simple agent, usm User Engine ID is always that agent's own snmp Engine ID value. The value can also take the value of the snmp Engine ID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.

User Name

A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Level

Indicates the security model that this entry should belong to. Possible security models are: **NoAuth, NoPriv:** No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.

Authentication Protocol

Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

None: No authentication protocol.

MD5: An optional flag to indicate that this user uses MD5 authentication protocol.

SHA: An optional flag to indicate that this user uses SHA authentication protocol.

The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.

Authentication Password

A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.

Privacy Protocol

Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

None: No privacy protocol.

DES: An optional flag to indicate that this user uses DES authentication protocol.

Privacy Password

A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

Add new user: Click to add a new user entry Save: Click to save changes Reset: Click to undo any changes made locally and revert to previously saved values

SNMPv3 Group Configuration

Configure SNMPv3 group table on this page:

The entry index keys are Security Mode and Security Name.

ALNET'		AL	L8944WMP - Gigabit PoE Switch	1 🕑 😨
onfiguration - System	SNMPv3 Group Con	figuration		
Power Reduction Ports	Delete Security Mo	del Security Name	Group Name	
Security	E	v1 public	default_ro_group	
- Switch		v1 private	default_rw_group	
Users Privilege Levels	E	v2c public	default_ro_group	
 Auth Method 	10	v2c private	default_rw_group	
SSH HTTPS	E 0	ism default_user	default_rw_group	
 SMMP System Communities Users Groups View5 Access RMON Natwork AAA Aggregation Loop Protection Spanning Tree MVR 				

Delete

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

Security Model

Indicates the security model that this entry should belong to. Possible security models are:

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM).

Security Name

A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Group Name

A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

Add new group: Click to add a new group entry

Save: Click to save changes

Reset: Click to undo any changes made locally and revert to previously saved values

SNMPv3 View Configuration

Configure SNMPv3 view table on this page.

BLNT'	ALL8944WMP - Gigabit PoE Switch	0 🕄
Configuration System Power Reduction Ports Security Security Switch Users Privilege Levels Auth Method SSH HTTPS Access Management SNMP System Communities Users Stress Access Acce	SNMPv3 View Configuration Delete View Name View Type OID Subtree default_view included •1 Add New Entry Save Reset	

The entry index keys are View Name and OID Sub-tree.

Delete

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

View Name

A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and

the allowed content is ASCII characters from 33 to 126.

HELMET '	ALL8944WMP - Gigabit PoE Switch	1
Configuration System Power Reduction Ports Security Security Security Security Security Security Statch Users Auth Method SSH HITTPS Access Management SMMP System Communities Users System Communities Users System Access FRMON Network Access FRMON Network Access FRMON Network Access Spanning Tree MVR IDPMC SUMP	SNMPv3 View Configuration Delete View Name View Type OID Subtree default_view included Add New Entry Savexcluded	

View Type

Indicates the view type that this entry should belong to. Possible view types are:

Included: An optional flag to indicate that this view sub-tree should be included.

excluded: An optional flag to indicate that this view sub-tree should be excluded.

In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID sub-tree should overstep the 'excluded' view entry.

OID Subtree

The OID defining the root of the sub-tree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

Buttons

Add new view: Click to add a new view entry

Save: Click to save changes

Reset: Click to undo any changes made locally and revert to previously saved values

SNMPv3 Access Configuration

Configure SNMPv3 access table on this page. The entry index keys are Group Name, Security Model, and Security Level.

-RUNET'		ALL8944WMP - Gigabit PoE Switch									
Configuration System Power Reduction		Access Config									
Ports	Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name					
✓ Security	1	default_ro_group	any	NoAuth, NoPriv	default_view 💌	None -					
 Switch 		default_rw_group	any	NoAuth, NoPriv	default_view -	default_view -					
Users Privilege Levels											
 Auth Method 	Add Nev	v Entry Save	Reset								
SSH HTTPS											
Access											
Management											
 SNMP System 											
 Communities 											
Users											
Groups Views											
 Access 											
RMON Network											
 AAA 											
 Aggregation 											
 Loop Protection 											
 Spanning Tree MVR 											
► IPMC											
NILDP *											
4 10 1											

Delete

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

Group Name

A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Model

Indicates the security model that this entry should belong to. Possible security models are:

Any: Any security model accepted(v1|v2c|usm).

V1:Reserved for SNMPv1.

V2c: Reserved for SNMPv2c.

Usm: User-based Security Model (USM).

Security Level : Indicates the security model that this entry should belong to. Possible security models are:

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

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, and the allowed content is ASCII characters from 33 to 126.

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, and the allowed content is ASCII characters from 33 to 126.

- ALLNET'					2			
Configuration System Power Reduction Power Reduction Ports Security Security Settch Users Privilega Levets Auth Method	Dele	Pv3 Access Config te Group Name default_ro_group default_rw_group	Security Model any any	Security Level NoAuth, NoPriv NoAuth, NoPriv	Read View Name default_view • default_view •	Vorite View Name	- Weight	
Auth Method SSH HTTPS Access Management SMMP System Communities Users Groups Views			Preser					
Access RMON Natheork AAA Aggregation Loop Protection Spanning Tree M//R IPMC II DP	٣							

Buttons

Add new access: Click to add a new access entry

Save: Click to save changes

Reset: Click to undo any changes made locally and revert to previously saved values

RMON Statistics Configuration

Configure RMON Statistics table on this page. The entry index key is ID.



Delete

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

ID

Indicates the index of the entry. The range is from 1 to 65535.

Data Source

Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch

ID-1), for example, if the port is switch 3 port 5, the value is 2005

Buttons

Add new entry: Click to add a new community entry

Save: Click to save changes

Reset: Click to undo any changes made locally and revert to previously saved values

RMON History Configuration

Configure RMON History table on this page. The entry index key is ID



Delete

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

ID

Indicates the index of the entry. The range is from 1 to 65535.

Data Source

Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch

ID-1), for example, if the port is switch 3 port 5, the value is 2005.

Interval

Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.

Buckets

Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.

Buckets Granted

The number of data shall be saved in the RMON.

Buttons

Add new entry: Click to add a new community entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

RMON Alarm Configuration

Configure RMON Alarm table on this page. The entry index key is ID.



Delete

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

ID

Indicates the index of the entry. The range is from 1 to 65535.

Interval

Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2/31-1.

Variable

Indicates the particular variable to be sampled, the possible variables are:

InOctets: The total number of octets received on the interface, including framing characters.

InUcastPkts:The number of uni-cast packets delivered to a higher-layer protocol.

InNUcastPkts: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.

InDiscards: The number of inbound packets that are discarded even the packets are normal.

InErrors: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

InUnknownProtos: The number of the inbound packets that were discarded because of the unknown or

un-support protocol.

OutOctets: The number of octets transmitted out of the interface , including framing characters. OutUcastPkts: The number of uni-cast packets that request to transmit.

OutNUcastPkts: The number of broad-cast and multi-cast packets that request to transmit.

OutDiscards: The number of outbound packets that are discarded event the packets is normal.

OutErrors: The number of outbound packets that could not be transmitted because of errors.

OutQlen: The length of the output packet queue (in packets).

Sample Type

The method of sampling the selected variable and calculating the value to be compared against the

thresholds, possible sample types are:

Absolute: Get the sample directly.

Delta: Calculate the difference between samples (default).

Value

The value of the statistic during the last sampling period.

Startup Alarm

The method of sampling the selected variable and calculating the value to be compared against the

thresholds, possible sample types are:

RisingTrigger alarm when the first value is larger than the rising threshold.

FallingTrigger alarm when the first value is less than the falling threshold.

RisingOrFallingTrigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).

Rising Threshold

Rising threshold value (-2147483648-2147483647).

Rising Index

Rising event index (1-65535).

Falling Threshold

Falling threshold value (-2147483648-2147483647)

Falling Index

Falling event index (1-65535).

Buttons

Add new entry: Click to add a new community entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

RMON Event Configuration

Configure RMON Event table on this page. The entry index key is ID.



Delete

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

ID

Indicates the index of the entry. The range is from 1 to 65535.

Desc

Indicates this event, the string length is from 0 to 127, default is a null string.

Туре

Indicates the notification of the event, the posible types are:

None: The total number of octets received on the interface, including framing characters.

Log: The number of uni-cast packets delivered to a higher-layer protocol.

Snmptrap: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.

Logandtrap: The number of inbound packets that are discarded even the packets are normal.

community

Specify the community when trap is sent, the string lengh is from 0 to 127, default is "public".

Event Last Time

Indicates the value of sysUp Time at the time this event entry last generated an event.

Buttons

Add new entry: Click to add a new community entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Port Security Limit Control Configuration

This page allows you to configure the Port Security Limit Control system and port settings.

LINET'					ALL8944	WMP - Gig	abit PoE Switch	
nfiguration –	David C	e e unite a s	mil Control	Confe	mation			(Department)
ystem	Ports	ecurity Li	mit Contro	Config	uration			Refresh
Power Reduction Ports	System	n Configur	ation					
Security	Mode		Disabled					
 Switch Notwork 		Enabled	0	1000				
Limit Control NAS	Aging	Period	3600 \$	econds				
ACL	Port C	onfiguratio	m					
IP Source Guard =	Port	Mode	Limit	1	Action	State	Re-open	
ARP Inspection AAA	7	and the second s	-	0	-	orare	No open	
Aggregation	1	Disabled		None		Disabled	Reopen	
Spanning Tree	2	Disabled		None	-	Disabled	Reppen	
WVR PMC	3	Disabled		None		Disabled	Reppen	
LLDP	4	Disabled				Disabled	Reopen	
PoE MAC Table	5	Disabled				Disabled	Reppen	
VLANs	6	Disabled		Lan prost of the		Disabled	Reopen	
Private VLANs VCL		Charles and the second			and a second			
Voice VLAN	7	Disabled				Disabled	Reopen	
CoS .	8	Disabled				Disabled	Reopen	
	9	Disabled		C. C		Disabled	Reopen	
	10	Disabled	648 ····			Disabled	Reopen	
	11	Disabled	•	None		Disabled	Reopen	
	12	Disabled		None	•	Disabled	Reopen	
	13	Disabled		None		Disabled	Reopen	
	14	Disabled	• •	None N	•	Disabled	Reopen	
	15	Disabled		None		Disabled	Reopen	
	16	Disabled	-	None		Disabled	Reopen	
	17	Disabled		None		Disabled	Reopen	
	18	Disabled	-	None		Disabled	Reopen	
	19	Disabled		None		Disabled	Reppen	
	20	Disabled	-	None		Disabled	Reopen	
	21	Disabled			v	Disabled	Reopen	
	22	Disabled	414			Disabled	Reopen	
	23	Disabled				Disabled	Reopen	
		and the second s		1			and the second	
	24	Disabled				Disabled	Reopen	
	26	Disabled	-			Disabled	Reopen	
	26	Disabled		None	•	Disabled	Reopan	

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

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

System Configuration

Mode

Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

Aging Enabled

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

Aging Period

If Aging Period is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.

The Aging Period can be set to a number between 10 and 10,000,000 seconds.

To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Port Configuration

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

Port

The port number to which the configuration below applies.

Mode

Controls whether Limit Control is enabled 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:

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. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:

1) Boot the switch,

2) Disable and re-enable Limit Control on the port or the switch,

3) Click the Reopen button.

Trap & Shutdown: If Limit + 1 MAC addresses 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:

Disabled: Limit Control is either globally disabled or disabled on the port.

Ready: The limit is not yet reached. This can be shown for all actions.

Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to

None or Trap.

Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to **Shutdown** or **Trap & Shutdown**.

Re-open Button

If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to **Shutdown** in the Action section.

Note that clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost.

Buttons

Refresh: Click to refresh the page. Note that non-committed changes will be lost.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Network / Network Access Server Configuration

This page allows you to configure the IEEE802.1X and MAC-based authentication system and port settings.

BLINET'				1	LL8944WMP - Gi	gabit PoE Swit	ich		
onfiguration	Martin	ale Annana Da		laura l'aur					(
System Power Reduction		ork Access Serve	ar Cont	guration					Refresh
Ports	System	n Configuration							
Security Switch	Mode		6	Disabled	•				
 Noteork Limit Control 		hentication Enabled	1	E .	-				
• NAS • ACL	and the local division of the	hentication Period		3600	seconds				
► DHCP	and the second second	Period		300	seconds				
ARP Inspection	Hold 1	fime		10	seconds				
• AAA Aggregation	and the second second	JS-Assigned QoS E JS-Assigned VLAN	and the second						
Loop Protection Spanning Tree		VLAN Enabled	enabled						
MVR	Guest	VLAN ID		1	1				
IPMC LLDP	10000	Reauth. Count	-	2	1				
PoE MAC Table		Guest VLAN If EAP	OL Seen						
VLANs	Port C	onfiguration							
Private VLANs VCL Voice VLAN QoS	Port	Admin State		RADIUS- Assigned QoS Enabled	RADIUS- Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Rest	art
		0	-	Enabled	Enabled				
	1	Force Authorized		10	0	0	Globally Disabled	Reautherdicate	Reinitializ
	2	Force Authorized	•				Globally Disabled	Reautheriticale	Reinitializ
	3	Force Authorized	•	.0	-	12	Globally Disabled	Reauthenticate	Reinitaliz
	4	Force Authorized					Globally Disabled	Reauthenticate	Reinitializa
	5	Force Authorized	·	E			Globally Disabled	Reauthernicate	Reinitialtz
	6	Force Authorized					Globally Disabled	Reauthenticate	Reinitieltz
	7	Force Authorized		Ð	.0	Ξ	Globally Disabled	Reauthenticate	Reinitializ
	8	Force Authorized	•				Globally Disabled	Reauthenticate	Reinitializ
	9	Force Authorized	-	Ð	<u>11</u>	12	Globally Disabled	Reauthenticate	Reinitiallz
	10	Force Authorized					Globally Disabled	Reauthenticate	Reinitializ
	11	Force Authorized	•				Globally Disabled	Reauthenticate	Reintialtz
	12	Force Authorized					Globally Disabled	Reauthenticate	Reinitializ
	13	Force Authorized					Globally Disabled	Reauthenticate	Reinitializ
	14	Force Authorized	•				Globally Disabled	Reautherticate	Reinitaliz
	15	Force Authorized		13			Globally	Reauthenticate	Reinitialize
	16	Force Authorized	-				Disabled Globally	Reauthenticate	Reinitializa
	17	Force Authorized	-				Disabled Globally	Reauthenticate	Reinitializ
	18	Force Authorized					Disabled Globally	Reauthenticate	Reintializ
	19	Force Authorized	125.1	0			Disabled Globally	Resuthenticate	Reinitializ
	20	Force Authorized		10	101	1401	Disabled Globally	Reauthenticate	Reinitializ
	2000		-				Disabled Globally	Reautheriticate	
	21	Force Authorized	*				Disabled Globally		Reinitializa
	22	Force Authorized					Disabled Globally	Reauthenticate	Reinitialize
	23	Force Authorized		D			Disabled Globally	Reauthenticate	Reinitializa
	24	Force Authorized					Disabled Globally	Reauthenticate	Reinitieliza
	25	Force Authorized					Disabled	Reauthenticate	Reinitializa
	26	Force Authorized					Globally Disabled	Reauthenticate	Reinitaliza

Save Reset

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

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

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

System Configuration

Mode

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 65535 seconds. This has no effect for MAC-based ports.

Aging Period

This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

- 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 Port Security functionality to secure MAC addresses:

- Single 802.1X
- Multi 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 RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature.

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 the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. 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 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 switchand a number of columns, which are:

Port

The port number for which the configuration below applies.

Admin State

If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:

Force Authorized

In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

Force Unauthorized

In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

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

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 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:

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.

RADIUS attributes used in identifying a VLAN ID:

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:

• The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-IDattributes must all be present at least once in the Access-Accept packet.

• 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-IDdoes not need to include a Tag):

- Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).

- Value of Tunnel-Type must be set to "VLAN" (ordinal 13).

- 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].

Guest VLAN Enabled

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.

This option is only available for EAPOL-based modes, i.e.:

- Port-based 802.1X
- Single 802.1X
- Multi 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.

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<u>http://192.168.1.6/help/help_nas.htm - max_reauth_cnt</u> 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:

Globally Disabled: NAS is globally disabled.

Link Down: NAS is globally enabled, but there is no link on the port.

Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized. Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.

X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

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.

Reauthenticate: Schedules a reauthentication whenever the quiet-period of the port runs out(EAPOL-based authentication).For MAC-based authentication, reauthentication will be attempted immediately.

The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

Reinitialize: 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.

Buttons

Refresh: Click to refresh the page. Save: Click to save changes. Reset: Click to undo any changes made locally and revert to previously saved values.

Access Control List Configuration

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.

elinet'	ALL8944WMP - Gigabit PoE Switch										
onfiguration System	ACL P	orts Config	uration						Refresh	Clear	
Power Reduction Ports Security	Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter	
Network Emit Control NAS	2	0	•	•	Port 1 Mil Port 2 *	•	•	•	•		
ACL Ports Rate Limiters Access	1	٥	Permit	Disabk •	Port 1 RP Port 2 *	Disabled •	Disabled	Disabled .	Enabled *	0	
Control List DHCP IP Source Guard ABP Inspection	2	0	Permit	Disable	Port 1 00 Port 2 -	Disabled	Disabled •	Disabled 💌	Enabled •	c	
ARP Inspection AAA Aggregation Loop Protection	3	0	Permit	Disable •	Port 1 Bill Port 2 -	Disabled *	Disabled •	Disabled 💌	Enabled *	0	
Spanning Tree MVR IPMC	4	0	Permit -	Disable -	Port 1 El Port 2 -	Disabled -	Disabled -	Disabled •	Enabled -	C	
LLDP PoE MAC Table	5	0	Permit •	Disabk *	Port 1 El Port 2 -	Disabled •	Disabled +	Disabled +	Enabled •	¢	
VLANs Private VLANs	6	0	Permit	Disabk -	Port 1 Port 2 *	Disabled -	Disabled -	Disabled -	Enabled -	¢	
	7	0	Permit	Disable •	Port 1 Port 2 -	Disabled .	Disabled	Disabled 💌	Enabled •	(
	8	0	Permit	Disabk +	Port 1 III Port 2 *	Disabled +	Disabled -	Disabled 💽	Enabled •	0	
	9	0	Permit •	Disabk •	Port 1 III Port 2 -	Disabled *	Disabled •	Disabled +	Enabled •	0	
	10	0	Permit -	Disabk -	Port 1 Port 2 -	Disabled -	Disabled -	Disabled +	Enabled -	c	
	11	0	Permit -	Disabk	Port 1 Port 2 *	Disabled -	Disabled •	Disabled 🔽	Enabled -	c	
	12	0	Permit	Disabk	Port 1 Port 2 T	Disabled •	Disabled	Disabled 💌	Enabled •	¢	
	13	0	Permit .	Disable	Port 1 1 Port 2 -	Disabled	Disabled .	Disabled •	Enabled •	¢	
	14	0	Permit	Disable	Port 1 Hill Port 2 *	Disabled -	Disabled -	Disabled 💌	Enabled 💌	7312	
	15	0	Permit	Disabk •	Port 1 Fil Port 2 -	Disabled -	Disabled ×	Disabled .	Enabled +	0	
	16	0	Permit •	Disabk •	Port 1 Port 2 -	Disabled	Disabled	Disabled	Enabled •	0	
	17	0	Permit •	Disabk -	Port 1 Fil Port 2 -	Disabled -	Disabled -	Disabled +	Enabled -	O	
	18	0	Permit	Disabk	Port 1 E Port 2 *	Disabled •	Disabled	Disabled -	Enabled -	O	
	19	0	Permit	Disabk •	Port 1 E Port 2 T	Disabled •	Disabled •	Disabled 🔹	Enabled -	٥	
	20	0	Permit	Disable	Port 1 Port 2 =	Disabled •	Disabled	Disabled 💌	Enabled 💌	0	
	21	0	Permit .	Disable •	Port 1 Hill Port 2 *	Disabled -	Disabled *	Disabled x	Enabled •	0	
	22	0	Permit	Disable	Port 1 III Port 2 -	Disabled	Disabled	Disabled .	Enabled •	0	
	23	0	Permit	Disabk •	Port 1 Port 2 -	Disabled ×	Disabled *	Disabled 💌	Enabled •	0	
	24	0	Permit -	Disabk -	Port 1 Port 2 -	Disabled -	Disabled -	Disabled -	Enabled •	0	
	25	0	Permit	Disabk +	Port 1 El Port 2 *	Disabled +	Disabled •	Disabled +	Enabled •	0	
	26	0	Permit -	Disabk -	Port 1 E	Disabled •	Disabled .	Disabled -	Enabled •	٥	

Save Reset

Port

The logical port for the settings contained in the same row.

Policy ID

Select the policy to apply to this port. The allowed values are **0** through **255**. The default value is 0.

Action

Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".

Rate Limiter ID

Select which rate limiter to apply on this port. The allowed values are **Disabled** or the values **1** through **16**. The default value is "Disabled".

DisabledPort Copy

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:

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored.

The default value is "Disabled".

Logging

Specify the logging operation of this port. The allowed values are:

Enabled: Frames received on the port are stored in the System Log.

Disabled : Frames received on the port are not logged.

The default value is "Disabled". Please note that the System Log memory size and logging rate is limited.

Shutdown

Specify the port shut down operation of this port. The allowed values are:

Enabled: If a frame is received on the port, the port will be disabled.

Disabled: Port shut down is disabled.

The default value is "Disabled".

Counter

Counts the number of frames that match this ACE.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Click to refresh the page. Any changes made locally will be undone..

Clear: Click to clear the counter

ACL Rate Limiters Configuration

Configure the rate limiter for the ACL of the switch

- PLINET'				ALL8944WMP - Gigabit PoE Switch	D (
, .,	CL Rate Limiter	Configura	tion		and the second
Power Reduction Ports	Rate Limiter ID	Rate	Un	t	
- Security		1	0		
Switch	1	1	pps	•	
 Network Limit Control 	2	1	pps	•	
• NAS • ACL	3	1	pps	•	
Ports	4	1	pps	•	
 Rate Limiters Access 	5	1	pps	•	
Control List	6	1	pps	•	
 DHCP IP Source Guard 	7	1	pps	•	
ARP Inspection	8	1	pps	•	
AAA Aggregation	9	1	pps		
Loop Protection	10	1	pps	•	
Spanning Tree	11	1	pps	•	
• MVR • IPMC	12	1	pps	•	
LLDP	13	1	pps	•	
PoE	14	1	pps	•	
MAC Table VLANs	15	1	pps	•	
Private VLANs	16	1	pps	•	

Rate Limiter ID

The rate limiter ID for the settings contained in the same row.

Rate

The allowed values are: 0-3276700 in pps

Or 0,100,200,300,...,1000000 in kbps.

Unit

Specify the rate unit. The allowed values are:

pps: packets per second.

kbps: Kbits per second.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Access Control List Configuration

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is **256** on each switch.

Runn'	AL	.8944WMP - Gigabit PoE Switch	6 2
Configuration System Power Reduction Ports Security Smitch NAS ACL Ports Rate Limiters Access Control List DHCP PIP Source Guard ARP Inspection Adgragation Loop Protection Spanning Tree MVR IPMC LLDP PoE MAC Table VLANs Private VLANs	Access Control List Configuration	Auto-refresh Crefresh	Clear Remove All

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

GUNT	ALL8944WMP - Gigabit PoE Switch						1 2	
Configuration System Power Reduction Ports Security Smitch Network Imit Control NAS ACL Ports Por	Access Control List Configura				Refresh	Counter	Remove All	

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.

Policy / Bitmask

Indicates the policy number and bitmask of the ACE.

Frame Type

Indicates the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.

EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.

IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.

IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.

IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.

IPv6: The ACE will match all IPv6 standard frames.

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 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. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored.

The default value is "Disabled".

Counter

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

Modification Buttons

You can modify each ACE (Access Control Entry) in the table using the following buttons:

Inserts a new ACE before the current row.

(e): Edits the ACE row.

- (1): Moves the ACE up the list.
- Solution: The ACE down the list.
- S: Deletes the ACE.
- 🕒: The lowest plus sign adds a new entry at the bottom of the ACE listings.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.

Refresh: Click to refresh the page. Note that non-committed changes will be lost.

Clear: Click to clear the counter

Remove All: Click to remove all ACEs

ACE Configuration

Configure an ACE (Access Control Entry) on this page.

An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type selected.

A frame that hits this ACE matches the configuration that is defined here.

Ingress Port

Select the ingress port for which this ACE applies.

All: The ACE applies to all port.

Port n: The ACE applies to this port number, where n is the number of the switch port.

Ploicy Filter

Specify the policy number filter for this ACE.

Any: No policy filter is specified. (policy filter status is "don't-care".)

Specific: If you want to filter a specific policy with this ACE, choose this value. Two field for entering an policy value and bitmask appears.

Ploicy Value

When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is **0** to **255**.

Ploicy Bitmask

When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is **0x0** to **0xff**.

Frame Type

Select the frame type for this ACE. These frame types are mutually exclusive.

Any: Any frame can match this ACE.

Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal). ARP: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type. IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.

IPv6: Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with ehternet type.

Action

Specify the action to take with a frame that hits this ACE.

Permit: The frame that hits this ACE is granted permission for the ACE operation.

Deny: The frame that hits this ACE is dropped.

Rate Limiter

Specify the rate limiter in number of base units. The allowed range is **1** to **16**. **Disabled** indicates that the rate limiter operation is disabled.

Port Copy

Frames that hit the ACE are copied to the port number specified here. The allowed range is the same as the switch port number range. **Disabled** indicates that the port copy operation is disabled.

Mirror

Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination

mirror port. The allowed values are:

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored.

The default value is "Disabled".

Logging

Specify the logging operation of the ACE. The allowed 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

Specify the port shut down operation of the ACE. The allowed values are:

Enabled: If a frame matches the ACE, the ingress port will be disabled.

Disabled: Port shut down is disabled for the ACE.

Counter

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

MAC Parameters

SMAC Filter

(Only displayed when the frame type is Ethernet Type or ARP.)

Specify the source MAC filter for this ACE.

Any: No SMAC filter is specified. (SMAC filter status is "don't-care".)

Specific: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.

SMAC Value

When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx". A frame that hits this ACE matches this SMAC value.

DMAC Filter

Specify the destination MAC filter for this ACE.

Any: No DMAC filter is specified. (DMAC filter status is "don't-care".)

MC: Frame must be multicast.

BC: Frame must be broadcast.

UC: Frame must be unicast.

Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.

DMAC Value

When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this DMAC value.

VLAN Parameters

802.1Q Tagged

Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are:

Any: Any value is allowed ("don't-care").

Enabled: Tagged frame only.

Disabled: Untagged frame only.

The default value is "Any".

VLAN ID Filter

Specify the VLAN ID filter for this ACE.

Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)

Specific: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.

VLAN ID

When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is **1** to **4095**. A frame that hits this ACE matches this VLAN ID value.

Tag Priority

Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is **0** to **7**. The value **Any** means that no tag priority is specified (tag priority is "don't-care".)

ARP Parameters

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

ARP/<u>RARP</u>

Specify the available ARP/RARP opcode (OP) flag for this ACE.

Any: No ARP/RARP OP flag is specified. (OP is "don't-care".)

ARP: Frame must have ARP/RARP opcode set to ARP.

RARP: Frame must have ARP/RARP opcode set to RARP.

Other: Frame has unknown ARP/RARP Opcode flag.

Request/Reply

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

Sender IP Filter

Specify the sender IP filter for this ACE.

Any: No sender IP filter is specified. (Sender IP filter is "don't-care".)

Host: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears.

Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.

Sender IP Address

When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in <u>dotted decimal notation</u>.

Sender IP Mask

When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in <u>dotted</u> <u>decimal notation</u>.

Target IP Filter

Specify the target IP filter for this specific ACE.

Any: No target IP filter is specified. (Target IP filter is "don't-care".)

Host: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that

appears.Network: Target IP filter is set to Network. Specify the target IP address and target IP mask

in the Target IP Address and Target IP Mask fields that appear.

Target IP Address

When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.

Target IP Mask

When "Network" is selected for the target IP filter, you can enter a specific target IP mask in <u>dotted</u> <u>decimal notation</u>.

ARP SMAC Match

Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.

0: ARP frames where SHA is not equal to the SMAC address.

1: ARP frames where SHA is equal to the SMAC address.

Any: Any value is allowed ("don't-care").

RARP DMAC Match

Specify whether frames can hit the action according to their target hardware address field (THA)

settings.

0: RARP frames where THA is not equal to the DMAC address.

1: RARP frames where THA is equal to the DMAC address.

Any: Any value is allowed ("don't-care").

IP/Ethernet Length

Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.

0: ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).

1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04).

Any: Any value is allowed ("don't-care").

IP

Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.

0: ARP/RARP frames where the HLD is not equal to Ethernet (1).

1: ARP/RARP frames where the HLD is equal to Ethernet (1).

Any: Any value is allowed ("don't-care").

Ethernet

Specify whether frames can hit the action according to their ARP/RARP protocol address space

(PRO) settings.

0: ARP/RARP frames where the PRO is not equal to IP (0x800).

1: ARP/RARP frames where the PRO is equal to IP (0x800).

Any: Any value is allowed ("don't-care").

IP Parameters

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

IP Protocol Filter

Specify the IP protocol filter for this ACE.

Any: No IP protocol filter is specified ("don't-care").

Specific: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears.

ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters

will appear. These fields are explained later in this help file.

UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.

TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.

IP Protocol Value

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

IP TTL

Specify the Time-to-Live settings for this ACE.

zero: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.
 non-zero: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.
 Any: Any value is allowed ("don't-care").

IP Fragment

Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.

No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.

Yes: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.

Any: Any value is allowed ("don't-care").

IP Option

Specify the options flag setting for this ACE.

No: IPv4 frames where the options flag is set must not be able to match this entry.

Yes: IPv4 frames where the options flag is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

SIP Filter

Specify the source IP filter for this ACE.

Any: No source IP filter is specified. (Source IP filter is "don't-care".)

Host: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.

Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.

SIP Address

When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in <u>dotted decimal notation</u>.

SIP Mask

When "Network" is selected for the source IP filter, you can enter a specific SIP mask in <u>dotted</u> <u>decimal notation</u>.

DIP Filter

Specify the destination IP filter for this ACE.

Any: No destination IP filter is specified. (Destination IP filter is "don't-care".)

Host: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.

Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.

DIP Address

When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.

DIP Mask

When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in <u>dotted</u> <u>decimal notation</u>.

ICMP Parameters

ICMP Type Filter

Specify the ICMP filter for this ACE.

Any: No ICMP filter is specified (ICMP filter status is "don't-care").

Specific: If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP

value. A field for entering an ICMP value appears.

ICMP Type Value

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

ICMP Code Filter

Specify the ICMP code filter for this ACE.

Any: No ICMP code filter is specified (ICMP code filter status is "don't-care").

Specific: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP

code value. A field for entering an ICMP code value appears.

ICMP Code Value

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

TCP/UDP Parameters

TCP/UDP Source Filter

Specify the TCP/UDP source filter for this ACE.

Any: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care").

Specific: If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific

TCP/UDP source value. A field for entering a TCP/UDP source value appears.

Range: If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.

TCP/UDP Source No.

When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Source Range

When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Destination Filter

Specify the TCP/UDP destination filter for this ACE.

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

TCP/UDP Destination Number

When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP destination value.

TCP/UDP Destination Range

When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP destination value.

TCP FIN

Specify the TCP "No more data from sender" (FIN) value for this ACE.

0: TCP frames where the FIN field is set must not be able to match this entry.

1: TCP frames where the FIN field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

TCP SYN

Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE.

0: TCP frames where the SYN field is set must not be able to match this entry.

1: TCP frames where the SYN field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

TCP RST

Specify the TCP "Reset the connection" (RST) value for this ACE.

0: TCP frames where the RST field is set must not be able to match this entry.

1: TCP frames where the RST field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

TCP PSH

Specify the TCP "Push Function" (PSH) value for this ACE.

0: TCP frames where the PSH field is set must not be able to match this entry.

1: TCP frames where the PSH field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

TCP ACK

Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.

0: TCP frames where the ACK field is set must not be able to match this entry.

1: TCP frames where the ACK field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

TCP URG

Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.

0: TCP frames where the URG field is set must not be able to match this entry.

1: TCP frames where the URG field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

Ethernet Type Parameters

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

EtherType Filter

Specify the Ethernet type filter for this ACE.

Any: No EtherType filter is specified (EtherType filter status is "don't-care").

Specific: If you want to filter a specific EtherType filter with this ACE, you can enter a specific

EtherType value. A field for entering a EtherType value appears.

Ethernet Type Value

When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is **0x600** to **0xFFFF** but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.

DHCP Snooping Configuration

Configure DHCP Snooping on this page.

Snooping Mode

Indicates the DHCP snooping mode operation. Possible modes are:

Enabled: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports. **Disabled**: Disable DHCP snooping mode operation.

Port Mode

Indicates the DHCP snooping port mode. Possible port modes are:

Trusted: Configures the port as trusted source of the DHCP messages.

Untrusted: Configures the port as untrusted source of the DHCP messages.

(ALLANT)		ALL8944WMP - Gigabit PoE Switch	1 2	
Configuration System Power Reduction Ports Security Smitch NAS NAS	DHCP Snooping Configuration Snooping Mode Disabled • Port Mode Configuration Port Mode Configuration Port Mode Configuration 1 Trusted • 1 Trusted • 2 Trusted • 3 Trusted • 4 Trusted • 5 Trusted • 6 Trusted • 10 Trusted • 11 Trusted • 12 Trusted • 13 Trusted • 14 Trusted • 15 Trusted • 16 Trusted • 17 Trusted • 17 Trusted • 18 Trusted • 19 Trusted • 19 Trusted • 119 Trusted • 100 Trusted • 12 Trusted • 13 Trusted • 14 Trusted • 15 Trusted • 16 Trusted • 17 Trusted • 17 Trusted • 18 Trusted • 19 Trusted • 20 Trusted • 21 Trusted • 21 Trusted • 21 Trusted • 23 Trusted • 23 Trusted •	ALL8944WMP - Gigabit PoE Switch		
	26 Trusted - Save Reset			

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

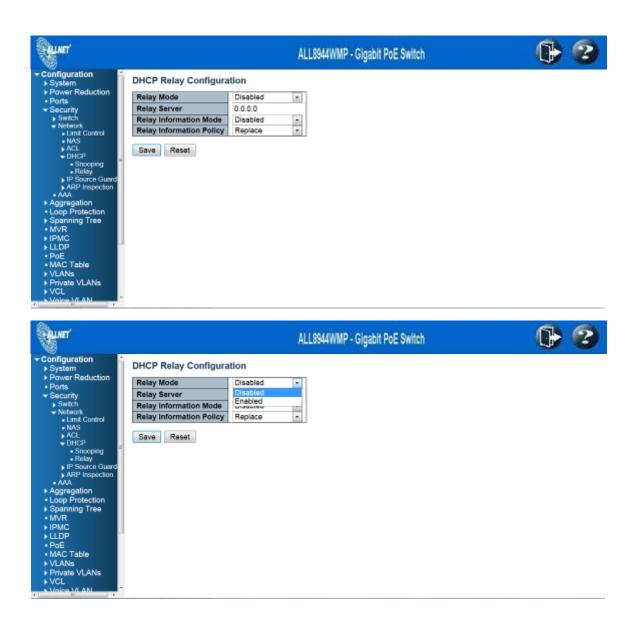
DHCP Relay Configuration

Configure DHCP Relay on this page.

Relay Mode

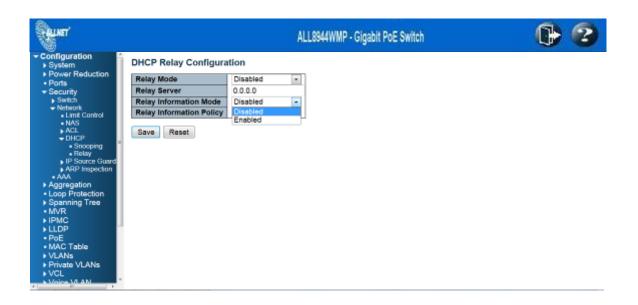
Indicates the DHCP relay mode operation. Possible modes are:

Enabled: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations. **Disabled**: Disable DHCP relay mode operation.



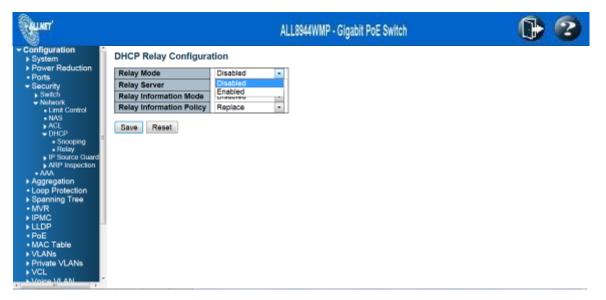
Relay Server

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 Mode

Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID(in standalone device it always equal 0, in stackable device it means switch ID).), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address. Possible modes are:





Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.

Disabled: Disable DHCP relay information mode operation.

Relay Information Policy

Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if 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: **Replace:** Replace the original relay information when a DHCP message that already contains it is received. **Keep:** Keep the original relay information when a DHCP message that already contains it is received. **DDrop:**:Drop the package when a DHCP message that already contains relay information is received.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

IP Source Guard Configuration

This page provides IP Source Guard related configuration.

Configuration System Prover Reduction Configuration Prots Source Guard Configuration Prots Source Guard Configuration Configuration Configuration System Source Guard Node Disabled Prot Prote	1 2
Notivouk Long Control Notivouk Control Contro Contro Control Control	
Proceeding of the second	
Configuration Configuration Configuration Configuration AAA Aggregation Cossbied Continue Cossbied Continute Cossbied Continu	
AGA Aggregation AGA Aggregation Loop Protection Spanning Tree MVR Spanning Tree MVR Disabled - Unlimited v v Disabled - Unlimited	
 AAA Aggregation Loop Protection Spanning Tree MVR IPMC IDisabled • Unlimited • Bisbled • Unlimited • Disabled • Unlimited • 	
Loop Protection Spanning Tree WVR PMC PMC POE POE MVR Port POE MVR Poe MVR Disabled Unlimited v Disabled Unlimited v	
Spanning Tree MVR PMR 4 0 Disabled Unlimited 4 0 Disabled Unlimited 4 0 Disabled Unlimited 4 0 Disabled Unlimited 4 0 Disabled Unlimited 4 0 Disabled Unlimited 4 0 Disabled Unlimited 4 1 1 1 0 Disabled Unlimited 4 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1	
AVXR SPACE Source Service Serv	
LLDP 6 Disabled • Unlimited • POE Disabled • Unlimited • VLANs 0 Disabled • Unlimited • Private VLANs 0 Disabled • Unlimited • 10 Disabled • Unlimited • • 11 Disabled • Unlimited • • 12 Disabled • Unlimited • • 13 Disabled • Unlimited • • 14 Disabled • Unlimited • • 15 Disabled • Unlimited • • 16 Disabled • Unlimited • • 17 Disabled • Unlimited • • 18 Disabled • Unlimited • • 19 Disabled • Unlimited • • 20 Disabled • Unlimited • • 21 Disabled • Unlimited • • 22 Disabled • Unlimited • • 21 Disabled • Unlimited • • 22 Disabled • Unlimited • •	
Pole MAC Table MAC Table MAC Table MAC Table VLANs Private VLANs VCLANs V	
NUCLANS 0 Disabled - Unlimited - Private VLANS 0 Disabled - Unlimited - VCL 10 Disabled - Unlimited - 11 Disabled - Unlimited - - 12 Disabled - Unlimited - - 13 Disabled - Unlimited - - 14 Disabled - Unlimited - - 15 Disabled - Unlimited - - 16 Disabled - Unlimited - - 17 Disabled - Unlimited - - 18 Disabled - Unlimited - - 19 Disabled - Unlimited - - 10 Disabled - Unlimited - - 12 Disabled - Unlimited - - 13 Disabled - Unlimited - - 14 Disabled - Unlimited - - 15 Disabled - Unlimited - - 18 Disabled - Unlimited - - 19 Disabled - Unlimited - - 20 Disabled - Unlimited - - 21 Disabled - Unlimited - - 22 Disabled - Unlimited - - 22 Disabled - Unlimited - - 22 Disabled - Unlimited - -	
Private VLANs VCL SVCL	
 VCL 10 Disabled - Unlimited - 11 Disabled - Unlimited - 12 Disabled - Unlimited - 13 Disabled - Unlimited - 14 Disabled - Unlimited - 15 Disabled - Unlimited - 16 Disabled - Unlimited - 17 Disabled - Unlimited - 18 Disabled - Unlimited - 19 Disabled - Unlimited - 20 Disabled - Unlimited - 21 Disabled - Unlimited - 22 Disabled - Unlimited - 	
11 Disabled Unlimited • 12 Disabled Unlimited • 13 Disabled Unlimited • 14 Disabled Unlimited • 15 Disabled Unlimited • 16 Disabled Unlimited • 17 Disabled Unlimited • 18 Disabled Unlimited • 19 Disabled Unlimited • 20 Disabled Unlimited • 21 Disabled Unlimited • 22 Disabled Unlimited •	
12 Disabled Unlimited + 13 Disabled Unlimited + 14 Disabled Unlimited + 15 Disabled Unlimited + 16 Disabled Unlimited + 17 Disabled Unlimited + 18 Disabled Unlimited + 19 Disabled Unlimited + 20 Disabled Unlimited + 21 Disabled Unlimited + 22 Disabled Unlimited +	
13 Disabled Unlimited • 14 Disabled Unlimited • 15 Disabled Unlimited • 16 Disabled Unlimited • 17 Disabled Unlimited • 18 Disabled Unlimited • 19 Disabled Unlimited • 20 Disabled Unlimited • 21 Disabled Unlimited •	
14 Disabled Unlimited • 15 Disabled Unlimited • 16 Disabled Unlimited • 17 Disabled Unlimited • 18 Disabled Unlimited • 19 Disabled Unlimited • 20 Disabled Unlimited • 21 Disabled Unlimited • 22 Disabled Unlimited •	
15 Disabled Unlimited * 16 Disabled Unlimited * 17 Disabled Unlimited * 18 Disabled Unlimited * 19 Disabled Unlimited * 20 Disabled Unlimited * 21 Disabled Unlimited * 22 Disabled Unlimited *	
16 Disabled • 17 Disabled • 18 Disabled • 19 Disabled • 20 Disabled • 21 Disabled • 22 Disabled • 23 Disabled • 24 Disabled •	
17 Disabled Unlimited • 18 Disabled Unlimited • 19 Disabled Unlimited • 20 Disabled Unlimited • 21 Disabled Unlimited • 22 Disabled Unlimited •	
18 Disabled • 19 Disabled • 20 Disabled • 21 Disabled • 22 Disabled • 23 Disabled •	
19 Disabled - 20 Disabled - 21 Disabled - 22 Disabled - 21 Disabled -	
20 Disabled • 21 Disabled • 22 Disabled •	
21 Disabled - Unlimited - 22 Disabled - Unlimited -	
22 Disabled • Unlimited •	
24 Disabled - Unlimited -	
25 Disabled - Unlimited -	
26 Disabled × Unlimited ×	

Mode of IP Source Guard Configuration

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 Mode Configuration

Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.

Max Dynamic Clients

Specify the maximum number of dynamic clients that can be learned on 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, it means only allow the IP packets forwarding that are matched in static entries on the specific port.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Translate dynamic to static: Click to translate all dynamic entries to static entries.

IP Source Guard Static Table

Delete

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

Port

The logical port for the settings.

VLAN ID

The vlan id for the settings.

IP Address

Allowed Source IP address.

MAC address

Allowed Source MAC address.

Adding new entry

Click to add a new entry to the Static IP Source Gurard table. Specify the Port, VLAN ID, IP address, and IP Mask for the new entry. Click "Save".





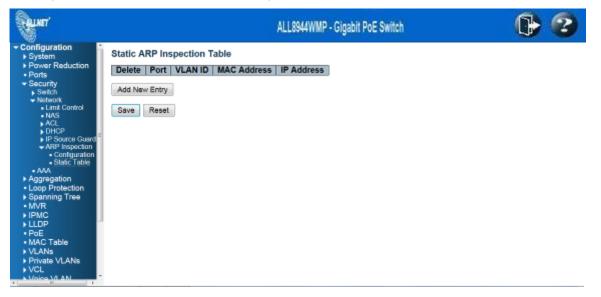
Buttons

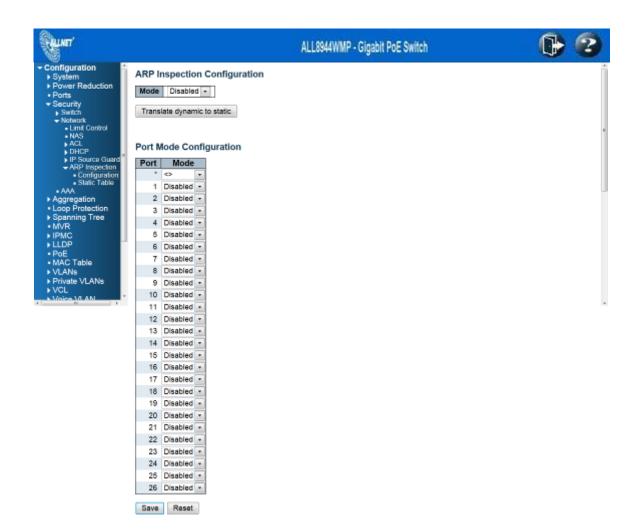
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

ARP Inspection

This page provides ARP Inspection related configuration.





Mode of ARP Inspection Configuration

Enable the Global ARP Inspection or disable the Global ARP Inspection.

Port Mode Configuration

Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Translate dynamic to static: Click to translate all dynamic entries to static entries.

ARP Inspection-Static Table

RUNET'	ALL8944WMP - Gigabit PoE Switch	0	2
 Configuration System Power Reduction Ports Security Switch Imm Control NAS ACL DHCP IP Source Guard APP Inspection Contiguration Contiguration Loop Protection Spanning Tree MVR ILDP POE MAC Table VLANs VLANs VLANs VLANs VLANs VLANs 			

Delete

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

Port

The logical port for the settings.

VLAND ID

The vlan id for the settings.

MAC Address

Allowed Source MAC address in ARP request packets.

IP Address

Allowed Source IP address in ARP request packets.

Adding new entry

Click to add a new entry to the Static ARP Inspection table. Specify the Port, VLAN ID, MAC address, and IP address for the new entry. Click "Save".

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Authentication Server Configuration

This page allows you to configure the Authentication Servers.

Common Server Configuration

These setting are common for all of the Authentication Servers.

Reliner'			ALL8944WMP - C	Sigabit PoE Switch	0	2
Configuration System Power Reduction Ports Security Switch Network Imit Control NAS ACL	Common Server C Timeout 15 Dead Time 300	erver Configuration configuration seconds seconds ation Server Configurat	tion			
DHCP PSource Guard ARP Inspection AMA Aggregation Loop Protection Spanning Tree MVR IPMC LLDP PoE	1 0 2 0 3 0 4 0 5 0	P Address/Hostname	Port 1812 1812 1812 1812 1812 1812	Secret		
MAC Table VLANs Private VLANs VCL Voice VLAN CoS		P Address/Hostname	Port 1813 1813 1813 1813 1813 ration	Secret		
		P Address/Hostname	Port 49 49 49 49 49 49 49 49 49 49	Secret		

Save Reset

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 won't 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.

RADIUS Authentication Server Configuration

The table has one row for each RADIUS Authentication Server and a number of columns, which are:

#

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 table has one row for each RADIUS Accounting Server and a number of columns, which are:

#

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+ Authentication Server Configuration

The table has one row for each TACACS+ Authentication Server and a number of columns, which are:

#

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.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Aggregation Configuration

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

Runer'												AL	L89	44\	NM	Ρ.	Gig	jab	it P	οE	Swi	tch	į					0	2
Configuration) System) Power Reduction Ports) Security · Aggregation · Static LACP · Loop Protection) Spanning Tree • MV/R	Aggregati Hash Cod Source MAC Destination N IP Address TCP/UDP Po Aggregati	le C Ad MAC	Con Idre: CAc	trib ss Idre: ber	uto ss	rs ▼ ▼																							
▶ IPMC												P	ort	Ме	eml	ber	5												
▶ LLDP	Group ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26		
 PoE MAC Table 	Normal	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲		
VLANs	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	\odot	0	0	\bigcirc	0	0	\bigcirc	0	0	0		
Private VLANs	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
VCL	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
Voice VLAN QoS	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
Mirroring	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
UPnP	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
sFlow	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
lonitor Diagnostics	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
laintenance	9		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
	11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
	12		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	~			
	13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			

Save Reset

Hash Code Contributors

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.

Aggregation Group Configuration

Group ID

Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.

Port Members

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

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Aggregation LACP

This page allows the user to inspect the current LACP port configurations, and possibly change them as well.

							Gigabit PoE Switch	and the second se
juration em	LACP	Port Configurat	tion					
er Reduction	Port	LACP Enabled		Key	Rol	e		
s urity	•		0	-	0	•	1	
regation	1	8	Auto	•	Active			
atic ACP	2		Auto	•	Active			
Protection	3	10	Auto	•	Active			
nning Tree	4		Auto	•	Active	•		
ç	5	8	Auto	•	Active	•		
P	6		Auto	•	Active	•		
Table	7	8	Auto	•	Active			
Ns ate VLANs	8		Auto	•	Active			
	9	8	Auto	•	Active	•		
e VLAN	10		Auto	•	Active			
oring	11	8	Auto	•	Active			
P W	12		Auto	•	Active			
w xr	13	8	Auto		Active			
ostics	14		Auto	•	Active			
nance	15		Auto	•	Active			
	16		Auto	•	Active	•		
	17		Auto		Active			
	18		Auto		Active			
	19	13	Auto		Active			
	20		Auto	•	Active			
	21	8	Auto	•	Active	•	1	
	22		Auto	•	Active	•		
	23	8	Auto	•	Active	•		
	24		Auto	•	Active			
	25	10	Auto	•	Active			
	26		Auto	•	Active			

Port

The switch port number.

LACP Enabled

Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner. LACP can form max 12 LLAGs per switch and 2 GLAGs per stack.

Key

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

Role

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

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

STP Bridge Configuration

This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the Switch.

FRUMET'		ALL8944WMP - Gigabit PoE Switch	1 2
Configuration System Power Reduction Ports Security Aggregation Loop Protection Spanning Tree Bridge Settings MSTI Mapping MSTI Mapping MSTI Prote MVR IPMC LLDP PoE MAC Table VLANs Private VLANs VCL Voice VLAN QOS Mirroring UPnP sFlow Monitor	STP Bridge Configuration Basic Softings Protocol Version Bridge Priority 32768 Forward Delay 15 Max Age 20 Maximum Hop Count 20 Transmit Hold Count 6 Advanced Softings Edge Port BPDU Filtering Edge Port BPDU Filtering Edge Port BPDU Guard Port Error Recovery Port Error Recovery Save Reset		

Basic Settings

Runer'		ALL8944WMP - Gigabit PoE Switch	0 🕑
Configuration System Power Reduction Ports Security Aggregation Loop Protection Spanning Tree Bridge Settings MSTI Mapping MSTI Protection ICST Ports MSTI Protection ILDP PoE MAC Table VLANs VCL VGice VLAN QoS Mirroring UPnP SFlow Monitor	STP Bridge Configuration Basic Settings Protocol Version Bridge Priority RSTP Forward Delay Max Age Maximum Hop Count Transmit Hold Count Edge Port BrDU Filtering Edge Port BrDU Filtering Edge Port BrDU Guard Port Error Recovery Port Error Recovery Save Reset		

Protocol Version

The STP protocol version setting. Valid values are STP, RSTP, and MSTP.

Gerner,		ALL8944WMP - Gigabit PoE Switch	1 🔁 🔁
Configuration System Power Reduction Ports Security Aggregation Loop Protection Spanning Tree MSTI Mapping MSTI Mapping MSTI Profiles MSTI Profile MSTI Ports MMR IPMC LLDP PoE MAC Table VLANs VCL Voice VLAN COS Mirroring UPNP sFlow	Bridge Priority 32 Forward Delay 0 Max Age 81 Maximum Hop Count 12 Transmit Hold Count 20 Advanced Settings 24 Edge Port BPDU Filten 36 Edge Port BPDU Filten 36 Edge Port BPDU Guard 40 Port Error Recovery 16 953	17P • 768 • 96 • 92 • 98 •	
 Monitor 			

Bridge Priority

Controls the bridge priority. Lower numeric values have better 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.

Forward Delay

The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 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 6 to 40 seconds, and MaxAge must be $\leq (FwdDelay-1)^2$.

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.

Advanced Settings

ALLNET'		ALL8944WMP - Gigabit PoE Switch	0
Configuration System Power Reduction Ports Security Aggregation Loop Protection Spanning Tree Bindge Settings MSTI Profiles CIST Ports MSTI Ports MSTI Ports MSTI Ports	STP Bridge Configuration Basic Settings Protocol Version MSTP ▼ Bridge Priority 32768 ▼ Forward Delay 15 Max Age 20 Maximum Hop Count 20 Transmit Hold Count 6		
IPMC ILDP POE MAC Table VLANs Vrivate VLANs Voice VLAN QoS Mirroring UPnP sFlow Monitor Diagnostics Maintenance	Advanced Settings Edge Port BPDU Filtering Edge Port BPDU Guard Port Error Recovery Port Error Recovery Timeout Save Reset		

Edge Port BPDU Filtering

Control whether a port explicitly configured as Edge will transmit and receive BPDUs.

Edge Port BPDU Guard

Control 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

Control whether a port in the *error-disabled* state automatically will 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).

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

STP MSTI Configuration

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

Gunt'	ALL8944WMP - Gigabit PoE Switch	•	2
Configuration System Power Reduction Ports Security Aggregation Loop Protection Spanning Tree Bridge Settings MSTI Priorities CIST Ports	MSTI Configuration Add VLANs separated by spaces or comma. Unmapped VLANs are mapped to the CIST. (The default bridge instance). Configuration Identification Configuration Name 00-01-c1-00-00-00 0		
MSTI Ports MVR MVR IPMC LLDP PoE MAC Table VLANs Private VLANs VCL	MSTI Mapping MSTI MSTI MSTII MSTI2 MSTI3		
Voice VLAN CoS Mirroring UPnP SFlow Monitor	MSTI4 1 MSTI6 1		
	MSTI7		

Configuration Name

The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

Configuration Revision

The revision of the MSTI configuration named above. This must be an integer between 0 and 65535. MSTI Mapping

MSTI

The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

VLANs 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. (I.e. not having any VLANs mapped to it.)

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

STP MSTI Priority Configuration

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

Runn'		ALL8944WMP - Gigabit PoE Switch	🕞 🕑
Configuration System Power Reduction Ports Security Aggregation Loop Protection Spanning Tree Bidge Settings MSTI Mapping MSTI Protes MSTI Ports MSTI Ports MSTI Ports MTI Ports MAC Table	A MSTI Configuration MSTI Priority		
VLANs Private VLANs Vict Voice VLAN Voice VLAN OoS Mirroring UPnP sFlow Monitor	Save Reset		

MSTI

The bridge instance. The CIST is the *default* instance, which is always active.

Priority

Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a *Bridge Identifier*.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

STP CIST Port Configuration

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well.

This page contains settings for physical and aggregated ports.

puner'					ALL8944WMP - Gigabit PoE Switch							
onfiguration	STP CIS	ST Port Co	nfigur	ation								
System Power Reduction			-									
Ports		ggregated Por	t Configu									
 Security Aggregation 	Port	STP Enabled		Path Cost	Priority	Admin Edge	Auto Edge	Restr	TCN	BPDU Guard	Point-to- point	•
 Loop Protection 	-		Auto	•	128 -	Non-Edge 👻					Forced True	•
 Spanning Tree Bridge Settings 												
 MSTI Mapping MSTI Priorities 	CIST N	lormal Port Co	nfiguratic	n –								
CIST Ports MSTI Ports ■	Port	STP		Path Cost	Priority	Admin	Auto	Restricted		BPDU	Point-to-	
MVR	*	Enabled				Edge	Edge	Role	TCN	Guard	<pre>point <></pre>	
► IPMC ► LLDP			<>	-	<> •	<> •						-
• PoE	1		Auto	•	128 -	Non-Edge -					Auto	-
 MAC Table VLANs 	3	V V	Auto Auto	•	128 •	Non-Edge •	V				Auto Auto	•
Private VLANs	4	V	Auto	•	128 -	Non-Edge •	v V				Auto	•
► VCL	5	V V	Auto		128 -	Non-Edge -	V				Auto	•
 Voice VLAN QoS 	6	V	Auto		128 -	Non-Edge -	V				Auto	•
Mirroring	7	V	Auto	- -	128 -	Non-Edge -	V				Auto	•
 UPnP sFlow 	8	V	Auto		128 -	Non-Edge •	v V				Auto	•
Monitor	9		Auto		128 -	Non-Edge -	V				Auto	-
	10		Auto		128 -	Non-Edge -	v				Auto	•
	11	V	Auto		128 -	Non-Edge •					Auto	-
	12		Auto	•	128 -	Non-Edge -					Auto	•
	13	V	Auto	•	128 -	Non-Edge -					Auto	•
	14	V	Auto	•	128 -	Non-Edge -					Auto	-
	15		Auto	•	128 -	Non-Edge -					Auto	-
	16	V	Auto	•	128 -	Non-Edge -	V				Auto	-
	17		Auto	•	128 -	Non-Edge 🔻					Auto	-
	18	V	Auto	•	128 -	Non-Edge 👻					Auto	-
	19		Auto	•	128 -	Non-Edge 👻					Auto	-
	20	V	Auto	•	128 -	Non-Edge 👻	V				Auto	•
	21		Auto	•	128 -	Non-Edge 💌					Auto	•
	22		Auto	•	128 -	Non-Edge 👻	V				Auto	-
	23		Auto	•	128 -	Non-Edge 💌					Auto	•
	24	V	Auto	•	128 -	Non-Edge 👻					Auto	-
	25	V	Auto	•	128 -	Non-Edge 👻					Auto	•
	26	V	Auto	•	128 -	Non-Edge 👻					Auto	•

Save Reset

Port

The switch port number of the logical STP port.

STP Enabled

Controls whether STP is enabled on this switch port.

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 the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in 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. (See above).

operEdge (state flag)

Operational flag describing whether the port is connecting directly to edge devices. (*No* Bridges attached). Transition to the forwarding state is faster for edge ports (having *operEdge true*) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.

Admin Edge

Controls whether the *operEdge* flag should start as set or cleared. (The initial *operEdge* state when a port is initialized).

Auto Edge

Controls whether the bridge should enable automatic edge detection on the bridge port. This allows *operEdge* to be derived from whether BPDU's are received on the port or not.

Restricted Role

If enabled, causes the port not to be selected as 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 influence 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, causes the port not to 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 effect this setting.

A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

Point2Point

Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Spanning Tree / MSTI Ports

STP MSTI Port Configuration

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well.

FRUMET		ALL8944WMP - Gigabit PoE Switch	1 🕄 🕄
Configuration System Power Reduction Ports Security Aggregation Loop Protection Spanning Tree Bridge Settings MSTI Profiles MSTI Profiles MSTI Profile MVR ILDP PoE MAC Table VLANs Private VLANs VCL Voice VLAN QOS Mirroring UPnP SFlow Monitor Manitor	MSTI Port Configuration Select MSTI MSTI Cet		

An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

This page contains MSTI port settings for physical and aggregated ports.

Port

The switch port number of the corresponding STP CIST (and MSTI) port.



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 the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in 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. (See above).

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Configuration /MVR

This page provides MVR related configurations.

- BLAET	ALL8944WMP - Gigabit PoE Switch	1 2))
- Configuration		State State	
 Configuration System 	MVR Configurations		
Power Reduction	MVR Mode Disabled -		
Ports	WYR MODE Disabled *		
 Security Aggregation 			
Loop Protection	VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])		
 Spanning Tree 			1
MVR IPMC	Delete MVR VID MVR Name Mode Tagging Priority LLQI Interface Channel Setting		
LLDP			
• PoE	Add New MVR VLAN		
 MAC Table 			
VLANs			
 Private VLANs VCL 	Immediate Leave Setting		
Voice VLAN	Port Immediate Leave		
> QoS	1 Disabled -		
Mirroring	2 Disabled -		
UPnP sFlow	3 Disabled •		
Monitor	4 Disabled -		
Diagnostics	5 Disabled *		
Maintenance	6 Disabled •		
	7 Disabled -		
			Ŧ
	10 Disabled •		
	11 Disabled •		
	12 Disabled •		
	13 Disabled •		
	14 Disabled •		
	15 Disabled •		
	16 Disabled •		
	17 Disabled -		
	18 Disabled •		
	19 Disabled -		
	20 Disabled -		
	21 Disabled -		
	22 Disabled -		
	23 Disabled •		
	24 Disabled •		
	25 Disabled -		
	26 Disabled -		

Course Course

The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP join message to Switch A to join the appropriate multicast. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

MVR Mode

Enable/Disable the Global MVR.

VLAN ID

Specify the Multicast VLAN ID.

Mode

Enable MVR on the port.

Туре

Specify the MVR port type on the port.

Immediate Leave

Enable the fast leave on the port.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

IGMP Snooping Configuration

This page provides IGMP Snooping related configuration.



Snooping Enabled

Enable the Global IGMP Snooping.

Unregistered IPMCv4 Flooding enabled

Enable unregistered IPMCv4 traffic flooding.

SSM Range

SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

Leave Proxy Enabled

Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled

Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Router Port

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

If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave

Enable the fast leave on the port.

Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD

Throttling

Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

IGMP Snooping VLAN Configuration

Navigating the IGMP Snooping VLAN Table

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table starting from that or the next closest VLAN Table match. The will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is

reached the text "No more entries" is shown in the displayed table. Use the button to start over.

-			AL	L8944WMP - Gigab	it PoE Switch		C	2
Configuration System Power Reduction Ports Security	GMP Snoopin	-	-	page.			Refresh	~ >>
Aggregation Loop Protection	VLAN ID	Snooping Enabled	IGMP Querier	Compatibility	RV QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
Spanning Tree MVR MVR IOMP Snooping IOMP Snooping Orniguration Out An Configuration Port Group Fittering MLD Snooping MLD Snooping MLD Snooping MLC Snooping MAC Table VLANs Private VLANs VCL VCLANs VCL VCaN Qos Mirroring M	1 Save Reset		8]	-		-

IGMP Snooping VLAN Table Columns

VLAN ID

The VLAN ID of the entry.

IGMP Snooping Enabled

Enable the per-VLAN IGMP Snooping. Only up to 64 VLANs can be selected.

IGMP Querier

Enable the IGMP Querier in the 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**, **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.

Buttons

Refresh : Refreshes the displayed table starting from the "VLAN" input fields.

<< : Updates the table starting from the first entry in the VALN Table, i.e. the entry with the lowest VLAND ID.</p>
>: Update the table, staring with the entry after the last entry currently displayed.

IGMP Snooping / Port Group Filtering

IGMP Snooping Port Group Filtering Configuration



Delete

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

Port

The logical port for the settings.

Filtering Groups

The IP Multicast Group that will be filtered.

Adding New Filtering Group

Click to add a new entry to the Group Filtering table. Specify the Port, and Filtering Group of the new entry. Click "Save".

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

MLD Snooping Configuration

This page provides MLD Snooping related configuration.

			ALL8944WMP - Gi	gabit PoE Switch
MLD Sn	ooping Co	nfiguration	1	
			Global Configuration	
Snooping	Enabled		0	
Unregister	red IPMCv6 F	looding Enab	led 🗵	
MLD SSM	Range		ff3e::	/ 96
Leave Pro	xy Enabled			
Proxy Ena	abled		8	
Port Rel	ated Confi	guration		
Port R	Router Port	Fast Leav	e Throttling	
			· ·	
1			unlimited -	
2			unlimited ·	
3			unlimited -	
4			unlimited -	
5		E	unlimited -	
6			unlimited -	
7		10	unlimited ·	
8			unlimited ·	
9			unlimited -	
10			unlimited +	
11			unlimited ·	
12			unlimited -	
13			unlimited -	
14			unlimited •	
15			unlimited -	
16			unlimited •	
17			unlimited ·	
18			unlimited •	
19			unlimited -	
20			unlimited -	
21			unlimited +	
22			unlimited •	
23			unlimited ·	
24			unlimited -	
25	8		unlimited •	
26		1	unlimited -	

Snooping Enabled

Enable the Global MLD Snooping.

Unregistered IPMCv6 Flooding enabled

Enable unregistered IPMCv6 traffic flooding. Please note that disabling unregistered IPMCv6 traffic flooding may lead to failure of Neighbor Discovery.

SSM Range

SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

Leave Proxy Enabled

Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled

Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Router Port

Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.

If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave

Enable the fast leave on the port.

Throttling

Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

MLD Snooping VLAN Configuration

Navigating the MLD Snooping VLAN Table

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table starting from that or the next closest VLAN Table match. The will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

MLD Snooping VLAN Table Columns

Rewer'			AL	L8944WMP - Gigat	bit PoE	Switch		0	2
Configuration System Power Reduction Ports	MLD Snoop Start from VLA	ing VLAN Config N 1 with 20		page.				Refresh	<< >>
Security Aggregation Loop Protection	VLAN ID	Snooping Enabled	MLD Querier	Compatibility	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
Spanning Tree MVR MVR IPMC IGMP Snooping MLD Snooping MLD Snooping WLAN Canfiguration VLAN Canfiguration Port Group Fitating LLDP PoE MAC Table VLANs VOLAN Voice VLANs VOLA Voice VLAN GoS Mirroring	Save Rei	et	¥.	- *	-			-	

VLAN ID

The VLAN ID of the entry.

MLD Snooping Enabled

Enable the per-VLAN MLD Snooping. Only up to 64 VLANs can be selected.

MLD Querier

Enable the IGMP Querier in the 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, ForcedMLDv1, Forced MLDv2, default compatibility value is MLD-Auto.

RV

Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a link. The allowed range is **1** to **255**, default robustness variable value is **2**.

QI

Query Interval. The Query Interval variable denotes 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 Maximum Response Delay used to calculate the Maximum Response 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

Last Listener Query Interval. The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages. The allowed range is **0** to **31744** in tenths of seconds, default last listener 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 node's initial report of interest in a multicast address. The allowed range is **0** to **31744** seconds, default unsolicited report interval is 1 second.

Buttons

Refresh: Refreshes the displayed table starting from the "VLAN" input fields.

<< : Updates the table starting from the first entry in the VALN Table, i.e. the entry with the lowest VLAND ID.</p>
>: Update the table, staring with the entry after the last entry currently displayed.

IPMC / MLD Snooping / Port Group Filtering

MLD Snooping Port Group Filtering Configuration



Delete

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

Port

The logical port for the settings.

Filtering Groups

The IP Multicast Group that will be filtered.

Adding New Filtering Group

Click to add a new entry to the Group Filtering table. Specify the Port and Filtering Group for the new entry. Click "Save".

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

LLDP Parameters

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

			ALL	8944WMP - G	igabit PoE Sw	ritch		
			PoE	GigaBit	Ethernet	Switch		0
LLDP (Configuratio	n						
duction LLDP P	arameters							
011	rval 30	seconds						
tion Tx Hok		times						
Tx Dela	-	seconds						
Tx Rein	iit 2	seconds						
LLDP P	ort Configura	ition						
					Optional TLV:			
Port	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr	
	• •	8	R	1	9	2	2	
1	Enabled •		10	x	X	×.	10	
2	Enabled •		12	2	10 N	2	12	
3	Enabled ·	8	×		8	2	1	
4	Enabled +		R	2	8	2	12	
5	Enabled ·	8	R	2	8	2	R	
6	Enabled + Enabled +	8	12	X.	8	Z Z	121 121	
8	Enabled •	0	N N	12	8	2	R	
9	Enabled •		10	2	8	2	10	
10	Enabled +		N.	X	N N	2	N.	
11	Enabled ×	8	2				8	
12	Enabled •		R	X	10	Z	N.	
13	Enabled +	8	10	x	10	2	10	
14	Enabled -		10	X	12	X	12	
15	Enabled +	8	10	2	10	2	10	
16	Enabled 💌		×	1	8	2	R	
17	Enabled +		10	x	X	×.	10	
18	Enabled -	8	2	2		2	8	
19	Enabled -		12	z	×	z	12	
20	Enabled •		R	2		2	R	
21	Enabled ·		10	2	R	Z	R.	
22	Enabled -	8	N.	22	52	2	10	
23	Enabled • Enabled •	8	2	2	2	2	2	
24	Enabled +	8	8	(X)	8	2	×	
40	-190 M -		10 10	2	×	2	10	

Tx Interval

The switch periodically transmits LLDP frames to its neighbours for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the **Tx Interval** value. Valid values are restricted to 5 - 32768 seconds.

Tx Hold

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

If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of **Tx Delay** seconds. **Tx Delay** cannot be larger than 1/4 of the **Tx Interval** value. Valid values are restricted to 1 - 8192 seconds.

Tx Reinit

When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring 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.

LLDP Port Configuration

Port

The switch port number of the logical LLDP http://192.168.1.6/help/glossary.htm - lldpport.

Mode

Select LLDP mode.

Rx only The switch will not send out LLDP information, but LLDP information from neighbour units is analyzed.

Tx only The switch will drop LLDP information received from neighbours, but will send out LLDP information.

Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbours.

Enabled The switch will send out LLDP information, and will analyze LLDP information received from neighbours.

CDP Aware

Select CDP awareness.

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.). CDPTLVs are mapped onto LLDP neighbours' table as shown below. CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field. CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbours table. CDP TLV "Port ID" is mapped to the LLDP "Port ID" field. CDP TLV "Port ID" is mapped to the LLDP "Port ID" field. CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field. 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 on a port is disabled the CDP information isn't removed immediately, but gets

removed when the hold time is exceeded.

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.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

LLDP Media Configuration

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

ALINET'		ALL8944WMP - Gigabit PoE Switch	i	1
Configuration System Power Reduction Ports Security Aggregation Soanning Tree MVR PMC LLDP LLDP LLDP	LLDP-MED Configuration Fast Start Repeat Count Fast start repeat count Coordinates Location Lathude Civic Address Location	.ongitude	Mittude	- Map Deturn
PoE PAE PAE PAE PAE PAUE VLANs Private VLANs VCL Vaice VLAN Voice VLAN Voice VLAN Oos Mirroring UPAP SFlow Monitor Monitor Monitor Maintenance	Country code City Street Street suffix Landmark Zip code Floor Postal community	State City district Leading street direction House no. Additional location info Building Room no. P.O. Box	County Block (Neighbourhood) Trailing street suffix Nouse no. suffix Name Apartment Place type Additional code	
		e Tag VLAN ID L2 Priority DSC ies present	P	

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 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 would 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.

Coordinates Location

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 the 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).

Meters: Representing meters of Altitude defined by the vertical datum specified.

Floors: 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:

WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, 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.

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

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, perish, gun (Japan), district.

City

City, township, shi (Japan) - Example: Copenhagen.

City district

City division, borough, city district, ward, chou (Japan)

Block (Neighbourhood)

Neighbourhood block

Street

Street - Example : Poppelvej

Leading Street Direction

Leading street direction - Example: N

Trailing street suffix

Trailing street suffix - Example: SW

Street suffix

Street suffix - Example : Ave, Platz

House no.

House number - Example: 21

House no. suffix

House number suffix - Example: A, 1/2

Landmark

Landmark or vanity address - Example : Columbia University.

Additional location info.

Additional location info - Example : South Wing.

Name

Name (residence and office occupant) - Example : Flemming Jahn.

Zip code

Postal /zip code - Example: 2791

Building

Building (structure) – Example : Low Library.

Apartment

Unit (Apartment, suite) - Example: Apt 42.

Floor

Floor – Example: 4

Room No.

Room number - Example: 450F.

Place type

Place type - Example: Office.

Postal community name

Postal community name - Example: Leonia.

P.O. Box

Post office box (P.O. Box) Example : 12345.

Additional code

Additional code - Example: 1320300003.

Emergency Call Service

Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

Emergency Call Service

Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Report'			ALL8944WI	MP - Gigabit PoE Swite	:h	0	2
Configuration System Power Reduction Ports Security Aggregation Loop Protection Spanning Tree MVR IPMC LLDP	LLDP-MED Con Fast Start Repeat Fast start repeat Coordinates Loc Latitude	t Count	ongitude _o		Altitude		Map Datum
LLDP LLDP.MED PoE MAC Table VLANs VCLNs VCL Voice VLANs Voice VLAN OoS Mirroring UPnP sFlow	Civic Address Lo Country code City Street Street suffix	cation	State City district Leading street direction House no. Additional		County Block (Neighbourhood) Trailing street suffix House no. suffix	-	
Monitor Diagnostics Maintenance	Landmark Zip code Floor		location info Building Room no.		Apartment Place type		=
	* Postal community name		P.O. Box		Additional code		5
¢	Emergency Call S Emergency Call S Policies Delete Policy Add New Policy Save Reset	Service	Tag VLAN	ID L2 Priority DS	CP		

Policies

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such 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:

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. Soft phone Voice
- 4. Video Conferencing
- 5. Streaming Veido
- 6. Control / Singalling (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

Check to delete the policy. It will be deleted during the next save.

Policy ID

ID for the policy. This is auto generated and shall be used when selecting the polices 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.

Adding a 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 Policies Configuration

Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.

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 check marking the checkboxes that corresponds to the policies.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

ΡοΕ

PoE (Power over Ethernet) Configuration

PoE technology is a system to pass electrical power safely, along with data, on Ethernet cabling. Power is supplied in common mode over two or more of the differential pairs of sires found in the Ethernet cables and comes from a power supply within a PoE enabled networking devise such as Switch or can be injected into a cable run with a midspan power supply.

This figure shows all the PoE 's status when connect or disconnect to the PD devise.

- > PoE Enabled: POE of the port is able to supply power to the attached PD (Powered Device)
- > PD Class: Detect the class of PD
- > Delivering Power (W): Output power.
- > Current (mA): The status of the port current
- Power output voltage per port
- > Power Budget Percentage of PoE power has been use

					ALL8944WMP - Gigabit PoE Switch	1
Powe	r Over Et	heri	net Co	onfig	uration	
_	ved Power			-		
				aby	Class Allocation LLDP-MED	
Powe	r Managem	ent	моде		Actual Consumption * Reserved Power	
PoE P	ower Supp	ply (Config	urati	on	
Prim	ary Power	Sur	nnly IV	va I		
	aly rower	oup	200			
		_				
PoE P	ort Config	urat	tion			
Port	PoE Mo	de	Prior	ritv	Maximum Power [W]	
	0	•	0		15.4	
1	PoE+	•	Low		15.4	
2	PoE+	-	Low	•	15.4	
3	PoE+	•	Low		15.4	
4	PoE+		Low		15.4	
5	PoE+	•	Low	•	16.4	
6	PoE+		Low		15.4	
7	PoE+		Low		16.4	
8	PoE+		Low		15.4	
9	PoE+		Low		15.4	
10	PoE+	•	Low		15.4	
11	PoE+	•	Low		15.4	
12	PoE+	•	Low	*	15.4	
13	PoE+	•	Low		15.4	
14	PoE+	•	Low	-	15.4	
15	PoE+	×	Low	*	15.4	
16	PoE+	•	Low	•	15.4	
17	PoE+	•	Low	-	15.4	
18	PoE+	-	Low	•	15.4	
19	PoE+	•	Low	-	15.4	
20	PoE+		Low		15.4	
21	PoE+	•	Low	•	16.4	
22	PoE+		Low		15.4	
23	PoE+	•	Low	•	15.4	
24	PoE+		Low	w.	15.4	

Save Reset

Port Configuration

Port

This is the logical port number for this row.

Ports that are not PoE-capable are grayed out and thus impossible to configure PoE for.

PoE Mode

The **PoE Mode** represents the PoE operating mode for the port.

Disabled: PoE disabled for the port.

PoE : Enables PoE IEEE 802.3af (Class 4 PDs limited to 15.4W)

PoE+ : Enables PoE+ IEEE 802.3at (Class 4 PDs limited to 30W)

Priority

The **Priority** represents the ports priority. There are three levels of power priority named Low, High and Critical.

The priority is used in the case where the remote devices requires more power than the power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.

Maximum Power

The **Maximum Power** value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device.

The maximum allowed value is 30 W.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

MAC Address Table Configuration

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.

Report											1	ALI	.894	4W	MP	- G	igal	bit	PoE	SV	vitc	i							C	₽	6	2	
Configuration System Power Reduction Ports Security Aggregation Loop Protection Spanning Tree MVR Verte	MAC A Aging C Disable Aging 1 MAC Ta	Conf e Aut Time	igur toma	atio	n Agin	gE		ura			onds																						
IPMC LLDP										-	Por	t N	/lem	be	rs	-		-				_		-	_								
PoE		1	2 3	4	6	6 1	7 8	8 9	10	1			3 14			17	18	19	20	21	22	23	24	25	26								
MAC Table	Auto															٠	۰					٠		٠									
VLANs	Disable	0.0	0.0	0	0	0.0	5.6	0.0	0		0 0	e	0	0	0	0	0	0	0	0	0	0	0	0	0								
 Private VLANs VCL 	Secure	0.0	0 0	0	0	0.0	5 6	0 0	0	0	0 0	0	0	0	0	0	0	0	0	0	0	0	0	0	0								
Voice VLAN QoS	Static M	IAC	Tab	ole C	ont	ligur	atic	on																									
Mirroring UPnP																			/len			_											
• sFlow	Delete	V	LAN	ID	M	AC /	٨dd	ires	S 1	2	34	5 6	78	9 1	0 11	12	13	14	15 1	6 1	7 18	19	20	21 2	22 23	24	25 20	6					
Monitor Diagnostics	Add Ne	w St	tatic	Entr	y																												
Maintenance	Save	R	eset																														

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; for example, **Age time** seconds.

Disable the automatic aging of dynamic entries by checking \Box 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. Each port can do learning based upon the following settings:

Auto

Learning is done automatically as soon as a frame with unknown SMAC is received.

Disable

No learning is done.

Secure

Only static MAC entries are learned, all other frames are dropped.

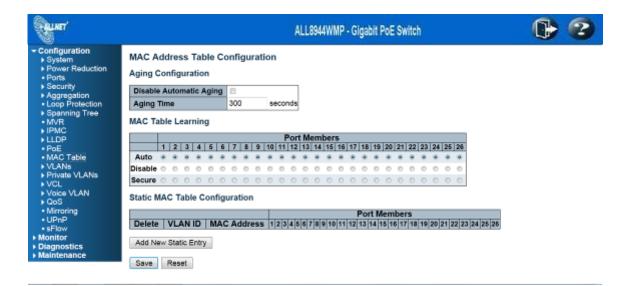
Note: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

Report'	ALL8944WMP - Gigabit PoE Switch	1
Configuration System Power Reduction Ports Security Aggregation Loop Protection Spanning Tree	MAC Address Table Configuration Aging Configuration Disable Automatic Aging Aging Time 300 seconds	
• MVR • IPMC • LLDP • PoE • MAC Table • VLANs • Private VLANs	MAC Table Learning	
VCL Voice VLAN OoS Mirroring UPnP sFlow Monitor Diagnostics Maintenance	Port Members Delete VLAN ID MAC Address 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 Add New Static Entry Save Reset	

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.

Adding a New Static Entry

Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

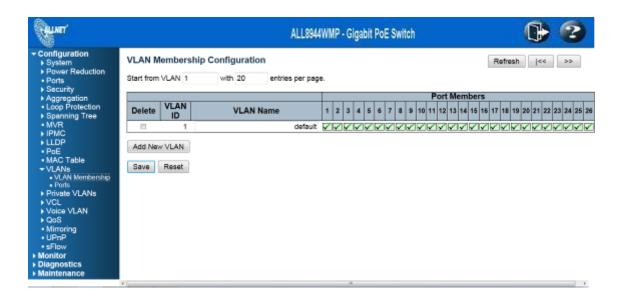
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

VLAN Membership Configuration

The VLAN membership configuration for theswitch can be monitored and modified here. Up to 4096 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.



Navigating the VLAN Table

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table starting from that or the closest next VLAN Table match. The will use the last entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

Delete

To delete a VLAN entry, check this box. The entry will be deleted during the next Save.

VLAN ID

Indicates the ID of this particular VLAN.

VLAN Name

Indicates the name of the VLAN. Maximum length of the VLAN Name String is 32. VLAN Name can only contain alphabets or numbers. VLAN name should contain atleast one alphabet. VLAN name can be edited for the existing VLAN entries or it can be added to the new entries.

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 as \checkmark .

To include a port in a forbidden port list, check the box as shown \bowtie .

To remove or exclude the port from the VLAN, make sure the box is unchecked as shown

By default, no ports are members, and for every new VLAN entry all boxes are unchecked.

Gauner'	ALL8944WMP - Gigabit PoE Switch	1 🕑 😨
Configuration System Power Reduction Ports Sacurity Aggregation Loop Protection Spanning Tree MVR IPMC LLDP PoE MAC Table VLANs VLAN Membership Ports Ports VLANs VCL VCL VCAN QoS	VLAN Membership Configuration Start from VLAN 1 with 20 entries per page. Provide the start from VLAN 1 with 20 entries per page. Provide the start from VLAN 1 with 20 entries per page.	Refresh <<
Mirroring UPnP SFlow Monitor Diagnostics Maintenance		

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.

The VLAN is enabled when you click on "Save". A VLAN without any port members will be deleted when you click "Save".

The button can be used to undo the addition of new VLANs.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Refreshes : Refreshes the displayed the table starting from the "VLAND ID" input fields.

<< : Updates the table starting from the first entry in the VALN Table, i.e. the entry with the lowest VLAND ID.

>>: Update the table, staring with the entry after the last entry currently displayed.

VLAN Port Configuration

This page is used for configuring the switch port VLAN.

ET'				ALL89	44WMP	- Gigabit PoE	Switch		
guration tem	Ethert	ype for Custor	n S-ports 0x 88A8					Auto-refres	sh 🗆 Refres
ver Reduction		Port Configura	ation						
ts :urity		Fort Configura							_
regation	Port	Port Type	Ingress Filtering	Frame	e Type	Port VL	.AN ID	Tx Tag	
p Protection	*		<u> </u>			Mode			1
ning Tree		<> •		<>	-	↔ •	1		
	1	Unaware -		All	•	Specific -	1	Untag_pvid -	
	2	Unaware -		All	-	Specific -	1	Untag_pvid -	
	3	Unaware -		All	-	Specific -	1	Untag_pvid -	
Table	4	Unaware -	—	All	-	Specific 💌	1	Untag_pvid -	
Ns AN Membership	5	Unaware -		All	-	Specific -	1	Untag_pvid -	1
orts	6	Unaware -		All	•	Specific -	1	Untag pvid -	
ate VLANs	7	Unaware -		All	-	Specific -	1	Untag pvid -	i
∋ VLAN	8	Unaware -		All	•	Specific -	1	Untag pvid -	
VLAN	9	Unaware -		All	-	Specific -	. 1	Untag_pvid -	
oring	10	Unaware -		All	-	Specific -	1	Untag_pvid -	
						· ·			
v r	11	Unaware -		All	-	Specific -	1	Untag_pvid -	
tics	12	Unaware -		All	-	Specific -	1	Untag_pvid -	
ance	13	Unaware -		All	-	Specific -	1	Untag_pvid -	
inarroo	14	Unaware -	[]	All	-	Specific 💌	1	Untag_pvid -	
	15	Unaware -		All		Specific 💌	1	Untag_pvid 🔹	
	16	Unaware -	[]	All	-	Specific -	1	Untag_pvid -	1
	17	Unaware -		All	-	Specific -	1	Untag_pvid -	
	18	Unaware -		All	-	Specific -	1	Untag pvid -	
	19	Unaware -		All	-	Specific -	1	Untag pvid -	
	20	Unaware -		All	-	Specific •	. 1	Untag pvid -	
	20	Unaware -		All	-	Specific -	1	Untag pvid -	
						·			
	22			All	-	Specific -	1	Untag_pvid -	
	23	Unaware -		All	-	Specific -	1	Untag_pvid -	
	24	Unaware -		All	-	Specific 💌	1	Untag_pvid -	
	25	Unaware -		All	-	Specific -	1	Untag_pvid -	
	26	Unaware -		All	-	Specific -	1	Untag_pvid -	

Save Reset

Ether type 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.

Port

This is the logical port number of this row.

Port Type

Port can be one of the following types: Unaware, Customer port(C-port), Service port(S-port), Custom Service port(S-custom-port)

If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed.

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 (no checkmark).

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**.

Port VLAN Mode

Configures the Port VLAN Mode. The allowed values are **None** or **Specific** This parameter affects VLAN ingress and egress processing.

If **None** is selected, a VLAN tag with the classified VLAN ID is inserted in frames transmitted on the port. This mode is normally used for ports connected to VLAN aware switches.

If **Specific** (the default value) is selected, a Port VLAN ID can be configured (see below). Untagged frames received on the port are classified to the Port VLAN ID. If VLAN awareness is disabled, all frames received on the port are classified to the Port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the Port VLAN ID, a VLAN tag with the classified VLAN ID is inserted in the frame.

Port VLAN ID

Configures the VLAN identifier for the port. The allowed values are 1 through 4095. The default value is 1. Note: The port must be a member of the same VLAN as the Port VLAN ID.

Tx Tag

Determines egress tagging of a port. Untag_pvid - All VLANs except the configured PVID will be tagged. Tag_all - All VLANs are tagged. Untag_all - All VLANs are untagged.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Private VLANs Private VLAN Membership Configuration

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs 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.

Configuration

System

Power Reduction

Power Reduction

Power Reduction

Configuration

Power Reduction

Power Reduction

Loop Protection

Spanning Tree

MWR

LOP

Poil

Mirroring

UPAR

Private VLAN

Mirroring

UPAR

Private VLAN

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

Delete

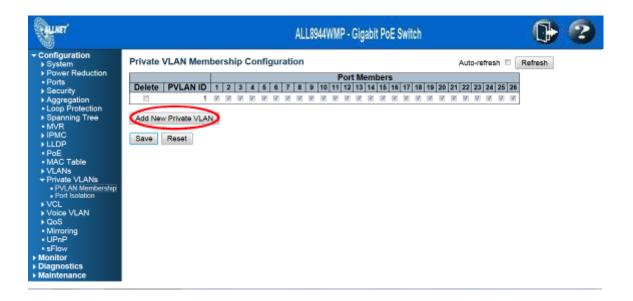
To delete a private VLAN entry, check this box. The entry will be deleted during the next save.

Private VLAN ID

Indicates the ID of this particular private VLAN.

Port Members

A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.



Adding a New Private VLAN

Click to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction.

The Private VLAN is enabled when you click "Save".

The button can be used to undo the addition of new Private VLANs.

Buttons

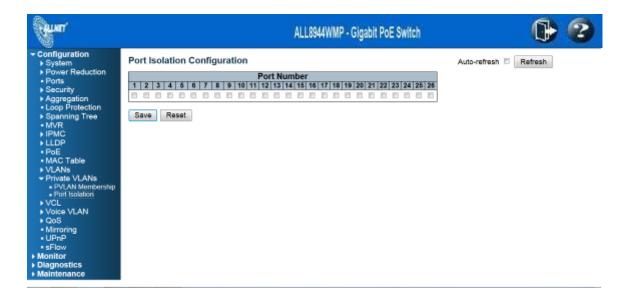
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Port Isolation Configuration

Overview

This page is used for enabling or disabling port isolation on ports in a Private VLAN.



A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

Configuration

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.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

VCL MAC-Based VLAN Configuration

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

RELART'	ALL8944WMP - Gigabit PoE Switch	1 2
Configuration System Power Reduction Ports Security Aggregation Loop Protection Spanning Tree MVR IPMC LLDP PoE MAC Table VLANs VCL MAC Table VLANs VCL MAC Table VLANs VCL MAC based VLAN Protocol-based VLAN VCL VLAN VCice VLAN OoS Mirroring UPnP sFlow Monitor VCL	MAC-based VLAN Membership Configuration Auto-refresh Refresh Port Members Delete MAC Address VLAN ID 123345667189191011121313141156161718119202112223242526 Currendy no entries present Currendy no entries present Add New Entry Save Reset	<u>k</u> « >>

Delete

To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted in the stack.

MAC Address

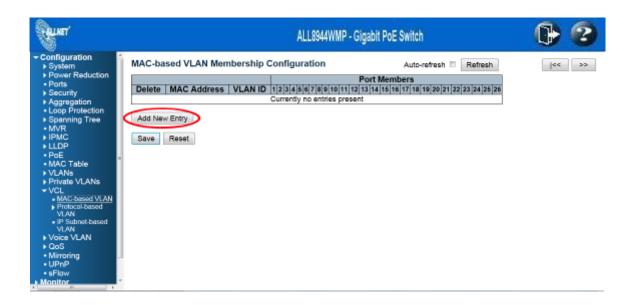
Indicates the MAC address.

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.



Adding a New MAC-based VLAN

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 when you click on "Save". A MAC-based VLAN without any port members will be deleted when you click "Save".

The button can be used to undo the addition of new MAC-based VLANs.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Refreshes : Refreshes the displayed the table starting from the "VLAND ID" input fields.

<< : Updates the table starting from the first entry in the VALN Table, i.e. the entry with the lowest VLAND ID.</p>
>: Update the table, staring with the entry after the last entry currently displayed.

Protocol to Group Mapping Table

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 switch .

The displayed settings are:

Runn'	ALL8944WMP - Gigab	oit PoE Switch 🚯 😰
Configuration System Power Reduction Ports Security Aggregation Loop Protection Spanning Tree MVR IPMC LLDP PoE MAC Table VLAN Protocol based VLAN Protocol b	Protocol to Group Mapping Table Delete Frame Type Value Group Name No Group entry found! Add New Entry Save Reset	Auto-refresh 🗖 Refresh

Delete

To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.

Frame Type

Frame Type can have one of the following values:

- 1. Ethernet
- 2. LLC
- 3. **SNAP**

Note: On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you selected.

Value

Valid value that can be entered in this text field depends on the option selected from the the preceding Frame

Type selection menu.

Below is the criteria for three different Frame Types:

- For Ethernet: Values in the text field when Ethernet is selected as a Frame Type is called etype.
 Valid values for etype ranges from 0x0600-0xffff
- 2. For LLC: 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)
- 3. For SNAP: 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

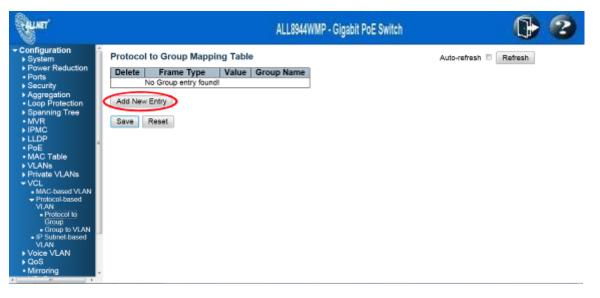
pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.

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).

Note: special character and underscore(_) are not allowed.



Adding a New Group to VLAN mapping entry

Click to add a new entry in mapping table. An empty row is added to the table; Frame Type, Value and the

Group Name can be configured as needed.

The button can be used to undo the addition of new entry.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

VCL / Protocol-based VLAN / Protocol to Group

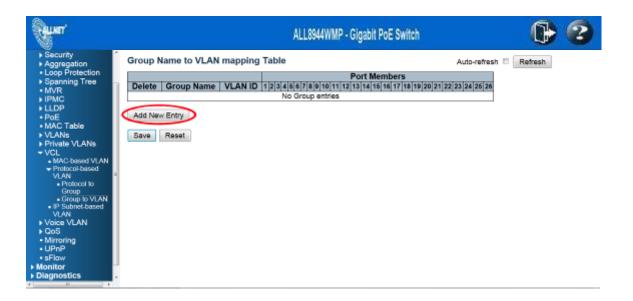
Runer'	ALL8944WMP - Gigabi	it PoE Switch	3
Security Aggregation Loop Protection Spanning Tree M/R IPMC LLDP PoE MAC Table VLANs VCL MAC-tased VLAN Vrotocol to Group Group to VLAN Voice VLAN Voice VLAN Voice VLAN Voice VLAN OoS Mirrering UPnP sFlaw Monitor Diagnostics	Group Name to VLAN mapping Table Port N Delete Group Name VLAN ID 1/2/3/4/5/6/7/8/9/10/11/12/13/14/1 No Group entries Add New Entry Save Reset	Auto-refresh 🗖 Refresh Members 15 16 17 18 19 20 21 22 23 24 26 26	

VCL / Protocol-based VLAN / Group to VLAN

Group Name to VLAN mapping Table

This page allows you to map a already configured Group Name to a VLAN for the switch .

The displayed settings are:



Delete

To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next Save

Group Name

A valid Group Name is a string of atmost 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers(0-9), no special character is allowed. whichever Group name you try map to a VLAN must be present in Protocol to Group mapping table and must not be preused by any other existing mapping entry on this page.

VLAD ID

Indicates the ID to which 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.

Adding a New Group to VLAN mapping entry

Click to add a new entry in mapping table. An empty row is added to the table, the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are **1** through **4095**.

The button can be used to undo the addition of new entry.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Voice VLAN Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAND ID correctly. It should be configured through its own GUI.

Runt'	ALL8944WMP - Gigabit PoE Switch	1
 Configuration System 	Voice VLAN Configuration	
Power Reduction	Mode Disabled -	
 Ports Security 	VLAN ID 1000	
 Aggregation 	Aging Time 86400 seconds	
Loop Protection	Traffic Class 7 (High)	
 Spanning Tree MVR 		
▶ IPMC		
► LLDP	Port Configuration	
 PoE MAC Table 	Port Mode Security Discovery Protocol	
▶ VLANs		
 Private VLANs VCL 	1 Disabled - Disabled - OUI	
VOL Voice VLAN	2 Disabled Disabled OUI	
Configuration	3 Disabled - Disabled - OUI -	
■ OUI ▶ QoS	4 Disabled Disabled OUI	
 Mirroring 	5 Disabled - Disabled - OUI	
• UPnP	6 Disabled - Disabled - OUI	
 sFlow Monitor 	7 Disabled - Disabled - OUI -	
Diagnostics	8 Disabled - Disabled - OUI -	
Maintenance	9 Disabled Disabled OUI	
	10 Disabled - Disabled - OUI -	
	11 Disabled - Disabled - OUI -	
	12 Disabled - Disabled - OUI	
	13 Disabled - Disabled - OUI -	
	14 Disabled Disabled OUI	
	15 Disabled Disabled OUI	
	16 Disabled - Disabled - OUI	
	17 Disabled Disabled OUI	
	18 Disabled Disabled OUI	
	19 Disabled - Disabled - OUI -	
	20 Disabled Disabled OUI	
	21 Disabled - Disabled - OUI -	
	22 Disabled Disabled OUI	
	23 Disabled Disabled OUI	
	24 Disabled Disabled OUI	
	25 Disabled Disabled OUI	
	26 Disabled Disabled OUI	

Save Reset

Mode

Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are:

Enabled: Enable Voice VLAN mode operation.

Disabled: Disable Voice VLAN mode operation.

VLAN ID

Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.

Aging Time

Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 1000000 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 Mode

Indicates the Voice VLAN port mode.

Possible port modes are:

Disabled: Disjoin from Voice VLAN.

Auto: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and

configures the Voice VLAN members automatically.

Forced: Force join to Voice VLAN.

Port Security

Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC

addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are:

Enabled: Enable Voice VLAN security mode operation.

Disabled: Disable Voice VLAN security mode operation.

Port 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.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Voice VLAN OUI Configuration

Configure VOICE VLAN OUI table on this page. The maximum entry number is **16**. Modifying the OUI table will restart auto detection of OUI process.

Rever'			ALL8944W
 Configuration System 	Voice VI	AN OUI Table	
 Power Reduction Ports 	Delete	Telephony OUI	Description
 Security 	13	00-01-e3	Siemens AG phones
Aggregation		00-03-6b	Cisco phones
Loop Protection	10	00-0f-e2	H3C phones
 Spanning Tree MVR 		00-60-b9	Philips and NEC AG phones
▶ IPMC	10	00-d0-1e	Pingtel phones
► LLDP • PoE		00-e0-75	Polycom phones
• MAC Table	8	00-e0-bb	3Com phones
VLANs			
Private VLANs	Add Nev	Entry	
VCL Voice VLAN	Save	Reset	
 Configuration 	oave	reser	
• OUI • QoS			
Mirroring			
• UPnP			
 sFlow 			
Monitor Diagnostics			
Maintenance			

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 by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a 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.

LNET					
figuration ystem	Voice V	LAN OUI Table			
ower Reduction	Delete	Telephony OUI	Description		
ecurity	8	00-01-e3	Siemens AG phones		
ggregation		00-03-6b	Cisco phones		
oop Protection		00-0f-e2	H3C phones		
panning Tree IVR		00-60-b9	Philips and NEC AG phones		
MC		00-d0-1e	Pingtel phones		
LDP		00-e0-75	Polycom phones		
οE	8	00-e0-bb	3Com phones		
IAC Table					
rivate VLANs	Add Ne	w Entry			
CL					
oice VLAN	Save	Reset			
Configuration					
oS					
lirroring					
PnP					
WOW					
nitor					

Buttons

Add new entry: Click to add a new access management entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

QoS/ Port Classification

QoS Ingress Port Classification

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

The displayed settings are:

WET'						ALL8944WMP	- Gigabit PoE Switch	•	
iguration	QoS Ir	aress Port	Classific	ation					
wer Reduction		QoS class		PCP	DEI	Tag Class.	DSCP Based		
rts	FOIL	Class .	<> ·	0.	O .	Tag Glass.	DOCF Dased		
curity gregation	1	0 -	0 -	0 -	0 +	Disabled	10		
op Protection	2		0 *	0 -	0 -	Disabled	E.		
anning Tree	3	0 -	0 -	0 -	0 -	Disabled	E.		
R	4	0 -	0 -	0 -	0 -	Disabled			
P 1		0 -	0 -	0 -	0 +		D		
and the second s	6		L-T-ADDER	ALC: NO DE		Disabled			
C Table	6	0 -	0 +	0 -	0 +	Disabled	63		
Ns ate VLANs	7	0 -	0 *	0 -	0 *	Disabled	E0		
	8	0 -	0 +	0 -	0 -	Disabled	13		
se VLAN	9	0 -	0 🔹	0 -	0 +	Disabled	Ð		
ort Classification	10	0 -	0 -	0 -	0 +	Disabled	13		
ort Policing	11	0 -	0 •	0 -	0 -	Disabled	0		
ort Scheduler ort Shaping	12	0 -	0 -	0 -	0 -	Disabled	13		
ont Snaping ont Tag	13	0 -	0 -	0 -	0 -	Disabled	0		
emarking ort DSCP	14	0 -	0 -	0 -	0 -	Disabled	23		
SCP-Based QoS	15	0 -	0 -	0 -	0 -	Disabled	10		
SCP Translation	16	0 -	0 -	0 -	0 -	Disabled	21		
	17	0 -	0 -	0 -	0 -	Disabled	10		
	18	0 -	D -	0 -	0 -	Disabled	10		
	19	0 -	0 -	0 -	0 -	Disabled	8		
	20	0 -	0 -	0 -	0 -	Disabled	10		
	21	0 -	0 -	0 -	0 +	Disabled	10		
	22	0 -	D -	0 -	0 -	Disabled	21		
	23	0 -	0 -	0 -	0 +	Disabled	10		
	24	0 -	0 -	0 -	0 -	Disabled	2		
	25	0 -	0 -	0 -	0 -	Disabled	10		
	26	0 -	0 -	0	0 -	Disabled	1		

Save Reset

Port

The port number for which the configuration below applies.

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

Controls the default Drop Precedence Level i.e., the DP level for frames not classified in any other way.

PCP

Controls the default PCP for untagged frames.

DEI

Controls the default DEI for untagged frames.

Tag Class.

Shows the classification mode for tagged frames on this port.

Disabled: Use default QoS class and DP level for tagged frames.

Enabled: 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.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

QoS / Policing

QoS Ingress Port Policer Config

This page allows you to configure the Policer settings for all switch ports.

The displayed settings are:

- ALLNET						ALL8944WMP	- Gigabit PoE Switch	0 2
Configuration System Power Reduction	QoS Ing	ress Port	Policers					
Power Reduction Ports	Port E	nabled	Rate	Un	it	Flow Control		
Security			500	<>				
Aggregation	1		500	kbps	٠	10		
Loop Protection Spanning Tree	2		500	kbps				
• MVR	3	8	500	kbps		13		
IPMC	4		500	kbps				
LLDP	6	8	500	kbps		8		
PoE MAC Table	6		500	kbps				
VLANs	7	8	500	kbps	_	10		
Private VLANs	8		500	kbps	_	10		
VCL	9	0	500	kbps		5		
Voice VLAN	-			_	_			
QoS Port Classification	10		500	kbps				
 Port Policing 	11		500	kbps		8		
 Port Scheduler Port Shaping 	12		500	kbps				
 Port Tag 	13		500	kbps	•	8		
Remarking • Port DSCP	14		500	kbps	•			
 DSCP-Based QoS 	15		500	kbps	•	13		
DSCP Translation	16		500	kbps	-			
m (*	17	8	500	kbps		10		
	18		500	kbps				
	19	8	500	kbps				
	20	0	500	kbps				
	21	8	500	kbps	-			
	22		500	kbps	_	1		
	23	8	500	_	-			
				kbps				
	24		500	kbps	_			
	25	8	500	kbps				
	26		500	kbps				

Save Reset

Port

The port number for which the configuration below applies.

Enabled

Controls whether the policer is enabled on this switch port.

Rate

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

Unit

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

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

QoS Egress Port Schedulers

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

The displayed settings are:

Renard'							AL	L8944
Configuration System Power Reduction	QoS E	gress Port	Sche	dule				
Power Reduction	Port	Mode				ight		
Security	. on		Q0	Q1	Q2	Q3	Q4	Q5
 Aggregation 	1	Strict Priority						
 Loop Protection 	2	Strict Priority				-		
Spanning Tree	3	Strict Priority	-		-	-	-	-
MVR	4	Strict Priority	-	-	-	-	-	-
▶ IPMC	5	Strict Priority		-		-		
LLDP	6	Strict Priority						
 PoE 	7	Strict Priority						
MAC Table	8	Strict Priority	-	-		-		
VLANs	9	Strict Priority						
Private VLANs	10	Strict Priority						
VCL	11	Strict Priority	-	-				
Voice VLAN	12	Strict Priority	-	-				
▼QoS	13	Strict Priority		-	-	-	-	-
 Port Classification 	14	Strict Priority		-				
Port Policing Port Scheduler				•		•		
 Port Shaping 	15	Strict Priority	-					
 Port Tag 	16	Strict Priority	-		-	-	-	-
Remarking	17	Strict Priority	•					
 Port DSCP DSCP-Based QoS 	18	Strict Priority						
DSCP-Based Qos DSCP Translation	19	Strict Priority	-	•	•	•	•	•
DOOD OLIVIER IN	20	Strict Priority	-	-	-	-	-	-
4 II. F	21	Strict Priority	-		-	-	-	-
	22	Strict Priority	-	-	-	-	-	-
	23	Strict Priority						
	24	Strict Priority						
	25	Strict Priority						
	26	Strict Priority	-			-		

Port

The logical port for the settings contained in the same row.

Click on the port number in order to configure the schedulers.

Mode

Shows the scheduling mode for this port.

Qn

Shows the weight for this queue and port.

QoS Egress Port Shapers

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

The displayed settings are:

Runer'						l	ALL8944W	MP - Giga	bit PoE Sv	vitch						
 Configuration System 	Î (QoS E	gress P	ess Port Shapers												
 Power Reduction Ports 		Port		Shapers												
 Pons Security 		For	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port					
 Aggregation 		1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
Loop Protection		2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
 Spanning Tree 		3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
 MVR 		4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
► IPMC		5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
	=	<u>6</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
		7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
• PoE		8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
 MAC Table 		<u>9</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
▶ VLANs		<u>10</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
Private VLANs		<u>11</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
▶ VCL		12	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
Voice VLAN		<u>13</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
▼QoS		<u>14</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
 Port Classification 		<u>15</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
Port Policing		<u>16</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
 Port Scheduler Port Shaping 		17	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
 Port Tag 		<u>18</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
Remarking		<u>19</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
Port DSCP		20	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
DSCP-Based QoS		21	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
 DSCP Translation 	-	22	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
		23	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
		24	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
		25	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					
		<u>26</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled					

Port

The logical port for the settings contained in the same row.

Click on the port number in order to configure the shapers.

Qn

Shows "disabled" or actual queue shaper rate - e.g. "800 Mbps".

Port

Shows "disabled" or actual port shaper rate - e.g. "800 Mbps".

QoS Egress Port Tag Remarking

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

The displayed settings are:

RUNET'		ALL8944WMP - Gigabit PoE Switch	6 🕑
MVR IPMC ILDP PoE MAC Table VLANs Private VLANs VCL Voice VLAN CoS Port Classification Port Policing Port Scheduler Port Schedu	Port Mode 1 Classified 2 Classified 3 Classified 4 Classified 5 Classified 6 Classified 7 Classified 9 Classified 10 Classified 11 Classified 12 Classified 13 Classified 14 Classified 15 Classified 16 Classified 17 Classified 18 Classified 19 Classified 20 Classified 21 Classified 22 Classified 23 Classified 24 Classified 25 Classified 26 Classified 26 Classified		

Port

The logical port for the settings contained in the same row.

Click on the port number in order to configure tag remarking.

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..

QoS / DSCP

Port DSCP Configuration

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

The displayed settings are:

ALMET'					ALLS	HAMMP	Gigabit PoE Switch	Ę
MVR	QoS P	ort DSCP	Configu	atio	'n			
LLDP	Port	Ing	ress		Egress			
PoE MAC Table	Port	Translate	Classi	fy	Rewrite			
VLANs	*		0		0			
Private VLANs	1	13	Disable		Disable			
VCL	2		Disable	-	Disable			
Voice VLAN OoS	3	8	Disable	-	Disable	-		
Port Classification	4		Disable		Disable			
 Port Policing Port Scheduler 	5		Disable	-	Disable			
 Port Scheduler Port Shaping 	6		Disable		Disable			
Port Tag	7	13	Disable		Disable			
Remarking Port DSCP	8		Disable		Disable	•		
 DSCP-Based QoS DSCP Translation 	9		Disable	•	Disable			
 DSCP Translation DSCP Classification 	10		Disable		Disable	•		
 QoS Control List 	11		Disable		Disable	•		
Mirroring UPnP	12		Disable		Disable	*		
• sFlow	13	10	Disable		Disable			
Monitor	14	0	Disable		Disable	•		
Diagnostics Maintenance	15		Disable		Disable	•		
maintenance	16		Disable	÷	Disable	•		
	17	0	Disable	-	Disable	•		
	18		Disable		Disable			
	19		Disable		Disable	_		
	20		Disable	-	Disable	•		
	20		Disable	-	Disable	•		
				-				
	22		Disable	•	Disable	•		
	23		Disable		Disable			
	24		Disable	-	Disable	•		
	25		Disable		Disable	•		
	26		Disable	-	Disable			

Port

The Port coulmn shows the list of ports for which you can configure dscp ingress and egress settings.

Ingress

In Ingress settings you can change ingress translation and classification settings for individual ports.

There are two configuration parameters available in Ingress:

1. Translate

2. Classify

1. Translate

To Enable the Ingress Translation click the checkbox.

2. Classify

Classification for a port have 4 different values.

- Disabled: No Ingress DSCP Classification.
- **DSCP=0**: Classify if incoming (or translated if enabled) DSCP is 0.
- Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.
 - All: Classify all DSCP.

Egress

Port Egress Rewriting can be one of -

- Disabled: No Egress rewrite.
- Enable: Rewrite enabled without remapping.
- Remap DP Unaware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table.
- Remap DP Aware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Port DSCP Configuration

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

The displayed settings are:

Runt'					ALL	8944WMP -	Gigabit PoE Switch	(B) (
• MVR • IPMC	QoS P	ort DSCP (Configu	ratio	n			
► LLDP	-	Ing	ress		Egres	8		
PoE	Port	Translate	Classi	fv	Rewrit			
MAC Table VLANs			0		0			
Private VLANs	1		Disable		Disable	*		
VCL	2		Disable		Disable	-		
Voice VLAN OoS	3		Disable	•	Disable	•		
Port Classification	4		Disable		Disable			
 Port Policing 	5		Disable		Disable			
 Port Scheduler Port Shaping 	6		Disable		Disable			
 Port Tag 	7	10	Disable		Disable			
Remarking Port DSCP	8		Disable		Disable			
 DSCP-Based QoS 	9		Disable	÷	Disable			
 DSCP Translation DSCP Classification 	10		Disable	-	Disable	•		
 QoS Control List 	11		Disable	÷	Disable			
Mirroring UPnP	12		Disable			•		
• sFlow				_	Disable			
Monitor	13		Disable	-	Disable	•		
Diagnostics	14		Disable	-	Disable	•		
Maintenance			Disable	-	Disable	•		
	16		Disable	•	Disable			
	17		Disable		Disable	*		
	18		Disable		Disable			
	19		Disable	-	Disable	•		
	20		Disable	-	Disable	•		
	21		Disable	-	Disable			
	22		Disable	•	Disable	-		
	23		Disable		Disable	*		
	24		Disable	•	Disable	•		
	25		Disable		Disable			
	26		Disable	-	Disable	-		

Save Reset

Port

The Port coulmn shows the list of ports for which you can configure dscp ingress and egress settings.

Ingress

In Ingress settings you can change ingress translation and classification settings for individual ports.

There are two configuration parameters available in Ingress:

1. Translate

2. Classify

1. Translate

To Enable the Ingress Translation click the checkbox.

2. Classify

Classification for a port have 4 different values.

- **Disabled:** No Ingress DSCP Classification.
- **DSCP=0**: Classify if incoming (or translated if enabled) DSCP is 0.
- Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.
- All: Classify all DSCP.

Egress

Port Egress Rewriting can be one of -

- **Disabled:** No Egress rewrite.
- Enable: Rewrite enabled without remapping.
- Remap DP Unaware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table.
- Remap DP Aware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

DSCP based QoS Ingress Classification

This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.

The displayed settings are:

1 DECD D	and Ori	S Ingress (Classifier
		QoS Class	
	13	••	••
0 (8E)	10	0 -	0 -
1	8	0 -	0 -
3	10	0 -	0 -
4		0 -	0 -
5		0 -	0
, 6 265 7	8	0 -	0 -
2S 7 an flor 8 (CS1)		0 -	0 -
9	8	0 -	0 -
10 (AF11)	10	0 -	0 -
11	10	0 -	0 -
12 (AF12)		0 -	0 -
13	8	0 -	0 -
14 (AF13) 15		0 -	0 -
16 (CS2)		0 -	0 -
17		0 -	0
18 (AF21)	8	0 -	0 -
19	10	0 -	0 -
20 (AF22) 21	8	0 -	0 -
22 (AF23)	10	0 -	0 -
23	13	0 -	0 -
24 (CS3)	13	0 -	0 -
25		0 *	0 💌
26 (AF31)	10	0 -	0 -
27 28 (AF32)		0 -	0 -
29		0 -	0 .
30 (AF33)	8	0 -	0 -
31		0 -	0 -
32 (CS4)	12	0 -	0 -
33		0 -	0 -
34 (AF41) 35	8	0 -	0 -
36 (AF42)	10	0 -	0 -
37		0 -	0 -
38 (AF43)	8	0 -	0
39		0 -	0 -
40 (CS5)	8	0 -	0 -
41	8	0 -	0 -
42		0 -	0 -
44		0 -	0 -
45		0 -	0 -
46 (EF)	8	0 -	0 =
47	E)	0 -	0 -
48 (CS6)		0 -	0 -
49	5	0 -	0 -
51	10	0 -	0 -
62	12	0 -	0 -
63	10	0 -	0 -
54	B	0 -	0 -
55	10	0 -	0 -
56 (CS7) 57		0 -	0 -
58	2	0 -	0 -
59	10	0 -	0 -
60	10	0 -	0 -
00			
61	5	0 -	0 -

Save Reset

DSCP

Maximum number of supported DSCP values are 64.

Trust

Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QOs class and Drop Precedence Level. Frames with un- trusted DSCP values are treated as a non-IP frame.

QoS Class

QoS class value can be any of (0-7)

DPL

Drop Precedence Level (0-1)

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

DSCP Translation

This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.

The displayed settings are:

нин

- A Spanning rise
 MVR
 MVR
 IPMC
 LLDP
 PoE
 MAC Table
 VLANs
 Private VLANs
 VCL
 Voice VLAN
 QoS
 Port Classification
 Port Policing
 Port Scheduler
 Port Scheduler
 Port Scheduler
 Port Scheduler
 Port Scheduler
 Port DSCP
 Translation
 DSCP Translation
 DSCP Classificative
 QoS Control List
 Mirroring
 UPAP
 SFlow
 Monitor
 Diagnostics
 Maintenance

DSCP	In	gress			Egr		
DSCF	Translat	e C	lassify	Remap D	P0	Remap D	P1
	\diamond	-		\diamond	•	\diamond	-
(BE)	0 (BE)	•		0 (BE)	-	0 (BE)	-
	1	•		1	-	1	-
	2	•		2	-	2	-
	3	•		3	-	3	-
	4	•		4	-	4	-
5	5	•		5	-	5	•
;	6	•		6	-	6	-
,	7	-		7	-	7	•
6 (CS1)	8 (CS1)	•		8 (CS1)	-	8 (CS1)	-
)	9	•		9	-	9	-
0 (AF11)	10 (AF11)	•		10 (AF11)	-	10 (AF11)	-
1	11	-	—	11	-	11	-
2 (AF12)	12 (AF12)	•		12 (AF12)	•	12 (AF12)	-
3	13	•		13	-	13	-
4 (AF13)	14 (AF13)	•		14 (AF13)	•	14 (AF13)	•
5	15	•		15	•	15	•
6 (CS2)	16 (CS2)	•		16 (CS2)	•	16 (CS2)	-
7	17	•		17	•	17	•
8 (AF21)	18 (AF21)	_		18 (AF21)		18 (AF21)	-
9	19	-		19	•	19	-
0 (AF22)	20 (AF22)			20 (AF22)	-	20 (AF22)	
1	21	-		21	•	21	-
2 (AF23)	22 (AF23)	•		22 (AF23)		22 (AF23)	
3	22 (/ 1 20)	•		23	•	23	-
4 (CS3)	24 (CS3)	•		24 (CS3)	•	24 (CS3)	-
5	25	-		25	•	25	-
.5 6 (AF31)	26 (AF31)			26 (AF31)		26 (AF31)	
	20 (AF31) 27	•		20 (AF31)	-	20 (AF31) 27	•
7							
8 (AF32)	28 (AF32)	=		28 (AF32)		28 (AF32)	-
9	29	•		29	-	29	-
0 (AF33)	30 (AF33)	•		30 (AF33)		30 (AF33)	
1	31	•		31	•	31	-
2 (CS4)	32 (CS4)	•		32 (CS4)	-	32 (CS4)	-
3	33	•		33	-	33	-
4 (AF41)	34 (AF41)	•		34 (AF41)	•	34 (AF41)	-
5	35	•		35	•	35	-
6 (AF42)	36 (AF42)	•		36 (AF42)	•	36 (AF42)	-
57	37	-		37	-	37	-
8 (AF43)	38 (AF43)	-		38 (AF43)	-	38 (AF43)	-
9	39	•		39	•	39	•
0 (CS5)	40 (CS5)	-		40 (CS5)	•	40 (CS5)	•
1	41	•		41	•	41	•
2	42	•		42	•	42	•
3	43	•		43	•	43	•
1	44	-		44	•	44	•
	45	•		45	•	45	•
6 (EF)	46 (EF)	•		46 (EF)	•	46 (EF)	•
7	47	•		47	-	47	•
8 (CS6)	48 (CS6)	-		48 (CS6)	•	48 (CS6)	•
9	49	•		49	•	49	•
2	50	•		50	•	50	-
1	51	•		51	-	51	•
2	52	•		52	•	52	•
3	53	•		52	•	53	•
5 1	53	•		53	-	53	•
+ 5	55	=		55		55	
		•		55 (CS7)	-		-
6 (CS7) 7	56 (CS7)	•			-	56 (CS7)	-
7	57	•		57	-	57	-
8	58	•		58	-	58	-
i9	59	•		59	-	59	-
0	60	•		60	•	60	-
51	61	•		61	•	61	-
52	62	•		62	•	62	-
3	63	-		63	-	63	-

ALL8944WMP - Gigabit PoE Switch

Save Reset

User Manual ALL8944WMP

1 2

DSCP

Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.

Ingress

Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.

There are two configuration parameters for DSCP Translation -

1. Translate

2. Classify

1. Translate

DSCP at Ingress side can be translated to any of (0-63) DSCP values.

2. Classify

Click to enable Classification at Ingress side.

Egress

There are the following configurable parameters for Egress side -

1. Remap DP0 Controls the remapping for frames with DP level 0.

2. Remap DP1 Controls the remapping for frames with DP level 1.

1. Remap DP0

Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

2. Remap DP1

Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

DSCP Classification

This page allows you to configure the mapping of QoS class and Drop Precedence Level to DSCP value.

The displayed settings are:

- BLINET'					ALL8944WMP - Gigabit PoE Switch	6
• MVR • IPMC	DSCP Clas				Ϋ́.	
LLDP PoE	QoS Class	DPL	DSCI	P		
MAC Table	•		\diamond			
VLANs	0	0	0 (BE)	-		
Private VLANs	0	1	0 (BE)	•		
VCL	1	0	0 (BE)	-		
Voice VLAN	1	1	0 (BE)			
QoS	2	0	0 (BE)	-		
 Port Classification Port Policing 	2	1	0 (BE)	x		
 Port Scheduler 	3	0	0 (BE)			
 Port Shaping Port Tag 	3	1	0 (BE)			
Remarking	4	0	0 (BE)			
Port DSCP	4	1	0 (BE)			
 DSCP-Based QoS DSCP Translation 	5	0	0 (BE)			
 DSCP Classification 	5	1	0 (BE)			
 QoS Control List 	6	0	0 (BE)	•		
Mirroring UPnP	6	1	0 (BE)			
sFlow	7	0	0 (BE)			
Ionitor	7		0 (BE)			
liagnostics			0 (32)	100		
laintenance	Save R	eset				

QoS Class

Actual QoS class.

DPL

Actual Drop Precedence Level.

DSCP

Select the classified DSCP value (0-63).

Buttons

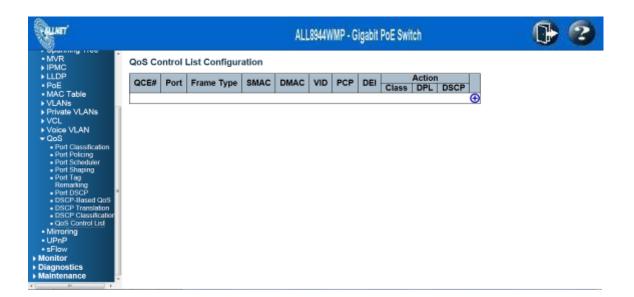
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

QoS Control List Configuration

QoS Control List Configuration

This page shows the QoS Control List(QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is **256** on each switch. Click on the lowest plus sign to add a new QCE to the list.



QCE#

Indicates the index of QCE.

Port

Indicates the list of ports configured with the QCE.

Frame Type

Indicates the type of frame to look for incomming frames. Possible frame types are:

Any: The QCE will match all frame type.

Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

LLC: Only (LLC) frames are allowed.

SNAP: Only (SNAP) frames are allowed.

IPv4: The QCE will match only IPV4 frames.

IPv6: The QCE will match only IPV6 frames.

SMAC

Displays the OUI field of Source MAC address, i.e. first three octet (byte) of MAC address.

DMAC

Specify the type of Destination MAC addresses for incoming frame. Possible values are:

Any: All types of Destination MAC addresses are allowed.

Unicast: Only Unicast MAC addresses are allowed.

Multicast: Only Multicast MAC addresses are allowed.

Broadcast: Only Broadcast MAC addresses are allowedd.

The default value is 'Any'.

VID

Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'

PCP

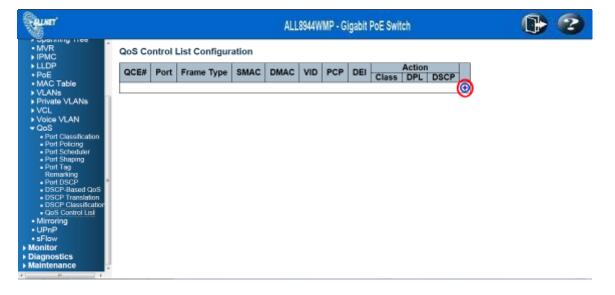
Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI

Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'.

Conflict

Displays QCE status. It may happen that resources required to add a QCE may not available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'.Please note that conflict can be resolved by releaseing the resource required by the QCE and pressing 'Refresh' button.



Action

Indicates the classification action taken on ingress frame if parameters configured are matched with the

frame's content.

There are three action fields: Class, DPL and DSCP.

Class: Classified QoS class..

DPL: Classified Drop Precedence Level.

DSCP: Classified DSCP value.

Modification Buttons

You can modify each QCE (QoS Control Entry) in the table using the following buttons:

: Inserts a new QCE before the current row.

(CE): Edits the QCE.

(1): Moves the QCE up the list.

- S Moves the QCE down the list.
- 8: Deletes the QCE.

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

Buttons

Refresh : Click to refresh the page. This will help to check the lates conflict status after releasing the resources.

Storm Control Configuration

Storm control for the switch is configured on this page.

There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table. The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch.

Frame Type

The settings in a particular row apply to the frame type listed here: Unicast, Multicast or Broadcast.

Enable

Enable or disable the storm control status for the given frame type.

Rate

The rate unit is packets per second (pps). Valid values

are:1,2,4,8,16,32,64,128,256,512,1K,2K,4K,8K,16K,32K,64K,128K,256K,512K,1024K,2048K,4096K,8192 K,16384K or 32768K.

Mirroring Configuration

Configure port Mirroring on this page.

To debug network problems, selected traffic can be copied, or mirrored, on a **mirror port** where a frame analyzer can be attached to analyze the frame flow.

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

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

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.

Mirror Port Configuration

The following table is used for Rx and Tx enabling.



Port

The logical port for the settings contained in the same row.

Mode

Select mirror mode.

Rx only Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.

Tx only Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.

Disabled: Neither frames transmitted nor frames received are mirrored.

Enabled Frames received and frames transmitted are mirrored on the mirror port.

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

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

UPnP Configuration

Configure UPnP on this page.

Runer'		ALL8944WMP - Gigabit PoE Switch	6 🕄
Configuration System Power Reduction Ports Security Aggregation Loop Protection Spanning Tree MVR IPMC LLDP PoE MAC Table VLANs VCL Voice VLANs VCL Voice VLANs OoS Mirroring UPnP sFlow Monitor Diagnostics Maintenance	UPnP Configuration Mode Disa TTL 4 Advertising Duration 100 Save Reset	abled	

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.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

MRP Configuration

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

The displayed settings are:

Port

The Port column shows the list of ports for which you can configure MRP settings. There are 2 types configuration settings which can be configured on per port bases.

- Timer Values
- Application
- Attribute Type
- MRP Applicant
- Periodic Tx

Application

Currently only supported application is MVRP.

Attribute Type

Currently only supported Attribute Type is VLAN.

MRP Applicant

This configuration is used to configure the Applicant state machine behaviour for MRP on a perticular port locally.

- Normal-participant: In this mode the Applicant state machine will operate normally in MRP protocol exchanges.
- Non-participant : In this mode the Applicant state machine will not participate in the protocol operation.

The default configuration is normal participant.

Timer Values

Three different timers can be configured on this page:

1. Join Timer

2. Leave Timer

3. Leave All Timer

1. Join Timer

The default value for Join timer is 200ms.

2. Leave Timer

The range of values for Leave Time is 600-1000ms. The default value for Leave Timer is 600ms.

3. Leave All Timer

The default value for Leave All Timer is 10000ms.

Periodic Tx

This configuration is used to configure transmission mode and this can be congured either as enabled or disable. The default value of Periodic Tx is disable.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

MVRP Configuration

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

The displayed settings are:

MVRP Mode

MVRP Mode is a global setting, to enable the MVRP globally select 'Enable' from menu and to disable MVRP globally select 'Disable'.

Default value of Global MVRP Mode is 'Disable'

Port

The Port coulmn shows the list of ports for which you can configure per port MVRP settings. There are three configuration settings which can be configured on per port bases.

- MVRP Mode:
- MVRP rrole:

1. MVRP Mode

This configuration is to enable/disable MVRP Mode on perticular port locally.

- **Disabled:**Select to Disable MVRP mode on this port.
- Enable: Select to Enable MVRP mode on this port.

The default value of configuration is disable.

2. MVRP rrole

This configuration is used to configure restricted role on an interface.

- Disabled:Select to Disable MVRP role on this port.
- Enable: Select to Enable MVRP role on this port.

The default configuration is disable.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Flow Receiver Configuration

The sFlow Receiver configuration for the switch can be monitored and modified here. Up to 1 Receiver is supported. This page allows for configuring sFlow Receiver IP type, sFlow Receiver IP Address, Port Number, for each sFlow Receiver.

elmet'				ALL8944WM	P - Gigabit i	POE SWIICH	
nfiguration System Power Reduction		Configuratio					Refresh
Ports Security	Owne		<none></none>			Release	
Aggregation Loop Protection		r dress/Hostnam	_			LABIARIA	
Spanning Tree	UDP F		6343				
MVR	Timed		0			seconds	
IPMC LLDP		Datagram Size	1400			bytes	
PoE MAC Table		onfiguration				-1	
VLANs Private VLANs			Flow Sampler		Counte	r Poller	
VCL	Port	Enabled 3	Sampling Rate	Max. Header		Interval	
Voice VLAN	-	8	0	128		0	
QoS Mirroring	1	8	0	128	10	0	
UPnP	2		0	128		0	
Flow	3		0	128		0	
onitor agnostics	4		0	128		0	
intenance	5	8	0	128		0	
	6		0	128		0	
	7	8	0	128		0	
	8		0	128		0	
	9	8	0	128	10	0	
	10	8	0	128		0	
	11		0	128		0	
	12		0	128		0	
	13	8	0	128		0	
	14		0	128		0	
	15	8	0	128		0	
	16		0	128		0	
	17		0	128		0	
	18		0	128		0	
	19	8	0	128		0	
	20		0	128		0	
	21	8	0	128		0	
	22		0	128		0	
	23	8	0	128		0	
	24		0	128		0	
	25		0	128		0	
	26	8	0	128		0	

Navigating the Receiver Configuration

The "Current" field displays the currently configured sFlow Receiver. The "Configured" field displays the new Receiver Configuration.

Receiver Id

The "Receiver ID" input fields allow the user to select the receiver ID. Indicates the ID of this particular sFlow Receiver. Currently one ID is supported as one receiver is supported.

IP Туре

A drop down list to select the type of IP of receiver is displayed. The default IP type of the receiver is IPV4.

IP Address

The address of a reachable IP is to be entered into the text box.

This IP is used to monitor the sFlow samples sent by sFlow Agent(our switch).

Port

A port to listen to the sFlow Agent has to be configured for the Receiver.

The value of the port number has to be typed into the text box.

The value accepted is within the range of 1-65535. But an appropriate port number, not used by other protocols need to be configured. The default port number is 6343.

Time Out

It is the duration during which the receiver receives samples, Once it is expired the sampler stops sending the samples. It is through the management the value is set before it expires. The value accepted is within the range of 0-2147483647 sec. The default is 0 sec.

Datagram Size

It is the maximum UDP datagram size to send out the sFlow samples to the receiver. The value accepted is within the range of 200-1500 bytes. The default is 1400 bytes.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

sFlow Sampler Configuration

This page displays the configured sFlow samplers on the switch .

sFlow Ports

List of the port numbers on which sFlow is configured.

sFlow Instance

Configured sFlow instance for the port number.

Flow Sampling

Packet flow sampling refers to arbitrarily choosing some packets out of a specified number, reading the first "Max Hdr Size" bytes and exporting the sampled datagram for analysis.

The attributes associated with the flow sampling are: sampler type, sampling rate, maximum header size.

Sampler Type

Configured sampler type on the port and could be any of the types: None, RX,TX, ALL.

Default value is "none".

Sampling Rate

Configured sampling rate on the ports.

Max Hdr Size

Configured size of the header of the sampled frame.

Counter Sampling

Counter sampling performs periodic, time-based sampling or polling of counters associated with an interface enabled for sFlow.

Attribute associated with counter sampling is polling interval.

Polling Interval

Configured polling interval for the counter sampling.

Editing Button

You can modify each port's sampler configuration the table using the following button:

(e): Edits the port sampler configuration.

Monitor System Information

The switch system information is provided here.

Runt'		ALL8944WMP - Gigabit PoE Switch	1
Configuration Monitor System	System Informat	Auto-refresh 🗆 Refresh	
 Information 	Contrat		
CPU Load Log Detailed Log	Contact Name Location		
+ Ports	Escation	Hardware	
State Traffic Overview QoS Statistics	MAC Address Chip ID	00:0F:C9:08:7A:AC VSC7427	
QOS Statistics QCL Status	and the second	Time	
Detailed Statistics Security	System Date System Uptime	1970-01-01T00:13:46+00:00 0d:00:13:46	
+ LACP		Software	
Loop Protection Spanning Tree	Software Version Software Date	PoE (standalone) dev-build by root@virtual-centos 2012-07-01T15:54:24+08:00 2012-07-01T15:54:24+08:00	
MVR IPMC LLDP	2		
PoE MAC Table			
VLANs VCL			
sFlow Diagnostics Maintenance			

Contact

The system contact configured in Configuration | System | Information | System Contact.

Name

The system name configured in Configuration | System | Information | System Name.

Location

The system location configured in Configuration | System | Information | System Location.

MAC Address

The MAC Address of this switch.

Chip ID

The Chip ID of this switch.

System Date

The current (GMT) system time and date. The system time is obtained through the configured SNTP Server, if any.

System Uptime

The period of time the device has been operational.

Software Version

The software version of this switch.

Software Date

The date when the switch software was produced.

Buttons

Auto-refresh : Check this box to enable an automatic refresh of the page at regular intervals.

Refresh : Click to refresh the page; any changes made locally will be undone.

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.

		ALL8944WMP - Gig	abit PoE Switch	1
CPU Load 100ms 3%	1sec 0%	10sec 0%	(all numbers running a	Auto-refresh 🖻 verage)
				75%
				25%
			CPU Load	

Buttons :

Auto-refresh : Check this box to enable an automatic refresh of the page at regular intervals.

System Log Information

The switch system log information is provided here.

FRUME T'	ALL8944WMP - Gigabit PoE Switch	1
Configuration Monitor System CPU Load Cg Defailed Log Ports State Traffic Overview QoS Statistics	System Log Information Auto-refresh Refresh Level All • Clear Level All • The total number of entries is 4 for the given level. Start from ID 1 with 20	Clear << <> >> >>
OCL Status Detailed Status(s) Security LACP Loop Protection Spanning Tree MYR IPMC ILDP PoE MAC Table VLANs VCL sFlow Diagnostics Maintenance	ID Level Time Message 1 Info 1970-01-01100:00:01+00:00 Switch just made a cold boot. 2 Info 1970-01-01100:00:04+00:00 Link up port 14 3 Info 1970-01-01100:02:29+00:00 Link down on port 14 4 Info 1970-01-01100:02:31+00:00 Link up on port 14	

ID

The ID (>= 1) of the system log entry.

- ALMET	ALL8944WMP - Gigabit PoE Switch
Configuration Configuration Monitor System Information CPU Load Log Dotated Log Ports State Traffic Overview	System Log Information Auto-refresh Refresh Clear I<
OoS Statistics OOL Statistics OOL Statistics Detailed Statistics Decarled Statistics Loop Protection Spanning Tree MVR IPMC ILUDP VOL VOL VOL SFlow Diagnostics Maintenance	ID Level Time Message 1 Info 1970-01-01100.00:01+00:00 Switch just made a cold boot. 2 Info 1970-01-01100:00:21+00:00 Link up on port 14 3 Info 1970-01-01100:00:21+00:00 Link up on port 14 4 Info 1970-01-01100:00:21+00:00 Link up on port 14

Level

The level of the system log entry. The following level types are supported:

Info: Information level of the system log.

Warning: Warning level of the system log.

Error: Error level of the system log.

All: All levels.

Time

The time of the system log entry.

Message

The message of the system log entry.

Buttons

Auto-refresh : Check this box to enable an automatic refresh of the page at regular intervals. Refresh: Updates the system log entries, starting from the current entry ID. Clear: Flushes all system log entries.

/<<: Updates the system log entries, starting from the first available entry ID.

<<: Updates the system log entries, ending at the last entry currently displayed.

>>: Updates the system log entries, starting from the last entry currently displayed.

>>/: Updates the system log entries, ending at the last available entry ID.

System / Detailed Log

Detailed System Log Information

The switch system detailed log information is provided here.

ID

The ID (>= 1) of the system log entry.

Message

The detailed message of the system log entry.

Buttons

Refresh : Updates the system log entry to the current entry ID.

/<<: Updates the system log entry to the first available entry ID.

<<: Updates the system log entry to the previous available entry ID.

>>: Updates the system log entry to the next available entry ID.

>>/: Updates the system log entry to the last available entry ID.

Thermal Protection Status

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

Thermal Protection Port Status

Shows if the port is thermally protected (link is down) or if the port is operating normally.

Chip Temperature

Shows the current chip temperature in degrees Celcius.

Buttons

Refresh: Click to refresh the page immediately.

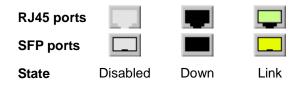
Auto-refresh \Box : Check this box to enable an automatic refresh of the page at regular intervals.

Port State

This page provides an overview of the current switch port states.



The port states are illustrated as follows:



Buttons

Auto-refresh \Box : Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.

Refresh : Click to refresh the page; any changes made locally will be undone.

Port Statistics Overview

This page provides an overview of general traffic statistics for all switch ports.

The displayed counters are:

RELINET'				A	LL8844WMP - G	igabit PoE S	witch			2
Configuration Monitor	Port S	itatistics O	verview				Aut	o-refresh 🗉 (Refresh Cle	ar
System		Pa	ckets	E	lytes	E	rrors	D	rops	Filtere
✓ Ports	Port	Received					Transmitted	Received	Transmitted	Receive
 State Traffic Overview 	1	0	0	0	0	0	0	0	0	1100011
 QoS Statistics 	2	ŏ	ő	ő	ő	ő	0	ő	ő	
QCL Status	3	ŏ	ő	ő	ŏ	ő	ő	ŏ	ŏ	
 Detailed Statistics 	Ă	ő	ő	ő	ő	ő	ő	ő	ő	
Security		ő	ő	ő	ő	ő	ő	ő	ŏ	
▶ LACP	ă	ő	ő	ő	ő	ő	ő	ő	ő	
 Loop Protection 	- ×	ŏ	õ	ő	ŏ	ő	ő	ŏ	ŏ	
Spanning Tree	ŝ	ŏ	ő	ő	ŏ	ő	ő	ŏ	ŏ	
▶ MVR	- ŝ	ő	ő	Ď	ő	ő	ő	ő	ő	
▶ IPMC	9 10	ő	ő	Ő.	ő	ő	ő	ő	ő	
> LLDP	11	ŏ	ő	Ő	ŏ	ő	ő	õ	ŏ	
• PoE	12	0	0	0	0	0	0	0	0	
MAC Table	12 13	Ő	õ	Ő	Ő	Ő	õ	õ	Ő	
► VLANs	14	4534	3426	751394	526890	0	0	0	0	21
▶ VCL	14 15 16 17 18 19 20	0	0	0	0	0	Ő	Ő	Ő	-
• sFlow	16	0	0	0	Ó	0	0	0	0	
Diagnostics	17	0	0	0	0	0	0	0	0	
	18	Ő	0	0	Ő	Ő	Ő	Ū.	Ő	
Maintenance	19	0	0	0	0	0	0	0	0	
	20	Ű.	0	0	Ó	0	0	Ű.	Ó	
	21	0	0	0	0	0	0	0	0	
	21 22	0	0	0	0	0	0	0	0	
						0	0			

Port

The logical port for the settings contained in the same row.

Packets

The number of received and transmitted packets per port.

Bytes

The number of received and transmitted bytes per port.

Errors

The number of frames received in error and the number of incomplete transmissions per port.

Drops

The number of frames discarded due to ingress or egress congestion.

Filtered

The number of received frames filtered by the forwarding process.

Buttons

Refresh : Click to refresh the page immediately.

Clear: Clears the counters for all ports.

Auto-refresh \Box : Check this box to enable an automatic refresh of the page at regular intervals.

QoS Statistics

This page provides statistics for the different queues for all switch ports.

The displayed counters are:

Reuner'									ALLS	944W	MP-	Gigat	it Po	E Swi	ich				1	0	9	3
 ▶ Configuration ▼ Monitor 	Queu	ing Co	unte	ers													Auto-re	efresh 🛛	Refresh	n Cle	ear	ŕ
▶ System		Q)	Q	1	Q	2	Q	3	Q	4	Q	5	Q	6	(27	1				
✓ Ports	Port	Rx	Тх	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx					
 State Traffic Overview 	1		0	0	0	0	0		0	0	0		0		0	0	0					
 Traffic Overview QoS Statistics 	$\frac{1}{2}$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0					
QCL Status	<u><u></u></u>	0	0	Ö	0	0	0	0	0	0	0	0	0	0	0	0	0					
 Detailed Statistics 	<u> </u>	ő	ŏ	ŏ	Ö	Ö	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ	Ö	ŏ	ŏ	Ö	Ő					
► Security	4 5 6	0	ŏ	ŏ	ő	0	0	0	Ö	ő	0	0	0	ő	0	ő	0					
LACP	Ē	Ő	Ő	Ő	Ő	Ö	Ő	Ő	Ő	ŏ	ŏ	Ő	0	Ö	ō	0	0					
 Loop Protection 	7	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ					
Spanning Tree	<u>7</u> 8	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ	ŏ					:
► MVR	9	ō	ō	ō	ō	ō	ō	Ō	ō	ō	ō	ō	ō	ō	ō	ō	Ő					
▶ IPMC	10	ō	Ō	0	0	Ō	Ō	Ō	Ō	ō	Ō	Ō	0	0	ō	Ō	Ō					
▶ LLDP	11	Ō	Ō	Ō	Ō	Ō	Ō	Ō	0	Ō	Ō	Ō	Ō	Ō	Ō	0	Ō					
• PoE	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0					
MAC Table	13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0					
► VLANs	14	4867	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3815					
VCL	15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0					
• sFlow	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0					
Diagnostics	17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0					
Maintenance	18 19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0					
P Multitenunce	<u>19</u>	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0					
	20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0					
	21 22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0					
	22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0					
	23 24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0					
	24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0					
	25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0					
	26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	J				

Port

The logical port for the settings contained in the same row.

Qn

There are 8 QoS queues per port. Q0 is the lowest priority queue.

Rx/Tx

The number of received and transmitted packets per queue.

Buttons

Refresh : Click to refresh the page immediately.

Clear: Clears the counters for all ports.

Auto-refresh \square : Check this box to enable an automatic refresh of the page at regular intervals.

QCL Status

This page shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is **256** on each switch.

Reward'	ALLS	944WMP - Gigabit PoE Switch	1 🔁
Configuration Monitor System Ports State Irafic Overview QoS Statistics OCL Status Detailed Statistics Security LACP Loop Protection Spanning Tree MVR IPMC LIDP PoE MAC Table VCL sFlow Diagnostics Maintenance		Combined Auto-refresh Resolve Conflict	Refresh

Lloor		
User		

Indicates the QCL user.

QCE#

Indicates the index of QCE.

Frame Type

Indicates the type of frame to look for incomming frames. Possible frame types are:

Any: The QCE will match all frame type.

Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

LLC: Only (LLC) frames are allowed.

SNAP: Only (SNAP) frames are allowed.

IPv4: The QCE will match only IPV4 frames.

IPv6: The QCE will match only IPV6 frames.

Port

Indicates the list of ports configured with the QCE.

Action

Indicates the classification action taken on ingress frame if parameters configured are matched with the

frame's content.

There are three action fields: Class, DPL and DSCP.

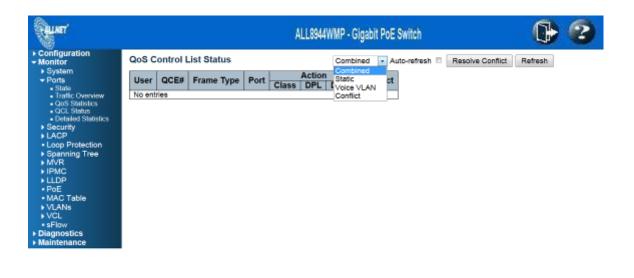
Class: Classified QoS class; if a frame matches the QCE it will be put in the queue.

DPL: <u>Drop Precedence Level</u>; if a frame matches the QCE then DP level will set to value displayed under DPL column.

DSCP: If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.

Conflict

Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releaseing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.



Buttons

: Select the QCL status from this drop down list.

Auto-refresh \Box : Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.

Resolve Conflict: Click to release the resources required to add QCL entry, incase conflict status for any QCL entry is 'yes'.

Refresh: Click to refresh the page; any changes made locally will be undone

Detailed Port Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

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

Rever'		ALL8944W	IMP - Gigabit PoE Switch	6	2
Configuration Monitor	Detailed Port Statistics Port 1		Port 1 × Aut	to-refresh 🗉 Refresh Clea	r
 System 	Receive Total		Transmit Tot	al	
	Rx Packets	0	Tx Packets	0	
 State Traffic Overview 	Rx Octets	0	Tx Octets	0	
QoS Statistics	Rx Unicast	ő	Tx Unicast	ő	
OCL Status	Rx Multicast	ŏ	Tx Multicast	ŏ	
 Detailed Statistics 	Rx Broadcast	0	Tx Broadcast	0	
Security	Rx Pause	0	Tx Pause	0	
LACP	Receive Size Counters		Transmit Size Cor	unters	
 Loop Protection 	Rx 64 Bytes	0	Tx 64 Bytes	0	
Spanning Tree	Rx 65-127 Bytes	Ő	Tx 65-127 Bytes	ŏ	
MVR	Rx 128-255 Bytes	0	Tx 128-255 Bytes	0	
IPMC	Rx 256-511 Bytes	0	Tx 256-511 Bytes	0	
LLDP	Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0	
PoE	Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0	
 MAC Table 	Rx 1527- Bytes	0	Tx 1527- Bytes	0	
VLANs	Receive Queue Counters		Transmit Queue Co	ounters	
VCL	Rx Q0	0	Tx Q0	0	
• sFlow	Rx Q1	0	Tx Q1	0	
lagnostics	Rx Q2	0	Tx Q2	0	
laintenance	Rx Q3	0	Tx Q3	0	
	Rx Q4	0	Tx Q4	0	
	Rx Q5	0	Tx Q5	0	
	Rx Q6	0	Tx Q6	0	
	Rx Q7	0	Tx Q7	0	
	Receive Error Counters		Transmit Error Co		
	Rx Drops	0	Tx Drops	0	
	Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0	
	Rx Undersize	0			
	Rx Oversize	0			
	Rx Fragments	0			
	Rx Jabber	0			
	Rx Filtered	0			

Receive Total and Transmit Total

Rx and Tx Packets

The number of received and transmitted (good and bad) packets.

Rx and Tx Octets

The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

Rx and Tx Unicast

The number of received and transmitted (good and bad) unicast packets.

Rx and Tx Multicast

The number of received and transmitted (good and bad) multicast packets.

Rx and Tx Broadcast

The number of received and transmitted (good and bad) broadcast packets.

Rx and Tx Pause

A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters

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

Receive and Transmit Queue Counters

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

Receive Error Counters

Rx Drops

The number of frames dropped due to lack of receive buffers or egress congestion.

Rx CRC/Alignment

The number of frames received with CRC or alignment errors.

Rx Undersize

The number of short¹ frames received with valid CRC.

Rx Oversize

The number of long² frames received with valid CRC.

Rx Fragments

The number of short¹ frames received with invalid CRC.

Rx Jabber

The number of long² frames received with invalid CRC.

Rx Filtered

The number of received frames filtered by the forwarding process.

¹ Short frames are frames that are smaller than 64 bytes.

²Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

Tx Drops

The number of frames dropped due to output buffer congestion.

Tx Late/Exc. Coll.

The number of frames dropped due to excessive or late collisions.

-RUNIT'		ALL8944WMP - Gigabit PoE Switch							
Configuration Monitor	Detailed Port Statistics Port 1			Port 1	Auto-refresh 🗆 Refresh	Clear			
 System Ports 	Receive Total			Port 2	Total				
Ports State	Rx Packets	0	Tx Packets	Port 3	0				
 Traffic Overview 	Rx Octets	0	Tx Octets	Port 4	0				
QoS Statistics	Rx Unicast	0	Tx Unicast	Port 5	0				
 QCL Status 	Rx Multicast	0	Tx Multicast	Port 6	0				
 Detailed Statistics 	Rx Broadcast	0	Tx Broadcast	Port 7	0				
 Security 	Rx Pause	0	Tx Pause	Port 8	0				
► LACP	Receive Size Counters		Trai	Port 9	Counters				
 Loop Protection 	Rx 64 Bytes	0	Tx 64 Bytes	Port 10	0				
Spanning Tree	Rx 65-127 Bytes	0	Tx 65-127 Bytes	Port 11	0				
▶ MVR	Rx 128-255 Bytes	0	Tx 128-255 Bytes	Port 12	0				
▶ IPMC	Rx 256-511 Bytes	0	Tx 256-511 Bytes	Port 13	0				
LLDP	Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	Port 14	0				
PoE	Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	Port 15	0				
 MAC Table 	Rx 1527- Bytes	0	Tx 1527- Bytes	Port 16	0				
▶ VLANs	Receive Queue Counters		Tran	Port 17	Counters				
▶ VCL	Rx Q0	0	Tx Q0	Port 18	0				
 sFlow 	Rx Q1	0	Tx Q1	Port 19	0				
Diagnostics	Rx Q2	0	Tx Q2	Port 20	0				
Maintenance	Rx Q3	0	Tx Q3	Port 21	0				
	Rx Q4	0	Tx Q4	Port 22	0				
	Rx Q5	0	Tx Q5	Port 23	0				
	Rx Q6	0	Tx Q6	Port 24	0				
	Rx Q7	0	Tx Q7	Port 25	0				
	Receive Error Counters		Trar	Port 26	Counters				

Buttons

The port select box determines which port is affected by clicking the buttons.

Refresh : Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

Auto-refresh \Box : Check this box to enable an automatic refresh of the page at regular intervals.

Access Management Statistics

This page provides statistics for access management.

Aunt.			itch	1		
Configuration Monitor System		anagement Statisti Received Packets	Auto-refresh	Refresh Clear		
Ports	HTTP	0	Allowed Packets	Discarded Packets		
 Security Access Management 	HTTPS	0	0	0		
Statistics	SNMP	0	0	0		
 Network AAA 	SSH SSH	0	0	0		
> Switch	aan	v	· · ·			
►LACP						
 Loop Protection 						
Spanning Tree						
MVR IPMC						
> LLDP						
• PoE						
MAC Table						
VLANs						
▶ VCL						
sFlow Diagnostics						
Maintenance						

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.

Buttons

Auto-refresh : Click this box to enable an automatic refresh of the page at regular intervals.Refresh: Click to refresh the page immediately.Clear : Clear all statistics.

Security / Network /Port Security/ Switch

Port Security Switch Status

This page 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.

RELNET'					ALL8944WMP - Gigabit PoE Switch	(
Configuration Monitor	Port S	Security	Switch St	atus		Auto-refresh
► System		-				Finite Letter and -
Ports	User	Nodule L	egend			
- Security				-		
 Access 		Module I		DF		
Management	802.1	Control	L 8	_		
Statistics Vetwork		A Shooping				
 Network Port Security 	Voice		v			
 Switch 	T GROUP	1000				
 Port 	Port S	tatus				
► NAS					_	
 ACL Status DHCP 	Port	Users	State	MAC Count		
ARP Inspection				Current Limi	t	
 IP Source Guard 	1		Disabled		-	
• AMA	2		Disabled Disabled		•	
Switch LACP	3		Disabled			
			Disabled			
Loop Protection	5		Disabled			
 Spanning Tree MVR 	7		Disabled			
IPMC	8		Disabled			
LLDP	9		Disabled	-	-	
• PoE	10		Disabled	-	-	
MAC Table	11		Disabled		•	
VLANs -	12		Disabled		-	
	13		Disabled		-	
	14		Disabled Disabled		•	
	15		Disabled			
	17		Disabled			
	18		Disabled			
	19		Disabled			
	20		Disabled			
	21		Disabled			
	22		Disabled			
	23		Disabled	-	-	
	24		Disabled			
	1 24		Disabled	-		
	25		Disabled	-		

User Module Legend

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

User Module Name

The full name of a module that may request Port Security services.

Abbr

A one-letter abbreviation of the user module. This is used in the Users column in the port status table.

Port Status

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

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 <u>Abbr</u>) has enabled port security.

State

Shows the current state of the port. It can take one of four values:

Disabled: No user modules are currently using the Port Security service.

Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.

Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in. Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.

MAC Count (Current, Limit)

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

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh : Click this box to enable an automatic refresh of the page at regular intervals.

Port Security Port Status

This page 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.

Gener,	ALL8944WMP - Gigabit PoE Switch		C	} 📀
Configuration Monitor System Ports Security Access Management Statistics Network Port Security Accuss Network Port Security Notion Port Port	Port Security Port Status Port 1 MAC Address VLAN ID State Time of Addition Age/Hold No MAC addresses attached	Pott 1 Port 2 Port 3 Port 4 Port 5 Port 6 Port 7 Port 8 Port 9 Port 10 Port 10 Port 11 Port 12 Port 13 Port 14 Port 13 Port 14 Port 12 Port 13 Port 14 Port 12 Port 13 Port 14 Port 12 Port 12 Port 12 Port 12 Port 12 Port 22 Port 23 Port 24 Port 24 Port 26 Port 26 Port 24 Port 26 Port 24 Port 26 Port 24 Port 26 Port 24 Port 26 Port 26 Port 26 Port 27 Port 27 Port 26 Port 27 Port 26 Port 27 Port 26 Port 27 Port 26 Port 27 Port 27 Port 27 Port 26 Port 27 Port 26 Port 27 Port 27 Port 27 Port 26 Port 27 Port 26 Port 27 Port 26 Port 27 Port 26 Port 26 Port 26 Port 27 Port 26 Port 26 Por	Auto-refresh	Refresh

MAC Address & VLAN ID

The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating *"No MAC addresses attached"* is displayed.

State

Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.

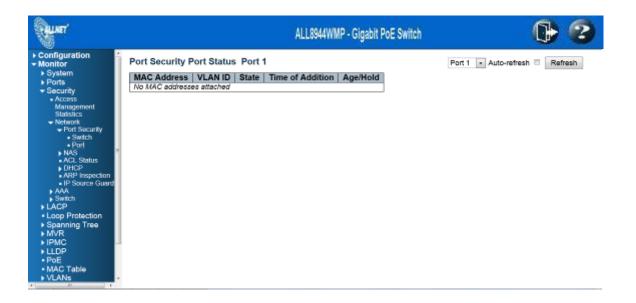
Time of Addition

Shows the date and time when this MAC address was first seen on the port.

Age/Hold

If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin.

If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.



Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh : Click this box to enable an automatic refresh of the page at regular intervals.

Security / Network / NAS

nfiguration	1.000				organi	PoE Switch			
nitor	Netwo	ork Access Serv	er Switch Statu	s				Auto-refresh	Refresh
System Ports	Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN	ID	
Security	1	Force Authorized	Globally Disabled						
Access	2	Force Authorized	Globally Disabled						
Management	3	Force Authorized	Globally Disabled						
Slatsacs	4	Force Authorized	Globally Disabled						
Network	5	Force Authorized	Globally Disabled						
Port Security	6	Force Authorized							
	Z	Force Authorized	Globally Disabled						
Switch	8	Force Authorized							
Port	9	Force Authorized	Globally Disabled					~	
ACL Status DHCP	10	Force Authorized							
ARP Inspection	11	Force Authorized	Globally Disabled						
. IP Source Guard	12	Force Authorized	Globally Disabled						
AAA	13	Force Authorized							
Switch	14	Force Authorized							
ACP	15	Force Authorized						-	
oop Protection	16	Force Authorized							
panning Tree	17	Force Authorized	Globally Disabled						
VR	18	Force Authorized	Globally Disabled						
MC	19	Force Authorized	Globally Disabled						
LDP	20	Force Authorized							
oE	21	Force Authorized	Globally Disabled						
AC Table	22	Force Authorized							
LANs -	23	Force Authorized							
LONING CONTRACT	24 25	Force Authorized							
	25	Force Authorized	Globally Disabled Globally Disabled						

This page provides an overview of the current NAS port states.

Port

The switch port number. Click to navigate to detailed NAS statistics for this port.

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. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh : Click this box to enable an automatic refresh of the page at regular intervals.

This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only.

Use the port select box to select which port details to be displayed.



Port State

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.

QoS Class

The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.

Port VLAN ID

The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Port Counters

EAPOL Counters

These supplicant frame counters are available for the following administrative states:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

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

Backend Server Counters

These backend (RADIUS) frame counters are available for the following administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

		Backend Server Counters	
Direction	Name	IEEE Name	Description
			802.1X-based:
			Counts the number of
			times that the switch
			receives the first
			request from the
			backend server
			following the first
			response from the
			supplicant. Indicates
Rx	A		that the backend
	Access Challenges	dot1xAuthBackendAccessChallenges	server has
			communication with
			the switch.
			MAC-based:
			Counts all Access
			Challenges received
			from the backend
			server for this port
			(left-most table) or
			client (right-most
			table).
			802.1X-based:
			Counts the number of
			times that the switch
By	Other	data v Auth Daalvand Othar Dagu aata Ta Cupplican	sends an EAP
Rx	Requests	dot1xAuthBackendOtherRequestsToSupplicant	Request packet
			following the first to the
			supplicant. Indicates
			that the backend

			server chose an
			EAP-method.
			MAC-based:
			Not applicable.
			802.1X- and
			MAC-based:
			Counts the number of
			times that the switch
	Auth.		receives a success
Rx	Successes	dot1xAuthBackendAuthSuccesses	indication. Indicates
	040000000		that the
			supplicant/client has
			successfully
			authenticated to the
			backend server.
			802.1X- and
			MAC-based:
			Counts the number of
			times that the switch
Rx	Auth. Failures	dot1xAuthBackendAuthFails	receives a failure
			message. This
			indicates that the
			supplicant/client has
			not authenticated to
			the backend server.
			802.1X-based:
			Counts the number of
			times that the switch
			attempts to send a
			supplicant's first
			response packet to the
Тх	Responses	dot1xAuthBackendResponses	backend server.
			Indicates the switch
			attempted
			communication with
			the backend server.
			Possible
			retransmissions are

not counted.
MAC-based:
Counts all the backend
server packets sent
from the switch
towards the backend
server for a given port
(left-most table) or
client (right-most
table). Possible
retransmissions are
not counted.

Last Supplicant/Client Info

Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

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

Not applicable.

Selected Counters

Selected Counters

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

- Multi 802.1X
- MAC-based Auth.

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

Attached MAC Addresses

Identity

Shows the identity of the supplicant, as received in the Response Identity EAPOL frame.

Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows *No supplicants attached*.

This column is not available for MAC-based Auth.

MAC Address

For Multi 802.1X, this column holds the MAC address of the attached supplicant.

For MAC-based Auth., this column holds the MAC address of the attached client.

Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows *No clients attached*.

VLAN ID

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

State

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

Last Authentication

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

FRIMET'	ALL	ALL8944WMP - Gigabit PoE Switch			
Configuration Monitor Source Source	NAS Statistics Port 1 Port State Port State Globally Disabled	Port 1 Auto-refresh Refree Port 2 Port 2 Port 3 Port 4 Port 5 Port 6 Port 7 Port 8 Port 9 Port 10 Port 10 Port 11 Port 12 Port 13 Port 15 Port 15 Port 15 Port 15 Port 16 Port 17 Port 12 Port 13 Port 18 Port 19 Port 20 Port 21 Port 22 Port 23 Port 24 Port 25 Port 25 Port 25 Port 26 Port 25 Port 26 Port 25 Port 26 Port 26 Po	sh		

Buttons

The port select box determines which port is affected when clicking the buttons.

Auto-refresh

Check this box to enable an automatic refresh of the page at regular intervals.

Click to refresh the page immediately.

This button is available in the following modes:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X

Click to clear the counters for the selected port.

This button is available in the following modes:

- Multi 802.1X
- MAC-based Auth.X

Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however.

This button is available in the following modes:

- Multi 802.1X
- MAC-based Auth.X

Click to clear only the currently selected client's counters.

ACL Status

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is **256**on each switch.

RUNT'	ALL8944WMP - Gigabit PoE Switch								2	
Configuration Monitor	ACL Status					Combi	ned	- Auto-n	afresh 🗆 🖡	Refresh
 System Ports Security 	User Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter	Conflict
Access Management Statistics Network Port Socurity NAS Switch NCL Status DitCP ARP Inspection IPCP ARP Inspection IPCP Loop Protection Spanning Tree MVR IPMC LLDP DoE	No entries									

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 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:

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.

GUNT		1	ALL8944WMP - Gigabit PoE Si	witch	🕞 😨
Configuration Monitor System Ports Security Security Access Management Statistics Network Port Socurity NAS Switch Port ACC, Status DHCP AAA Switch LACP Loop Protection Spanning Tree MVR LLDP PoE MVR MC Table	ACL Status User Port No entries	Frame Action	Rate Port Limiter Redirect		Counter Conflict

Buttons

: Select the ACL status from this drop down list.

Refresh: Click to refresh the page immediately.

Auto-refresh : Click this box to enable an automatic refresh of the page at regular intervals.

DHCP Snooping Statistics

This page provides statistics for DHCP snooping. The statistics show only packet counters when DHCP snooping mode is enabled and relay mode is disabled. And it doesn't count the DHCP packets for DHCP client.

9			ALL8944WMP - Gigabi			
onfiguration 4	DHCP Snooping Port Statis	tics	Port 1		Port 1 · Auto-refresh	Refresh Clear
System Ports	Receive Packets		Transmit Packets			
Security	Rx Discover	0	Tx Discover	0		
Access	Rx Offer	0	Tx Offer	0		
Management	Rx Request	0	Tx Request	0		
Statistics	Rx Decline	0	Tx Decline	0		
- Network	Rx ACK	0	Tx ACK	0		
Port Security	Rx NAK	0	Tx NAK	0		
NAS	Rx Release	0	Tx Release	0		
ACL Status DHCP	Rx Inform	0	Tx Inform	0		
Shooping	Rx Lease Query	0	Tx Lease Query	0		
Statistics	Rx Lease Unassigned	0	Tx Lease Unassigned	0		
 Relay 	Rx Lease Unknown	0	Tx Lease Unknown	0		
Statistics	Rx Lease Active	0	Tx Lease Active	0		
 ARP Inspection 						
 IP Source Guard 						
> AAA > Switch						
LACP						
Loop Protection						
Spanning Tree						
MVR						
IPMC						

Receive and Transmit Packets

Rx and Tx Discover

The number of discover (option 53 with value 1) packets received and transmitted.

Rx and Tx Offer

The number of offer (option 53 with value 2) packets received and transmitted.

Rx and Tx Request

The number of request (option 53 with value 3) packets received and transmitted.

Rx and Tx Decline

The number of decline (option 53 with value 4) packets received and transmitted.

Rx and Tx ACK

The number of ACK (option 53 with value 5) packets received and transmitted.

Rx and Tx NAK

The number of NAK (option 53 with value 6) packets received and transmitted.

Rx and Tx Release

The number of release (option 53 with value 7) packets received and transmitted.

Rx and Tx Inform

The number of inform (option 53 with value 8) packets received and transmitted.

Rx and Tx Lease Query

The number of lease query (option 53 with value 10) packets received and transmitted.

Rx and Tx Lease Unassigned

The number of lease unassigned (option 53 with value 11) packets received and transmitted.

Rx and Tx Lease Unknown

The number of lease unknown (option 53 with value 12) packets received and transmitted.

Rx and Tx Lease Active

The number of lease active (option 53 with value 13) packets received and transmitted.

LINET'			ALL8944WMP - Gigabit P	oE Swi	itch	
nfiguration 4 nitor	DHCP Snooping Port Statis	stics	Port 1		Port 1 • Auto-refresh	Refresh Clear
System Ports	Receive Packets		Transmit Packets		Port 1 Port 2	
Security	Rx Discover	0	Tx Discover	0	Port 3	
Access	Rx Offer	0	Tx Offer	0	Port 4	
Management	Rx Request	0	Tx Request	0	Port 5	
Statistics	Rx Decline	0	Tx Decline	0	Port 6	
- Nebwork	Rx ACK	0	TX ACK	0	Port 7	
Port Security	Rx NAK	0	Tx NAK	0	Port 8	
▶ NAS	Rx Release	0	Tx Release	0	Port 9	
 ACL Status 	Rx Inform	0	Tx Inform	0	Port 10	
➡ DHCP	Rx Lease Query	0	Tx Lease Query	0	Port 11	
 Snooping Statistics 	Rx Lease Unassigned	0	Tx Lease Unassigned	0	Port 12	
Relay	Rx Lease Unknown	0	Tx Lease Unknown	0	Port 13	
Statistics	Rx Lease Active	0	Tx Lease Active	0	Port 14	
ARP Inspection					Port 15	
 IP Source Guard 					Port 16	
AAA					Port 17	
Switch					Port 18	
ACP					Port 19	
oop Protection					Port 20	
panning Tree					Port 21	
ÍVR					Port 22	
PMC					Port 23	
LDP					Port 24	
PoE					Port 25	

Buttons

Auto-refresh : Click this box to enable an automatic refresh of the page at regular intervals.

Refresh: Click to refresh the page immediately.

Clear : Clears the counters for the selected port.

DHCP Relay Statistics

This page provides statistics for DHCP relay.

		ALL8944W	MP - Gigabit Pol	Switch		(▶ 📀
DHCP Relay Statistic Server Statistics	s				Auto-refresi	n 🗆 🛛 Refres	h Clear
Transmit to Server	Receive from Server		Missing Circuit I	Missi Remot	ng eID C	Bad Circuit ID	Receive Bad Remote ID
Client Statistics	Receive	Receive	Replace	Keep	Drop		
to Client Error	from Client 0	Agent Option 0	Agent Option 0	Agent Option 0	Agent Op	otion 0	
	Server Statistics Transmit to Server 0 0 Client Statistics Transmit to Client Transmit Error	Transmit to Server Transmit Error Receive from Server 0 0 0 Client Statistics Transmit to Client Receive From Client	DHCP Relay Statistics Server Statistics Transmit to Transmit from Missing Server 0 0 0 Client Statistics Transmit Transmit Receive Receive to Client Error from Client Agent Option	DHCP Relay Statistics Server Statistics Transmit to Transmit from Server Receive Missing Agent Option Receive III 0 0 0 0 0 Client Statistics Transmit Transmit Receive Receive Agent Option Replace Agent Option	Server Statistics Transmit to Transmit from Receive from Receive Missing Missing </th <th>DHCP Relay Statistics Auto-refrest Server Statistics Transmit to from Server Receive Missing Missing Missing Circuit ID Receive Missing Circuit ID 0 0 0 0 0 0 Client Statistics Transmit Transmit Receive Receive Agent Option Remote ID O</th> <th>DHCP Relay Statistics Auto-refresh Refrest Server Statistics Transmit to grow Server Receive from Server Receive Missing Agent Option Receive Missing Circuit ID Receive Bad Circuit ID Receive ID Receive ID 0 0 0 0 0 0 0 0 Client Statistics Transmit Transmit Transmit Receive Agent Option Replace Agent Option Keep Agent Option Drop Agent Option</th>	DHCP Relay Statistics Auto-refrest Server Statistics Transmit to from Server Receive Missing Missing Missing Circuit ID Receive Missing Circuit ID 0 0 0 0 0 0 Client Statistics Transmit Transmit Receive Receive Agent Option Remote ID O	DHCP Relay Statistics Auto-refresh Refrest Server Statistics Transmit to grow Server Receive from Server Receive Missing Agent Option Receive Missing Circuit ID Receive Bad Circuit ID Receive ID Receive ID 0 0 0 0 0 0 0 0 Client Statistics Transmit Transmit Transmit Receive Agent Option Replace Agent Option Keep Agent Option Drop Agent Option

Server Statistics

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.

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.

Buttons

Auto-refresh : Click this box to enable an automatic refresh of the page at regular intervals.Refresh: Click to refresh the page immediately.Clear : Clears statistics.

Dynamic ARP Inspection Table

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

Navigating the ARP Inspection Table

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

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

The 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.

Report	ALL8944WMP - Gigabit Po	1	
Configuration Monitor Siystem Ports Security Access Management Statistics Natwork Port Security NAS ACL Status DHCP AAP Inspection IP Source Guard AAA Switch LACP	Dynamic ARP Inspection Table Start from Port 1 • , VLAN 1 . , MAC address per page. Port VLAN ID MAC Address IP Address No more entries	Auto-refresh E Refre	sh i< >> with 20 entries

ARP Inspection Table Columns

Port

Switch Port Number for which the entries are displayed.

illunt'	Port Port Port Port Port Port Port Port		ALL8	144WMP - Gigabit Po	DE Switch	0 2
onfiguration	Dynami(Port	11 pection Table	•		Auto-refresh 🗏 📗	Refresh << >>
System Ports Security • Access	Start from Port 1 per page. Port 1 Port 1	13 , VLAN 1 14	, MAC address	00-00-00-00-00	and IP address 0.0.0.0	with 20 entries
Management Statistics • Network • Not Socurity • NAS • ACL Status • DHCP • ARP Inspection • IP Source Guard • ANA • Smitch LACP Loop Protection	Port V Port Port Port Port Port Port Port Port	more entries	IP Address			
oop Protection ipanning Tree MR PMC LDP NC MAC Table MAC Table MANs /CL Flow						

VLAN ID

VLAN-ID in which the ARP traffic is permitted.

MAC Address

User MAC address of the entry.

IP Address

User IP address of the entry.

Buttons

Auto-refresh : Click this box to enable an automatic refresh of the page at regular intervals.

Refresh: Click to refresh the page immediately.

Clear : Flushes all dynamic entries.

/<< : Updates the table starting from the first entry in the Dynamic ARP Inspection Tables.

>> : Updates the table, starting with the entry after the last entry currently displayed.

Dynamic IP Source Guard Table

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

FRUMET '	ALL8944WMP - Gigabit PoE Swi	tch 🚯 😨
Configuration Monitor System Ports Security Access Management Statistics Network Port Socurity NAS AAS ACL Status DHCP AAA Switch LACP Loop Protection Spanning Tree MMC Table VCL MAC Table VLANs VCL sElow	Dynamic IP Source Guard Table Start from Port 1 . , VLAN 1 and IP address 0.0.0 with 3 Port VLAN ID IP Address MAC Address No more entries	Auto-refresh

Navigating the IP Source Guard Table

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

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

The 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.

IP Source Guard Table Columns

Salant,	Port 2 Port 2 Port 3 Port 6 Port 6 Port 6 Port 8 Port 9		ALL89	44WMP - Gigabil	l PoE Switch	0 🕄
Configuration Monitor System Ports Coccurity Access Management Statistics Network Port Security NAS ACL Status DHCP ARP Inspecton AAA Switch LACP Loop Protection Spanning Tree MVR IPMC LDP LOOP MAC Table VCL sElow VCL	Port 10 Dynam Port 11 Port 12 Start from Port 14 Port 14 Port 14 Port 14 Port 14 Port 16 Port 16 Port 17 Port 18 Port 19 Port 21 Port 22 Port 22 Port 22 Port 25 Port 26	ce Guard Tat	and IP address	0.0.0	with 20	Auto-refresh Refresh I<< >> entries per page.

Port

Switch Port Number for which the entries are displayed.

VLAN ID

VLAN-ID in which the IP traffic is permitted.

IP Address

User IP address of the entry.

MAC Address

Source MAC address.

Buttons

Auto-refresh: Click this box to enable an automatic refresh of the page at regular intervals.

Refresh: Click to refresh the page immediately.

Clear: Flushes all dynamic entries.

I<<: Updates the table starting from the first entry in the Dynamic IP Source Guard Tables.

>>: Updates the table, starting with the entry after the last entry currently displayed.

RADIUS Authentication Overview

This page provides an overview of the status of the RADIUS servers configurable on the Authentication configuration page.

RELINET'		ALL894	W
Configuration Monitor	RADIUS Authentication	on Server Status Overvi	9
System Ports Socurity Access Management Statistics Network AAA RADIUS Overview RADIUS Details	# IP Address 1 0.0.0.01812 2 0.0.0.01812 3 0.0.0.01812 4 0.0.001812 5 0.0.001812 5 0.0.001812 5 0.0.001812 2 0.0.001812	Status Disabled Disabled Disabled Disabled Disabled Server Status Overview	
Switch LACP	# IP Address	Status	
Loop Protection Spenning Tree	1 0.0.0.0:1813 2 0.0.0:0:1813	Disabled Disabled	
 Spanning Tree MVR 	3 0.0.0.0:1813	Disabled	
▶ IPMC	<u>4</u> 0.0.0.0:1813	Disabled	
LLDP PoE	<u>5</u> 0.0.0.0:1813	Disabled	_
MAC Table			
VLANs ▶ VCL			
• sFlow			
Diagnostics			

RADIUS Authentication Servers

#

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.

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

#

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.

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 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.

Buttons

Auto-refresh : Click this box to enable an automatic refresh of the page at regular intervals. Refresh: Click to refresh the page immediately.

RADIUS Authentication Statistics

This page provides detailed statistics for a particular RADIUS server.

- ALMET		• •			
Configuration Monitor	RADIUS Authentication Statist	ics for	Server #1	Server #1 -	Auto-refresh 🛛 Refresh Clear
System	Receive Packets		Transmit Packe	Server #1	
Ports	Access Accepts	0	Access Requests	Server #2	
 Security 	Access Rejects	ŏ	Access Retransmissions	Server #3	
 Access Management 	Access Challenges	ŏ	Pending Requests	Server #4	
Statistics Notwork	Malformed Access Responses	ő	Timeouts	Server #5	
- AAA	Bad Authenticators	ŏ			
RADIUS Overview	Unknown Types	ŏ			
 RADIUS Details 	Packets Dropped	õ			
Switch	T defecto artopped	Othe	r Info		
LACP	IP Address	ound		0.0.0.0:1812	
 Loop Protection 	State			Disabled	
Spanning Tree	Round-Trip Time			0 ms	
MVR	Roand-Trip Time			0110	
▶ IPMC	RADIUS Accounting Statistics	for Se	rver #1		
LLDP					
PoE	Receive Packets		Transmit Packe	Its	
	Responses	0	Requests	0	
 MAC Table 			Retransmissions	D	
	Malformed Responses	0		-	
	Bad Authenticators	0	Pending Requests	ō	
VLANs	Bad Authenticators Unknown Types	0		-	
> VLANs > VCL • sFlow	Bad Authenticators	õ	Pending Requests Timeouts	ō	
VLANs VCL sFlow Diagnostics	Bad Authenticators Unknown Types	õ	Pending Requests	ō	
VLANs VCL SFlow Diagnostics	Bad Authenticators Unknown Types Packets Dropped	õ	Pending Requests Timeouts	ō	
VLANs VCL	Bad Authenticators Unknown Types Packets Dropped	õ	Pending Requests Timeouts	0 D	

RADIUS Authentication Statistics

The statistics map closely to those specified in RFC4668-RADIUS.Authentication Client MIB.

Use the server select box to switch between the backend servers to show details for.

Packet Counters

RADIUS authentication server packet counter. There are seven receive and four transmit counters.

Direction	Name	RFC4668 Name	Description
Rx	Access Accepts	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	Access Rejects	radiusAuthClientExtAccessRejects	The number of RADIUS

			Access-Reject
			packets (valid or
			invalid) received from
			the server.
			The number of
			RADIUS
Rx	Access Challenges	radiusAuthClientExtAccessChallenges	Access-Challenge
	-		packets (valid or
			invalid) received
			from the server.
			The number of
			malformed RADIUS
			Access-Response
			packets received
			from the server.
			Malformed packets
			include packets
			with an invalid
Rx	Malformed Access Responses	radiusAuthClientExtMalformedAccessResponses	length. Bad
			authenticators or
			Message
			Authenticator
			attributes or
			unknown types are
			not included as
			malformed access
			responses.
			The number of
			RADIUS
			Access-Response
			packets containing
Rx	Bad	radiusAuthClientExtBadAuthenticators	invalid
	Authenticators		authenticators or
			Message
			Authenticator
			attributes received
			from the server.
Rx	Unknown Types	radiusAuthClientExtUnknownTypes	The number of

			RADIUS packets
			that were received
			with unknown types
			from the server on
			the authentication
			port and dropped.
			The number of
			RADIUS packets
			that were received
Rx	Poekete Drenned	Padius Auth Client Ext Deskets Dropped	from the server on
KX.	Packets Dropped	Radius Auth Client Ext-Packets Dropped	the authentication
			port and dropped
			for some other
			reason.
			The number of
			RADIUS
	Access Requests		Access-Request
Тх		Radius AuthClientExtAccess Requests	packets sent to the
			server. This does
			not include
			retransmissions.
			The number of
			RADIUS
			Access-Request
Tx	Access	radiusAuthClientExtAccessRetransmissions	packets
	Retransmissions		retransmitted to the
			RADIUS
			authentication
			server.
			The number of
			RADIUS
			Access-Request
_	Pending		packets destined
Tx	Requests	radiusAuthClientExtPendingRequests	for the server that
			have not yet timed
			out or received a
			response. This
			variable is

	1		
			incremented when
			an Access-Request
			is sent and
			decremented due to
			receipt of an
			Access-Accept,
			Access-Reject,
			Access-Challenge,
			timeout, or
			retransmission.
			The number of
			authentication
			timeouts to the
			server. After a
			timeout, the client
			may retry to the
			same server, send
			to a different server,
Тх	Timeouts	radiusAuthClientExtTimeouts	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
		Shows the state of the server. It takes one of the
		following values:
		Disabled: The selected server is disabled.
State	-	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.				
		The time interval (measured in milliseconds)				
		between the most recent				
		Access-Reply/Access-Challenge and the				
Round-Trip Time		Access-Request that matched it from the RADIUS				
Round-mp mile	Radius AuthClientExtRoundTripTime	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

The statistics map closely to those specified in RFC4670-RADIUS.Accounting Client MIB.

Use the server select box to switch between the backend servers to show details for.

Renner'			6	2			
Configuration Monitor	RADIUS Authentication Statist	Auto-refresh	Refresh Clear	ı î			
System	Receive Packets		Transmit Packet	Server #1 Server #2			
 Ports Security 	Access Accepts	0	Access Requests	Server #3			
 Access Management 	Access Rejects	0	Access Retransmissions	Server #4			
Statistics	Access Challenges	0	Pending Requests	Server #5			
Notwork	Malformed Access Responses	0	Timeouts	U U			
÷ AAA	Bad Authenticators	0					
 RADIUS Overview 	Unknown Types	0					
 RADIUS Details 	Packets Dropped	0	r Info				
 Switch 							
+ LACP	IP Address						
 Loop Protection 	State			Disabled			
 Spanning Tree 	Round-Trip Time						
MVR							
▶ IPMC	RADIUS Accounting Statistics	for Se	rver #1				
LLDP PoE	Receive Packets		Transmit Packet	e	1		
	Responses	0	Requests	0			
MAC Table VLANs	Malformed Responses	ŏ	Retransmissions	ő			
	Bad Authenticators	ő	Pending Requests	ő			
VCL	Unknown Types	ő	Timeouts	ő			
sFlow	Packets Dropped	õ		-			
Diagnostics	T dollers ar opped	Othe	r Info				
Maintenance	IP Address	June		0.0.0.0:1813			
	State			Disabled			
	Round-Trip Time			0 ms			

Packet Counters

RADIUS accounting server packet counter. There are five receive and 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	radiusAccClientExtMalformedResponses	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.
Rx	Bad Authenticators	radiusAcctClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	Unknown Types	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	Packets Dropped	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Тх	Requests	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Тх	Retransmissions	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.

Тх	Pending Requests	radiusAccClientExtPendingRequests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response,
			timeout, or retransmission. The number of
			accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different
Тх	Timeouts	radiusAccClientExtTimeouts	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
		Shows the state of the server. It takes one of the
		following values:
		Not Ready:
		Disabled : The selected server is disabled.
State		Not Ready: The server is enabled, but IP
State	-	communication is not yet up and running.
		aReady: 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.
		The time interval (measured in milliseconds)
		between the most recent Response and the
		Request that matched it from the RADIUS
Round-Trip Time	radiusAccClientExtRoundTripTime	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.

Buttons

The server select box determines which server is affected by clicking the buttons.

Auto-refresh : Click this box to enable an automatic refresh of the page at regular intervals.

Refresh: Click to refresh the page immediately.

Clear : Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operations..

Switch / SNMP / RMON / Statistics

RMON Statistics Overview

This page provides an overview of RMON statistics entries.

The displayed counters are:

Report'	ALL8944WMP - Gigabit PoE Switch										2								
Configuration Monitor System		ON Statist			rview		rian oar r				Auto-refre	osh 🗆 🛛	Refresh	n <<	>>				
Ports Security Access Management		Data				Broad	ries per p Multi	CRC	Under	Over	-			64	65	128	256	512	1024
Statistics Network AAA Switch	ID No i	Source (ifIndex) more entries		Octets	Pkts	cast	cast	Errors	size	size	Frag.	Jabb.	Coll.	Bytes	127	255	511	1023	1588
RMON Statistics History																			
Alam Event LACP																			
Loop Protection Spanning Tree MVR																			

Data Source

The port ID which wants to be monitored.

Drop

The total number of events in which packets were dropped by the probe due to lack of resources.

Octets

The total number of octets of data (including those in bad packets) received on the network.

Pkts

The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broad-cast

The total number of good packets received that weredirected to the broadcast address.

Multi-cast

The total number of good packets received that were directed to a multicast address.

CRC Errors

The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets.

Under-size

The total number of packets received that were less than 64 octets.

Over-size

The total number of packets received that were longer than 1518 octets.

Frag.

The number of frames which size is less than 64 octets received with invalid CRC.

Jabb.

The number of frames which size is larger than 64 octets received with invalid CRC.

Coll.

The best estimate of the total number of collisions on this Ethernet segment.

64

The total number of packets (including bad packets) received that were 64 octets in length.

65~127

The total number of packets (including bad packets) received that were between 65 to 127 octets in length.

128~255

The total number of packets (including bad packets) received that were between 128 to 255 octets in length.

256~511

The total number of packets (including bad packets) received that were between 256 to 511 octets in length.

512~1023

The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.

1024~1588

The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh : Click this box to enable an automatic refresh of the page at regular intervals.

RMON History Overview

This page provides an overview of RMON history entries.

The displayed fields are:

BLAET

ALL8944WMP - Gigabit PoE Switch



					Pol	E Gig	jaBit E	ther	net Sw	/itch				6	2
Configuration Monitor System Ports		istory Ov Control Inde		and Si	ample Inde	ix 0	with	20	entries p	Auto-refi er page.	resh 🗆	Refres	h <<	>>	
Security Access Management Statistics Network AAA	History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad - cast	Multi cast	CRC Errors	Under size	Over size	Frag.	Jabb.	Coll.	Utilization
Switch RMON Statistics History	No more o	entries													
Alarm Event LACP Loop Protection															
Spanning Tree MVR IPMC LLDP															
PoE MAC Table VLANs															
VCL sFlow Diagnostics Maintenance															

History Index

Indicates the index of History control entry.

Sample Index

Indicates the index of the data entry associated with the control entry

Sample Start

The total number of events in which packets were dropped by the probe due to lack of resources.

Drops

The total number of events in which packets were dropped by the probe due to lack of resources.

Octets

The total number of octets of data (including those in bad packets) received on the network.

Pkts

The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broadcast

The total number of good packets received that were directed to the broadcast address.

Multicast

The total number of good packets received that were directed to a multicast address.

CRCErrors

The total number of packets received that had a length (excluding framing bits, but including FCS octets) of

between 64 and 1518 octets.

Undersize

The total number of packets received that were less than 64 octets.

Oversize

The total number of packets received that were longer than 1518 octets.

Frag.

The number of frames which size is less than 64 octets received with invalid CRC.

Jabb.

The number of frames which size is larger than 64 octets received with invalid CRC.

Coll.

The best estimate of the total number of collisions on this Ethernet segment.

Utilization

The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh : Click this box to enable an automatic refresh of the page at regular intervals.

RMON Alarm Overview

This page provides an overview of RMON alarm entries.

The displayed fields are:

Configuration Configuration Configuration Configuration Configuration Configuration System Port Statistics Overview System Port Statistics Overview Substation Statistics Statistics Statistics Notwork System Control Index 0 With 20 entries per page. Statistics Statistics Notwork Control Index 0 With 20 entries per page. Statistics Statistics Notwork System Control Index 0 With 20 entries per page. Statistics Statistics Notwork Control Index 0 With 20 entries per page. Statistics Statistics Notwork System Control Index 0 With 20 entries per page. Statistics Notwork Statistics Statistics Notwork Control Index 0 With 20 entries per page. Statistics Stat	-RLAT'		LL8944WMP - Gigabit PoE Switc	ð -	1
PoE MAC Table	Monitor System System Ports Security Access Management Statistics Notwork AAA Switch KAA Switch KAA Switch AAA Switch AAA Switch Latary Loop Protection Spanning Tree MVR IPMC LLDP PoE	Port Statistics Overview Start from Control Index 0 with 20 ID Interval Variable Sample Type Value	entries per page. Startup Rising Rising	Auto-refresh E Refree	ah << >>

ID

Indicates the index of Alarm control entry.

Interval

Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

Variable

Indicates the particular variable to be sampled

Sample Type

The method of sampling the selected variable and calculating the value to be compared against the

thresholds, posible sample types are:

Rising Threshold

Rising threshold value.

Rising Index

Rising event index.

Falling Threshold

Falling threshold value.

Falling Index

Falling event index.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh : Click this box to enable an automatic refresh of the page at regular intervals.

RMON Event Overview

This page provides an overview of RMON event entries.

The displayed fields are:

RELINET'		ALL8944WMP -	Gigabit PoE Switch	🕞 🕑 😨)
 Configuration Monitor System Ports Security Access Management Statistics Network AAA Smitch RMON Statistics History Alarm Event LACP Loop Protection Spanning Tree MAC Table VLANs VCL sFlow Diagnostics Maintenance 	Event Overview Start from Control Index 0 Event Index LogIndex LogTime No more entries	and Sample Index 0	with 20 entries	Auto-refresh Refresh <>>	

Event Index

Indicates the index of the event entry.

Log Index

Indicates the index of the log entry.

Log Time

Indicates Event log time

Log Description

Indicates the Event description.

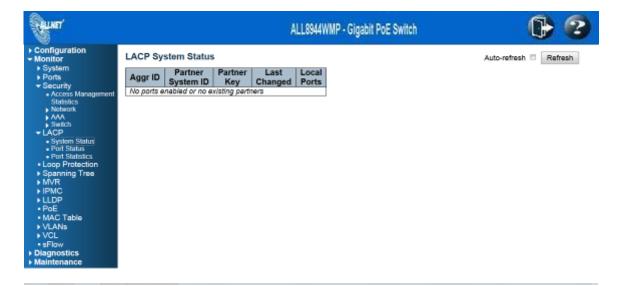
Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh : Click this box to enable an automatic refresh of the page at regular intervals.

LACP System Status

This page provides a status overview for all LACP instances.



Aggr ID

The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'

Partner System ID

The system ID (MAC address) of the aggregation partner.

Partner Key

The Key that the partner has assigned to this aggregation ID.

Last changed

The time since this aggregation changed.

Local Ports

Shows which ports are a part of this aggregation for this switch.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh : Click this box to enable an automatic refresh of the page at regular intervals.

LACP Port Status

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

26 No - - - -

RUNET'						ALL8944WI	IP - Gigabit Po	E Switch		1
Configuration Monitor	LAC	P Status							Auto-refresh 🗖	Refresh
 System Ports 	Port	LACP	Key	Aggr ID	Partner System ID	Partner Port			_	
Security LACP		No			-					
System Status		No								
Port Status	3					-				
 Port Statistics 	4			-		-				
Loop Protection		5 No				-				
Spanning Tree	6	5 No								
MVR IPMC	7	No	-	-	-	-				
> LLDP	8	8 No	-	-	-	-				
• PoE	8	No No	-	-	-	-				
 MAC Table 	10) No	-	-	-	-				
▶ VLANs	11		-	-	-	-				
VCL	12	No No	-	-	-	-				
 sFlow 	13		-	-	-	-				
Diagnostics	14		-	-	-	-				
Maintenance	16			-		-				
	16		-	-	-	-				
	17		-	-	-	-				
	18		-	-	-	-				
	19									
	20									
	21									
	22		-		-	-				
	23		-	-	•	-				
	24		-	-		-				

- ALINET				AL	L18944W	MP - Gigabit PoE Switch	0
Configuration Monitor	LACP St	atistics					Auto-refresh 🗏 Refresh Ci
System Ports Security		LACP eceived	LACP Transmitted	Discare Unknown			
- LACP	1	0	0	0	0		
 System Status 	2	0	0	0	0		
Port Status	3	0	0	0	0		
 Port Statistics 	4	0	0	0	0		
Loop Protection	5	0	0	0	0		
Spanning Tree	6	0	0	0	0		
MVR	7	0	0	0	0		
IPMC	8	0	0	0	0		
LLDP	9	0	0	0	0		
PoE	10	0	0	0	0		
MAC Table	11	0	0	0	0		
VLANs	12	0	0	0	0		
VCL	13	0	0	0	0		
sFlow	14	0	0	0	0		
lagnostics	15	0	0	0	0		
laintenance	16	0	0	0	0		
annenance	17	0	0	0	0		
	18	0	0	0	0		
	19	0	0	0	0		
	20	0	0	0	0		
	21	0	0	0	0		
	22	0	0	0	0		
	23	0	0	0	0		
	24	0	0	0	0		
	25	0	0	0	0		
	26	0	0	0	0		

Port

The switch port number.

LACP

'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.

Key

The key assigned to this port. Only ports with the same key can aggregate together.

Aggr ID

The Aggregation ID assigned to this aggregation group.

Partner System ID

The partner's System ID (MAC address).

Partner Port

The partner's port number connected to this port.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh : Click this box to enable an automatic refresh of the page at regular intervals.

LACP statistics

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

Relief				Al	LL8944W	NP - Gigabit PoE Switch	• • •
Configuration Monitor	LACP	Statistics					Auto-refresh 🗉 Refresh Clear
 System 		LACP	LACP	Discan	ded		
 Ports 	Port	Received	Transmitted				
Security		0	0	0	0		
 LACP System Status 	2	0	0	0	0		
 Port Status 	3	Ő	Ő.	0	0		
Port Statistics	4	0	0	0	0		
 Loop Protection 	5	0	0	0	0		
Spanning Tree	6	0	0	0	0		
MVR	7	0	0	0	0		
► IPMC	8	0	0	0	0		
► LLDP	9	0	0	0	0		
• PoE	10	0	0	0	0		
 MAC Table 	11	0	0	0	0		
▶ VLANs	12	0	0	0	0		
▶ VCL	13	0	0	0	0		
 sFlow 	14	0	0	0	0		
Diagnostics	15	0	0	0	0		
Maintenance	16	0	0	0	0		
	17	0	0	0	0		
	18	0	0	0	0		
	20	0	0	0	0		
	20	0	ő	0	ő		
	22	ő	ő	ő	0		
	23	ŏ	ő	ő	ŏ		
	24	ŏ	ő	ő	ŏ		
	25	ŏ	ő	ŏ	ŏ		
	26	ŏ	ő	ő	Ő		

Port

The switch port number.

LACP Received

Shows how many LACP frames have been received at each port.

LACP Transmitted

Shows how many LACP frames have been sent from each port.

Discarded

Shows how many unknown or illegal LACP frames have been discarded at each port.

Buttons

Auto-refresh: Click this box to enable an automatic refresh of the page at regular intervals.

Refresh: Click to refresh the page immediately.

Clear : Clears the counters for all ports.

STP Bridge Status

This page provides a status overview of all STP bridge instances.

The displayed table contains a row for each STP bridge instance, where the column displays the following information:

FRUNET'			ALL8944WM	IP - Gig	abit Pol	E Switch		1
Configuration Monitor	STP B	ridges					A	uto-refresh 🗏 Refresh
System Ports	MSTI	Bridge ID	Root	Port	Cost	Topology Flag	Topology Change Last	
Security LACP	CIST	80:00-00:01:11:65:74:33	80:00-00:01:11:65:74:33		0	Steady		
 Loop Protection Spanning Tree 								
 Bridge Status Port Status 								
 Port Statistics MVR 								
IPMC LLDP								
PoE MAC Table								
VLANs VCL								
 sFlow 								
Diagnostics Maintenance								

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 is 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 last Topology Change occurred.

Buttons

Refresh : Click to refresh the page immediately.

Auto-refresh \Box : Check this box to enable an automatic refresh of the page at regular intervals.

STP Port Status

This page displays the STP CIST port status for physical ports of the switch.

STP port status is:

- PLINET				ALL	1944WMP - Gigabit PoE Switch	1
Configuration Monitor	STP F	Port Status				Auto-refresh 🗏 Refresh
 System Ports 	Port	CIST Role	CIST State	Uptime	1	
	1	Disabled	Discarding		1	
Security	2	Disabled	Discarding	-		
LACP	3	Disabled	Discarding			
Loop Protection	4	Disabled	Discarding			
Spanning Tree	5	Disabled	Discarding			
 Bridge Status 	6	Disabled	Discarding			
 Port Status Port Statistics 	7	Disabled	Discarding			
MVR	8	Disabled	Discarding	-		
IPMC	9	Disabled	Discarding			
LLDP	10	Disabled	Discarding			
PoE	11	Disabled	Discarding			
MAC Table	12	Disabled	Discarding			
	13	Disabled	Discarding	-		
VLANs	14	DesignatedPort	Forwarding	0d 02:59:38		
VCL	15	Disabled	Discarding			
sFlow	16	Disabled	Discarding	-		
agnostics	17	Disabled	Discarding	-		
aintenance	18	Disabled	Discarding	-		
	19	Disabled	Discarding	-		
	20	Disabled	Discarding	-		
	21	Disabled	Discarding	-		
	22	Disabled	Discarding	-		
	23	Disabled	Discarding	-		
	24	Disabled	Discarding	-		
	25	Disabled	Discarding			
	26	Disabled	Discarding	-		

Port

The switch port number of the logical STP port.

CIST Role

The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort

BackupPort RootPort DesignatedPort Disabled.

CIST State

The current STP port state of the CIST port. The port state can be one of the following values: Discarding

Learning Forwarding.

Uptime

The time since the bridge port was last initialized.

Buttons

Refresh : Click to refresh the page immediately.

Auto-refresh \square : Check this box to enable an automatic refresh of the page at regular intervals.

STP Port Statistics

This page displays the STP port statistics counters of bridge ports in the switch.

The STP port statistics counters are:

Rewer'						A	LL8944W	MP-G	igabit F	PoE Switch			(6
Configuration Monitor	STP S	tatistic	s								А	uto-refresh	Refresh	Clear
 System 	-		Transm	itted			Receiv	/ed		Discar	ded	1		
Ports	Port	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	llegal	1		
 Security LACP 	14	5457	0	0	0	0	0	0	0	0	0	1		
Loop Protection												4		
 Spanning Tree 														
 Bridge Status 														
 Port Status Port Statistics 														
→ MVR														
▶ IPMC														
► LLDP														
• PoE														
MAC Table														
VLANs VCL														
▶ VGL														

Port

The switch port number of the logical STP port.

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.

Buttons

Refresh : Click to refresh the page immediately.

Auto-refresh \square : Check this box to enable an automatic refresh of the page at regular intervals.

MVR Status

This page provides MVR Statistics information.

TRUNET		ALL	8944WMP - Giga	bit PoE Switch		1 2
Configuration Monitor	MVR Statistics				Auto-refresh 🗉	Refresh Clear
System Ports Security LACP	VLAN IGMP/MLD ID Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
Loop Protection Spanning Tree MVR Statistics	No more entrice					
MVR Channel Groups MVR SFM						
Information IPMC LLDP						
PoE MAC Table						

VLAN ID

The Multicast VLAN ID.

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.

Buttons

Refresh : Click to refresh the page immediately.

Clear : Clears all Statistics counters.

Auto-refresh \square : Check this box to enable an automatic refresh of the page at regular intervals.

MVR Group Table

Entries in the MVR Group Table are shown on this page. The MVR Group Table is sorted first by VLAN ID, and then by group.

ALMIT'	ALL8944WMP - Gigs	abit PoE Switch 🚯 😰
Configuration Monitor System Ports Security	MVR Channels (Groups) Information Start from VLAN 1 and Group Address	Auto-refresh Refresh << >> with 20 entries per page.
LACP Loop Protection Spanning Tree Bridge Status Port Status Port Status Port Status WR	Port Me VLAN ID Groups 1 2 3 4 6 6 7 8 9 10 11 12 13	mbers 14 15 16 17 18 19 20 21 22 23 24 25 26
Statistics MVR Channel Groups MVR SFM Information IPMC		

Navigating the MVR Group Table

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

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

The 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.

MVR Group Table Columns

VLAN ID

VLAN ID of the group.

Groups

Group ID of the group displayed.

Port Members

Ports under this group.

Buttons

Auto-refresh \Box : Check this box to enable an automatic refresh of the page at regular intervals.

 $\label{eq:Refresh} \ensuremath{\mathsf{Refreshes}}\xspace \ensuremath{\mathsf{teshes}}\xspace \ensuremath{$

- << : Updates the table starting from the first entry in the MVR Group Table.
- >> : Updates the table, starting with the entry after the last entry currently displayed.

IPMC / IGMP Snooping IGMP Snooping Status

This page provides IGMP Snooping status.

					PoF Gig	aBit Eth	ernet Swi	tch		<u>a</u> 6
Stauner'					ALL ROAMW	MP - Gigabit	PoE Switch		1	B S
					ne south	nir - oigauit	ros onnon			
 System 	Statistic									
Ports	outout	-0								
 Security LACP 	VLAN	Querier	Host	Querier	Queries	Queries	V1	V2	V3	V2
Loop Protection	ID	Version	Version	Status	Transmitted	Received	Reports	Reports	Reports	Leaves
Spanning Tree							Received	Received	Received	Received
▶ MVR	Router	Port								
 IPMC IGMP Snooping 										
 Status 	Port	Status								
 Groups 	1	•								
Information	2									
 IPv4 SFM Information 	3	•								
► MLD Snooping	4	-								
► LLDP	5	-								
• PoE	7									
MAC Table	8	-								
VLANs VCL	9									
• sFlow	10									
Diagnostics	11									
Maintenance	12									
	13									
	14	-								
	15	-								
	16	-								
	17	-								
	18									
	19	-								
	20	-								
	21	•								
	22									
	23	-								
	24									
	25	-								
	26									

VLAND ID

The <u>VLAN</u> ID of the entry.

Querier Version

Working Querier Version currently.

Host Version

Working Host Version currently.

Querier Status

Shows the Querier status is "ACTIVE" or "IDLE".

"DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted

The number of Transmitted Queries.

Queries Received

The number of Received Queries.

V1 Reports Received

The number of Received V1 Reports.

V2 Reports Received

The number of Received V2 Reports.

V3 Reports Received

The number of Received V3 Reports.

V2 Leaves Received

The number of Received V2 Leaves.

Router Port

Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the

Layer 3 multicast device or IGMP querier.

Static denotes the specific port is configured to be a router port.

Dynamic denotes the specific port is learnt to be a router port.

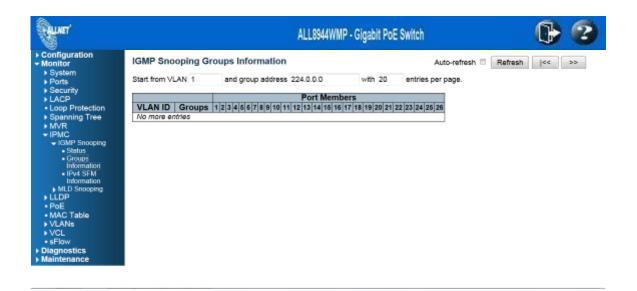
Both denotes the specific port is configured and learnt to be a router port.

Buttons

Refresh : Click to refresh the page immediately. Clear : Clears all Statistics counters.

IGMP Group Table

Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group.



Navigating the IGMP Group Table

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

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

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

IGMP Group Table Columns

VLAN ID

VLAN ID of the group.

Groups

Group address of the group displayed.

Port Members

Ports under this group.

Buttons

Auto-refresh \square : Check this box to enable an automatic refresh of the page at regular intervals. Refresh : Refreshes the displayed table starting from the input fields.

- << : Updates the table, starting with the first entry in the IGMP Group Table.
- >> : Updates the table, starting with the entry after the last entry currently displayed.

IGMP SFM Information Table

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Souce-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port No. Different source addresses belong to the same group are treated as single entry.

RUNT'	ALL8944WMP - G	igabit PoE Switch	1 🕑 🕑
Configuration Monitor System Ports Security LACP Loop Protection Spanning Tree Bradge Status Port Statistics MVR Statistics Statistics MVR Statistics MVR Statistics MVR Statistics Statistatistics Statistic	MVR SFM Information Start from VLAN 1 and Group Address :: VLAN ID Group Port Mode Source Address Type No more entries	Auto-refresh with 20 Hardware Filter/Switch	Refresh I< >> entries per page.

Navigating the IGMP SFM Information Table

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

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP SFM Information Table. Clicking the button will update the displayed table starting from that or the closest next IGMP SFM Information Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. The will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

IGMP SFM Information Table Columns

VLAN ID

VLAN ID of the group.

Group

Group address of the group displayed.

Port

Switch port number.

Mode

Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address

IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

Туре

Indicates the Type. It can be either Allow or Deny.

Buttons

Auto-refresh \Box : Check this box to enable an automatic refresh of the page at regular intervals. Refresh : Refreshes the displayed table starting from the input fields.

<< : Updates the table starting from the first entry in the IGMP SFM Information Table.

>> : Updates the table, starting with the entry after the last entry currently displayed.

MLD Snooping Status

This page provides MLD Snooping status.

Figurer'		ALL	8944WMP - Gigabit PoE Swite	h	
Configuration Monitor	MLD Snooping Stat	s		Auto-refresh 🗉 Refre	sh Clear
 System Ports 	Statistics				
 Security 	VLAN Querier	ost Querier Que	ies Queries V1 Repo	orts V2 Reports V1 Leaves	-
+ LACP		sion Status Transr			
Loop Protection Spanning Tree MVR	Router Port				_
- IPMC	Port Status				
 IGMP Snooping MLD Snooping 	1 -				
 MLD Snooping Status 	2 -				
 Groups 	3 -				
Information IPv6 SFM	4 -				
Information	5 -				
LLDP	6 - 7 -				
• PoE	8 -				
 MAC Table VLANs 	9 -				
VCL	10 -				
• sFlow	11 -				
Diagnostics	12 -				
Maintenance	13 -				
	14 -				
	15 -				
	16 -				
	17 -				
	18 -				
	19 -				
	20 -				
	21 - 22 -				
	22 -				
	23 -				
	24 -				
	26 -				

VLAND ID

The <u>VLAN</u> ID of the entry.

Querier Version

Working Querier Version currently.

Host Version

Working Host Version currently.

Querier Status

Show the Querier status is "ACTIVE" or "IDLE".

"DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted

The number of Transmitted Queries.

Queries Received

The number of Received Queries.

V1 Reports Received

The number of Received V1 Reports.

V2 Reports Received

The number of Received V2 Reports.

V1 Leaves Received

The number of Received V1 Leaves.

Router Port

Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the

Layer 3 multicast device or IGMP querier.

Static denotes the specific port is configured to be a router port.

Dynamic denotes the specific port is learnt to be a router port.

Both denotes the specific port is configured and learnt to be a router port.

Buttons

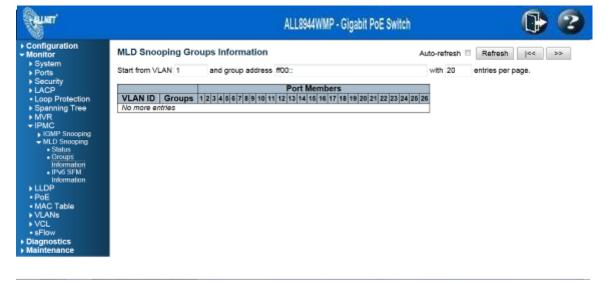
Refresh : Click to refresh the page immediately.

Clear : Clears all Statistics counters.

Auto-refresh \Box : Check this box to enable an automatic refresh of the page at regular intervals.

MLD Group Table

Entries in the MLD Group Table are shown on this page. The MLD Group Table is sorted first by VLAN ID, and then by group.



Navigating the MLD Group Table

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

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

The will use the last entry of the currently displayed 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.

Buttons

Auto-refresh \Box : Check this box to enable an automatic refresh of the page at regular intervals. Refresh : Refreshes the displayed table starting from the input fields.

<< : Updates the table starting from the first entry in the MLD Group Table.

>> : Updates the table, starting with the entry after the last entry.

MLD SFM Information Table

Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Souce-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port No. Diffrent source addresses belong to the same group are treated as single entry.



Navigating the MLD SFM Information Table

Each page shows up to 64 entries from the MLD SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD SFM Information Table.

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

MLD SFM Information Table Columns

VLAN ID

VLAN ID of the group.

Group

Group address of the group displayed.

Port

Switch port number.

Mode

Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address

IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

Туре

Indicates the Type. It can be either Allow or Deny.

Buttons

Auto-refresh \Box : Check this box to enable an automatic refresh of the page at regular intervals. Refresh : Refreshes the displayed table starting from the input fields.

<< : Updates the table starting from the first entry in the MLD SFM Information Table.

>> : Updates the table, starting with the entry after the last entry currently displayed.

LLDP Neighbour

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

FRIMET'				ALL8944WMP -	Gigabit PoE Switch		1
Configuration Monitor	LLDP Neig	hbour Infor	mation			Auto	-refresh 🗆 Refresh 🔍
System Ports Security	Local Port	Chassis ID	Remote Port ID	System Name	Port Description	System Capabilities	Management Address
LACP Loop Protection							
 Spanning Tree MVR IPMC 							
LLDP Neighbours LLDP-MED							
Neighbours • PoE • EEE							
Port Statistics PoE MAC Table							
VLANs VCL							
sFlow Diagnostics Maintenance							

Local Port

The port on which the LLDP frame was received.

Chassis ID

The Chassis ID is the identification of the neighbour's 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:

- 1. Other
- 2. Repeater
- 3. Bridge

- 4. WAN Access Point
- 5. Router
- 6. Telephone
- 7. DOCSIS cable device
- 8. Station only
- 9. Reserved

When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

Management Address

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.

Buttons

Refresh : Click to refresh the page immediately.

Auto-refresh \Box : Check this box to enable an automatic refresh of the page at regular intervals.

LLDP Media

This page provides a status overview of all LLDP-MED neighbours. 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. The columns hold the following information:



Port

The port on which the LLDP frame was 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 Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

- 1. LAN Switch / Router
- 2. IEEE 802.1 Bridge
- 3. IEEE 802.3 Repeater (included for historical reasons)
- 4. IEEE 802.11 Wireless Access Point
- Any device that supports the IEEE 802.1AB and MED extentions defined by TIA-1057 and can relay IEEE 802 frames via any method.

LLDP-MED Endpoint Device Definition

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.

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 neighbour 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

Unknown: The network policy for the specified application type is currently unknown.

Defined: 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.

Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.

Tagged: 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 behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).

Buttons

Refresh : Click to refresh the page immediately.

Auto-refresh \Box : Check this box to enable an automatic refresh of the page at regular intervals.

LLDP EEE

By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs due to that the circuits EEE turn off to save power, need time to boot up before sending traffic over the link. This time is called "wakeup time". To achieve minimal latency, devices can use LLDP to exchange information about their respective tx and rx "wakeup time ", as a way to agree upon the minimum wakeup time they need.

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

Runt'				ALLS	1944WMP - Gi	gabit PoE Swit	tch	C	•
Configuration Monitor	LLDP Neig	hbors	EEE In	formation				Auto-refresh	Refresh
 System Ports Security 	Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
LACP Loop Protection				N	IO LLDP EEE II	nformation foun	d		
 Spanning Tree MVR 									
▶ IPMC ▼LLDP									
 Neighbours LLDP-MED 									
Neighbours • PoE • EEE									
Port Statistics PoE									
MAC Table VLANs									
► VCL • sFlow									
Diagnostics Maintenance									

LLDP Neighbors EEE Information

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

Local Port

The port on which LLDP frames are received or transmitted.

Tx Tw

The link parther's maximum time that transmit path can holdoff sending data after deassertion of LPI.

Rx Tw

The link parther's time that receiver would like the transmitter to holdoff to allow time for the receiver to wake from sleep.

Fallback Receive Tw

The link parther'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 partners 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 parther

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 parther

The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).

EEE activated

Show if the switch and the link partner have agree upon which wakeup times to use.

Red - Switch and link partner have not agreed upon wakeup time.

Green - Switch and link partner have agreed upon wakeup time.

Buttons

Refresh : Click to refresh the page immediately.

Auto-refresh \Box : Check this box to enable an automatic refresh of the page at regular intervals.

LLDP Statistics

This page provides an overview of all LLDP traffic.

Two types of counters are shown. **Global counters** are counters that refer to the whole switch, while **local counters** refer to per port counters for the currently selected switch.

ALMET'				1	ALL8944WMP - G	igabit PoE Switch		6	
Configuration Monitor	LLDP GI	obal Count	ters				Auto-refresh	Refresh	Clear
 System Ports 			Glo	oal Counte	rs				
 Ports Security 	Neighbou	r entries were	last changed	1970-01-01	IT00:00:00+00:00	(15233 sec. ago)			
► LACP	Total Neig	hbours Entrie	es Added		0				
 Loop Protection 	Total Neig	hbours Entrie	es Deleted		0				
Spanning Tree	Total Neig	hbours Entrie	es Dropped		0				
▶ MVR	Total Neig	hbours Entrie	es Aged Out		0				
▶ IPMC									
LLDP Neighbours	LLDP Sta	atistics Loo	cal Counte	rs					
 LLDP-MED Neighbours 	Local	Tx	Rx	Rx	Frames	TLVs	TLVs	Ora.	Age-
 PoĚ 	Port	Frames	Frames	Errors	Discarded	Discarded	Unrecognized	Discarded	Outs
• EEE	1	0	0	0	0	0	0	0	0
 Port Statistics PoE 	2	0	0	0	0	0	0	0	0
MAC Table	3	0	0	0	0	0	0	0	0
VLANs	4	0	0	0	0	0	0	0	0
► VCL	5	0	0	0	0	0	0	0	0
• sFlow	6	0	0	0	0	0	0	0	0
Diagnostics	7	0	0	0	0	0	0	0	0
Maintenance	8	0	0	0	0	0	0	0	0
	9	0	0	0	0	0	0	0	0
	10	0	0	0	0	0	0	0	0
	11	0	0	0	0	0	0	0	0
	12	0	0	0	0 0	õ	0	0	ō
	13	0	0	0	0	0	0	0	0
	14	513	0	0	ő	ő	0	0	0
	15	0	0	0	Ö	0	0	0	ō
	16	0	0	0	0	0	0	0	0
	17	0	0	0	0	0	0	0	0
	18	0	0 0	0	Ő	õ	0	0	0
	19	0	0	0	0	0	0	0	0
	20	0	0	0	0	0	0	0	0
	21	0	0	0	õ	õ	0	0	Ö
	22	0	Ő	0	ő	ő	0	0	Ö
	23	0	0	0	õ	õ	0	õ	ō
	24	0	0	0	0	0	0	0	ō
		-		-	-	0	0	0	-
	25	0	0	0	0	U		U	0

Global Counters

Neighbour entries were last changed on

It also 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.

Total Neighbours Entries Dropped

Shows the number of LLDP frames dropped due to the entry table being full.

Total Neighbours Entries Aged Out

Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

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

Local Port

The port on which LLDP frames are received or transmitted.

Tx Frames

The number of LLDP frames transmitted on the port.

Rx Frames

The number of LLDP frames received on the port.

Rx Errors

The number of received LLDP frames containing some kind of error.

Frames Discarded

If 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.

TLVs Discarded

Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

TLVs Unrecognized

The number of well-formed TLVs, but with an unknown type value.

Org. Discarded

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.

Buttons

Refresh : Click to refresh the page immediately.

Clear : Clears the local counters. All counters (including global counters) are cleared upon reboot.

Auto-refresh \Box : Check this box to enable an automatic refresh of the page at regular intervals.

ΡοΕ

Power Over Ethernet Configuration

ALINET'				ALL8944WMP -	Gigabit PoE S	witch		1
Configuration Monitor	Power Ove	er Etherne		Auto	-refresh 🔲 Refresh			
 ▶ System ▼ Ports ■ State 	Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
 Traffic Overview QoS Statistics 	1	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
QCL Status Detailed Statistics	2	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
Security LACP	3	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
 Loop Protection Spanning Tree 	4	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
► MVR ► IPMC ► LLDP	5		0 [W]	0 [W]	0 [VV]	0 [mA]	Low	PoE turned OFF - PoE disabled
• PoE	6	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
MAC Table VLANs	7	-	0 [W]	0 [W]	0 [VV]	0 [mA]	Low	PoE turned OFF - PoE disabled
 VCL sFlow Diagnostics 	8	-	0 [W]	0 [W]	0 [VV]	0 [mA]	Low	PoE turned OFF - PoE disabled
Maintenance	9	-	0 [W]	0 [W]	0 [VV]	0 [mA]	Low	PoE turned OFF - PoE disabled
	10	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
	11	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
	12	-	0 [W]	0 [W]	0 [VV]	0 [mA]	Low	PoE turned OFF - PoE disabled
	13	-	0 [W]	0 [VV]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
	14	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
	15	-	0 [W]	0 [W]	0 [VV]	0 [mA]	Low	PoE turned OFF - PoE disabled
	16	-	0 [W]	0 [W]	0 [VV]	0 [mA]	Low	PoE turned OFF - PoE disabled
	17	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
	18	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
	19	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
	20	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
	21	-	0 [VV]	0 [W]	0 [VV]	0 [mA]	Low	PoE turned OFF - PoE disabled
	22	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
	23	-	0 [VV]	0 [W]	0 [VV]	0 [mA]	Low	PoE turned OFF - PoE disabled
	24	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
	Total		0 [VV]	0 [VV]	0 [W]	0 [mA]		

Reserved Power determined by

There are three modes for configuring how the ports/PDs may reserve power.

1. Allocated mode: In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields.

2. Class mode: In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 or 30 Watts.

In this mode the Maximum Power fields have no effect.

3. LLDP-MED mode: This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode In this mode the Maximum Power fields have no effect

For all modes: If a port uses more power than the reserved power for the port, the port is shut down.

Power Management Mode

There are 2 modes for configuring when to shut down the ports:

1. Actual Consumption: In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down.

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

Power Supply Configuration

Primary and Backup Power Source

Some switches support having two PoE power supplies. One is used as primary power source, and one as backup power source. If the switch doesn't support backup power supply only the primary power supply settings will be shown. In case that the primary power source fails the backup power source will take over. For being able to determine the amount of power the PD may use, it must be defined what amount of power the primary and backup power sources can deliver.

Valid values are in the range 0 to 2000 Watts.

-BLNET'				ALL8944WMP -	Gigabit PoE Sv	witch		1
Configuration Monitor	Power Ove	er Etherne	t Status				Auto	-refresh 🔲 Refresh
 System Ports State 	Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
 Traffic Overview QoS Statistics 	1	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
QCL Status Detailed Statistics	2	-	0 [W]	0 [W]	0 [VV]	0 [mA]	Low	PoE turned OFF - PoE disabled
Security LACP	3	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
 Loop Protection Spanning Tree 	4	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
► MVR ► IPMC	5	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
 LLDP PoE 	6	-	0 [W]	0 [W]	0 [VV]	0 [mA]	Low	PoE turned OFF - PoE disabled
 MAC Table VLANs 	7	-	0 [W]	0 [W]	0 [VV]	0 [mA]	Low	PoE turned OFF - PoE disabled
 VCL sFlow 	8	-	0 [W]	0 [W]	0 [VV]	0 [mA]	Low	PoE turned OFF - PoE disabled
Diagnostics Maintenance	9	-	0 [VV]	0 [W]	0 [VV]	0 [mA]	Low	PoE turned OFF - PoE disabled
	10	-	0 [VV]	0 [W]	0 [VV]	0 [mA]	Low	PoE turned OFF - PoE disabled
	11	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
	12	-	0 [W]	0 [W]	0 [VV]	0 [mA]	Low	PoE turned OFF - PoE disabled
	13	-	0 [VV]	0 [W]	0 [VV]	0 [mA]	Low	PoE turned OFF - PoE disabled
	14	-	0 [VV]	0 [W]	0 [VV]	0 [mA]	Low	PoE turned OFF - PoE disabled
	15	-	0 [VV]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
	16	-	0 [VV]	0 [W]	0 [VV]	0 [mA]	Low	PoE turned OFF - PoE disabled
	17	-	0 [VV]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
	18	-	0 [VV]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
	19	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
	20		0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
	21		0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
	22		0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
	23		0 [W]	0 [W]	0 [VV]	0 [mA]	Low	PoE turned OFF - PoE disabled
	24	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
	Total		0 [W]	0 [W]	0 [W]	0 [mA]		alganica

Power Over Ethernet Status Help

is page allows the user to inspect the currer	t status for all <u>PoE</u> ports.
.ocal Port	
This is the logical port number for this row.	
PD Class	
Each \underline{PD} is classified according to a class the	at defines the maximum power the PD will use. The PD Class shows the PDs class.
Five Classes are defined:	
Class 0: Max. power 15.4 W	
Class 1: Max. power 4.0 W	
Class 2: Max. power 7.0 W	
Class 3: Max. power 15.4 W	
Class 4: Max. power 30.0 W	
Power Requested	
The Power Requested shows the requested	amount of power the PD wants to be reserved.
Power Allocated	
The Power Allocated shows the amount of	power the switch has allocated for the PD.
Power Used	
The Power Used shows how much power the	e PD currently is using.
Current Used	
The Power Used shows how much current	he <u>PD</u> currently is using.
Priority	
The Priority shows the port's priority configu	ired by the user.
Port Status	
The Port Status shows the port's status. Th	e status can be one of the following values:
PoE not available - No PoE chip	found - POE not supported for the port.
PoE turned OFF - PoE disabled :	<u>PoE</u> is disabled by user.
PoE turned OFF - Power budget ex the lowest priority is/are powered down.	ceeded - The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) w
No PD detected - No PD detected for the	ie port.
PoE turned OFF - PD overload - Th	PD has requested or used more power than the port can deliver, and is powered down.
PoE turned OFF - PD is off.	
Invalid PD - PD detected, but is not wo	rking correctly.
uttons	

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 VLAND ID, then by MAC address.

Navigating the MAC Table

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

MAC Table.

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

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

Rever'						ALL8944WMP - Gigabit PoE Switch						6 2												
System Ports	MAC Add		able	and MAC ad	dress	00-0	0-00-0	0-00-(00	with	1 20	Auto	-refre	ish ⊟ les pe		tefrei ge.	sh	Cle	a.	<	¢	>>		
Security LACP													Pol	rt Me	mbe	rs								
 Loop Protection 	Type	VLAN	MA	C Address	CPI	U 1	2 3	4	6 (6 7	8	9 10	11	12 1	3 14	16	16 1	7 18	19	20	21 2	2 23	24 2	5 26
Spanning Tree	Static	1	00-01	-11-65-74-3	33 🧹																			
MVR IPMC	Dynamic	1	00-26	-6C-48-AF-	57										1									
> LLDP	Static	1	33-33	-00-00-00-	01 🧹	1	11	1	7.	75	1	/ /	1	15	17	1	10	1	7	7.	75	1	7	7
PoE	Static	1	33-33	-00-00-00-	02 /	Ż	11	Ċ.	1	11	1	10	Ż	1	11	Ż.	11	Ċ.	Ż	1	1.	ċ.	1	÷.
MAC Table	Static	1		-FF-65-74-3		2	23	1	7.	15	12	15	1	23	17	2	23	Ċ.	2	2	75	1	2	1
VLANs VCL	Static	1		-FF-A8-02-		Ż	11	Ċ.	1	11	1	15	Ż	1	1	1	1	à	Ż	2	7.	Ż	1	÷.
sFlow Diagnostics	Static	1		-FF-FF-FF-		V	~	Ż	7.	à	2	~	Ż	22	$\dot{\mathbf{v}}$	2	~~	Ŵ	Ż	2	2	Ż	~~	\sim

MAC Table Columns

Switch (stack only)

The stack unit where the entry is learned.

Туре

Indicates whether the entry is a static or a dynamic entry.

MAC address

The MAC address of the entry.

VLAN

The VLAN ID of the entry.

Port Members

The ports that are members of the entry.

Auto-refresh : Check this box to enable an automatic refresh of the page at regular intervals. Refresh : Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields. Clear : Flushes all dynamic entries.

\<< : Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.

>> : Updates the table, starting with the entry after the last entry currently displayed.

VLAN Membership Status

This page provides an overview of membership status of VLAN users.

ALLNET'	ALL8944WMP - Gigabit PoE Switch 🛛 🕀 🕗
Configuration Monitor System Ports Security	VLAN Membership Status for Combined users Combined • Auto-refresh • Refresh Start from VLAN 1 with 20 entries per page.
LACP Loop Protection Spanning Tree MVR IPMC LLDP PoE	Port Members VLAN ID 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 1 V
MAC Table VLANs VLANs VLAN Membership V.AN Port VCL sFlow	

VLAN USER

VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configurations such as PVID and UVID. Currently we support the following VLAN user types:

CLI/Web/SNMP : These are referred to as static.

NAS : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

MVRP : Multiple VLAN Registration Protocol (MVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.

Voice VLAN : Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones.

MVR : MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.

MSTP : The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

Port Members

A row of check boxes for each port is displayed for each VLAN ID.

If a port is included in a VLAN, an image vill be displayed.

If a port is included in a Forbidden port list, an image Kwill be displayed.

If a port is included in a Forbidden port list and dynamic VLAN user register VLAN on same Forbidden port, then conflict port will be displayed as 🔀.

VLAN Membership

The VLAN Membership Status Page shall show the current VLAN port members for all VLANs configured by a selected VLAN User (selection shall be allowed by a Combo Box). When ALL VLAN Users are selected, it shall show this information for all the VLAN Users, and this is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

Navigating the VLAN Monitor page

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table starting from that or the closest next VLAN Table match. The will use the last entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

Navigating the VLAN Monitor page

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table starting from that or the closest next VLAN Table match. The will use the last entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

: Select VLAN Users from this drop down list.

Auto-refresh \Box : Check this box to enable an automatic refresh of the page at regular intervals. Refresh : Click to refresh the page immediately.

VLAN Port Status

This page provides VLAN Port Status.

Renner'	ALL8944WMP - Gigabit PoE Switch									
Configuration Monitor	VLAN	Port S	tatus for St	atic user			Sta	atic 🔹 A	uto-refresh 🗉	Refres
 System Ports 	Port	PVID	Port Type	Ingress Filtering	Frame Type	Tx Tag	UVID	Conflicts		
 Security 	1	. 1	UnAware	Disabled	All	Untag_this	1	No		
	2	1	UnAware	Disabled	All	Untag this	1	No		
► LACP	3	1	UnAware	Disabled	All	Untag this	1	No		
Loop Protection	4	1	UnAware	Disabled	All	Untag_this	1	No		
Spanning Tree	5	1	UnAware	Disabled	All	Untag_this	1	No		
► MVR	6	1	UnAware	Disabled	All	Untag_this	1	No		
▶ IPMC	7	1	UnAware	Disabled	All	Untag_this	1	No		
► LLDP	8	1	UnAware	Disabled	All	Untag_this	1	No		
• PoE	9	1	UnAware	Disabled	All	Untag_this	1	No		
 MAC Table 	10	1	UnAware	Disabled	All	Untag_this	1	No		
✓ VLANs	11	1	UnAware	Disabled	All	Untag_this	1	No		
 VLAN Membership 	12	1	UnAware	Disabled	All	Untag_this	1	No		
VLAN Port	13	1	UnAware	Disabled	All	Untag_this	1	No		
▶ VCL	14	1	UnAware	Disabled	All	Untag_this	1	No		
• sFlow	15	1	UnAware	Disabled	All	Untag_this	1	No		
Diagnostics	16	1	UnAware	Disabled	All	Untag_this	1	No		
Maintenance	17	1	UnAware	Disabled	All	Untag_this	1	No		
	18	1	UnAware	Disabled	All	Untag_this	1	No		
	19	1	UnAware	Disabled	All	Untag_this	1	No		
	20	1	UnAware	Disabled	All	Untag_this	1	No		
	21	1	UnAware	Disabled	All	Untag_this	1	No		
	22	1	UnAware	Disabled	All	Untag_this	1	No		
	23	1	UnAware	Disabled	All	Untag_this	1	No		
	24	1	UnAware	Disabled	All	Untag_this	1	No		
	25	1	UnAware	Disabled	All	Untag_this	1	No		
	26	1	UnAware	Disabled	All	Untag_this	1	No		

VLAN USER

VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID, UVID. Currently we support following VLAN User types:

CLI/Web/SNMP : These are referred to as static.

NAS : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

MVRP : Multiple VLAN Registration Protocol (MVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.

Voice VLAN : Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones.

MVR : MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.

MSTP : The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

Port

The logical port for the settings contained in the same row.

PVID

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

Port Type

Shows the Port Type. Port type can be any of Unaware, C-port, S-port, Custom S-port.

If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed.

C-port is Customer Port. S-port is Service port. Custom S-port is S-port with Custom TPID.

Ingress Filtering

Shows the ingress filtering on a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN, the frame is discarded.

Frame Type

Shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.

Tx Tag

Shows egress filtering frame status whether tagged or untagged.

UVID

Shows UVID (untagged VLAN ID). Port's UVID determines the packet's behaviour at the egress side.

Conflicts

Shows status of Conflicts whether exists or not. When a Volatile VLAN User requests to set VLAN membership or VLAN port configuration, the following conflicts can occur:

Functional Conflicts between features.

Conflicts due to hardware limitation.

Direct conflict between user modules.

: Select VLAN Users from this drop down list.

Auto-refresh \Box : Check this box to enable an automatic refresh of the page at regular intervals. Refresh : Click to refresh the page immediately.

Runer'				AL	.L8944WMP - Gi	gabit PoE S	witch			1	2
Configuration Monitor	VLAN	Port S	tatus for SI	atic user			Static	5	Auto-refresh	Refresh	1
 System 	-				-		Citatic				4
Ports	Port	PVID	Port Type	Ingress Filtering	Frame Type	Tx Tag	UVICNAS				
Security	1	1	UnAware	Disabled	All	Untag_this	MVR				
LACP	2	1	UnAware	Disabled	Ali	Untag_this	Voice	VLAN			
Loop Protection	3	1	UnAware	Disabled	All	Untag_this	MSTP				
	4	1	UnAware	Disabled	Ali	Untag_this	VCL				
 Spanning Tree 	5	 1 	UnAware	Disabled	Ali	Untag_this	Comb	ined			
MVR	6	1	UnAware	Disabled	All	Untag_this	Contrac	IND I	10		
▶ IPMC	7	1	UnAware	Disabled	All	Untag_this	1	No			
► LLDP	8	1	UnAware	Disabled	IIA	Untag_this	1	No			
PoE	9	1	UnAware	Disabled	All	Unteg_this	1	No			
 MAC Table 	10	1	UnAware	Disabled	All	Untag_this	1	No			
VLANs	11	1	UnAware	Disabled	All	Untag_this	1	No			
 VLAN Membership 	12	1	UnAware	Disabled	All	Untag_this	1	No			
VLAN Port	13		UnAware	Disabled	All	Untag_this	1	No			
VCL	14	1	UnAware	Disabled	All	Untag_this	1	No			
• sElaw	46	4	Lin Augen	Disabled		Listan Hale		Alo.			

MRP Statistics

This page port statistics of MRP for all switch ports.

The displayed statistics are:

Port

The Port column shows the list of all ports for which per port MRP statistics are shown.

Peer MAC

Peer MAC is MAC address of the neighbour Switch from with MRP frame is received.

Failed Count

explain Failed count here...

Buttons

Auto-refresh \Box : Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.

Refresh : Click to refresh the page; any changes made locally will be undone

MVRP Statistics

This page shows the basic MVRP Port statistics for all switch ports.

The displayed settings are:

Port

The Port coulmn shows the list of ports for which you can see port counters and statistics.

Join Tx Count

explain Join tx Count here...

Leave Tx Count

explain Leave Tx Count here...

Buttons

Auto-refresh \Box : Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.

Refresh : Click to refresh the page; any changes made locally will be undone

VCL MAC-Based VLAN Status

This page shows MAC-based VLAN entries configured by various MAC-based VLAN users. Currently we support following VLAN User types:

RELART'	ALL8944WMP - Gigabit PoE Switch	0 🕄
Configuration Monitor System Security Loop Protection Spanning Tree M/VR ILDP PoE MAC Table VLANs VCL MAC tassed VLAN	MAC-based VLAN Membership Configuration for User Static Port Members MAC Address VLAN ID 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 No date exists for the user	Static • Auto-refresh Refresh 20 21 22 23 24 26 26

CLI/Web/SNMP : These are referred to as static.

NAS : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

MAC Address

Indicates the MAC address.

VLAN ID

Indicates the VLAN ID.

Port Members

Port members of the MAC-based VLAN entry.

Buttons

Refresh : Refreshes the displayed table.

FRUMET	ALL8944WMP - Gigabit PoE Switch 🕞 😰	
Configuration Monitor System Ports Security LACP Loop Protection Spanning Tree MVR IPMC LIDP POE MAC Table VLANs VCL SFlow VCL Security Security VCL Security VCL Security Security Security Security Security Security VCL Security VCL Security VCL Security S	MAC-based VLAN Membership Configuration for User Static Static Auto-retresh Refresh Port Members NAS MAC Address VLAN ID 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 2 Combined Ze No data exists for the user	

Ping

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.

After you press, 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING server 10.10.132.20

64 bytes from 10.10.132.20: icmp_seq=0, time=0ms 64 bytes from 10.10.132.20: icmp_seq=1, time=0ms 64 bytes from 10.10.132.20: icmp_seq=2, time=0ms 64 bytes from 10.10.132.20: icmp_seq=3, time=0ms 64 bytes from 10.10.132.20: icmp_seq=4, time=0ms Sent 5 packets, received 5 OK, 0 bad This page allows you to retrieve the Local or Remote OAM MIB variable data on a particular port. Select the appropriate Radio button to retrieve the content of interest, Enter the Port number for the switch. Click on Start to retrieve the content.

Ping6

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

After you press, 5 ICMPv6 packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING6 server ::10.10.132.20 64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms 64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms 64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms 64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms 64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms Sent 5 packets, received 5 OK, 0 bad

You can configure the following properties of the issued ICMP packets:

IP Address

The destination IP Address.

Ping Size

The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes for IPv4. Values range from 1 bytes to 1452 bytes for IPv6.

Runer'			ALL8944WMP - Gigabit PoE Switch	1 🕄
Configuration Monitor	ICMP Ping			
 Diagnostics Ping 	IP Address	0.0.0.0		
 Ping6 	Ping Length Ping Count	56		
VeriPHY		5		
Maintenance	Ping Interval	1		
	Start			

Diagnostics Help (ICMPv6 Ping)

Ping

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.

After you press, 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING server 10.10.132.20

64 bytes from 10.10.132.20: icmp_seq=0, time=0ms 64 bytes from 10.10.132.20: icmp_seq=1, time=0ms 64 bytes from 10.10.132.20: icmp_seq=2, time=0ms 64 bytes from 10.10.132.20: icmp_seq=3, time=0ms 64 bytes from 10.10.132.20: icmp_seq=4, time=0ms Sent 5 packets, received 5 OK, 0 bad

This page allows you to retrieve the Local or Remote OAM MIB variable data on a particular port. Select the appropriate Radio button to retrieve the content of interest, Enter the Port number for the switch. Click on Start to retrieve the content.

ALMET			ALL8944WN	IP - Gigabit PoE Switch	()	2
Configuration Monitor Diagnostics	ICMPv6 Ping	0:0:0:0:0:0:0:0		1		
Ping Ping8 VeriPHY	Ping Length	56				
Maintenance	Ping Count Ping Interval	1				
	Start					

Ping6

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

After you press, 5 ICMPv6 packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING6 server ::10.10.132.20 64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms 64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms 64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms 64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms 64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms Sent 5 packets, received 5 OK, 0 bad

You can configure the following properties of the issued ICMP packets:

IP Address

The destination IP Address.

Ping Size

The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes for IPv4. Values range from 1 bytes to 1452 bytes for IPv6.

VeriPHY

This page 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.

BUNET

Configuration Monitor Diagnostics • Ping

> ng6 nPHY

ALL8944WMP - Gigabit PoE Switch

1 2

VeriPHY Cable Diagnostics

Start

Cable Status									
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D	
1									
2									
3									
- 4		-	-						
5		-	-				-	-	
6		-							
7									
8		-							
9		-	-				-		
10		-	-						
11									
12		-							
13		-							
14		-							
15									
16		-							
17									
18		-	-						
19		-							
20		-	-						
21									
22		-							
23		-	-				-		
24									

Port

The port where you are requesting VeriPHY Cable Diagnostics.

Cable Status

Port: Port number.

Pair: The status of the cable pair.

Length: The length (in meters) of the cable pair.

Restart Device

You can restart the switch on this page. After restart, the switch will boot normally.



Yes : Click to restart device.

No : Click to return to the Port State page without restarting.

Factory Defaults

You can reset the configuration of the switch on this page. Only the IP configuration is retained.

The new configuration is available immediately, which means that no restart is necessary.

Ren Mar	ALL8944WMP - Gigabit PoE Switch	1 🕑 🕑
Configuration Monitor Diagnostics	Factory Defaults	
Maintenance Restart Device Factory Defaults Software Configuration	Are you sure you want to reset the configuration to Factory Defaults?	
	Yes No	

Yes : Click to reset the configuration to Factory Defaults.

No : Click to return to the Port State page without resetting the configuration.

Note: Restoring factory default can also be performed by making a physical loopback between port 1 and port 2 within the first minute from switch reboot. In the first minute after boot, 'loopback' packets will be transmitted at port 1. If a 'loopback' packet is received at port 2 the switch will do a restore to default . (192.168.2.1)

Software Upload

This page facilitates an update of the firmware controlling the switch.

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

ALLNET	ALL8944WMP - Gigabit PoE Switch	6 2
Configuration Monitor Diagnostics Maintenance Restart Device Factory Defaults Software Upload	Firmware Update	
 Image Select Configuration 		

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.

Firmware Selection

This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

The web page displays two tables with information about the active and alternate firmware images.

Note:

- 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.
- 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.

Image Information

Image

The flash index name of the firmware image. The name of primary (preferred) image is **image**, the alternate image is named **image.bk**.

Version

The version of the firmware image.

Date

The date where the firmware was produced.

Yes : Click to use the alternate image. This button may be disabled depending on system state.

No : Cancel activating the backup image. Navigates away from this page.

Configuration

You can save/view or load the switch configuration. The configuration file is in XML format with a hierarchy of tags:



GULNET'	ALL8944WMP - Gigabit PoE Switch	00
 Configuration Monitor Diagnostics Maintenance Restart Device Factory Defaults Software Configuration Save Upload 	Configuration Upload Durchsuchen Upload	

Header tags: <?xml version="1.0"?> and <configuration>. These tags are mandatory and must be present at the beginning of the file.

Section tags: <platform>, <global> and <switch>. The platform section must be the first section tag and this section must include the correct platform ID and version. The global section is optional and includes configuration which is not related to specific switch ports. The switch section is optional and includes configuration which is related to specific switch ports.

Module tags: <ip>, <mac>, <port> etc. These tags identify a module controlling specific parts of the configuration.

Group tags: <port_table>, <vlan_table> etc. These tags identify a group of parameters, typically a table.

Parameter tags: <mode>, <entry> etc. These tags identify parameters for the specific section, module and group. The <entry> tag is used for table entries.

Configuration parameters are represented as attribute values. When saving the configuration from the switch, the entire configuration including syntax descriptions is included in the file. The file may then be modified using an editor and loaded to a switch.

The example below shows a small configuration file only including configuration of the MAC address age time and the learning mode per port. When loading this file, only the included parameters will be changed. This means that the age time will be set to 200 and the learn mode will be set to automatic.

< ?xml version="1.0"?> <configuration> <platform> <pid val="3"></pid> <version val="1"></version> </platform> <global> <mac> <age val="200"></age>> </mac> </global> <switch sid="1"> <mac> <entry port="1-24" learn_mode="auto"></entry> </mac> </switch> < /configuration>

CE-Declaration of Conformity



For following equipment:

Germering, January 03, 2013

24 x 10/100/1000 Gigabit + 2 Gigabit SFP Port

ALL8944WMP



The safety advice in the documentation accompanying the products shall be obeyed. The conformity to the above directive is indicated by the CE sign on the device.

The Allnet ALL8944WMP conforms to the Council Directives of 1999/5/EC.

This equipment meets the following conformance standards:

EN55022:2010: Class B IEC61000-3-2:2005+A1:2008+A2:2009 IEC61000-3-3:2008 EN55024:2010 IEC61000-4-2:2008 IEC61000-4-3:2006+A1:2007+A2:2010 IEC61000-4-4:2004+A1:2010 IEC61000-4-5:2005 IEC61000-4-6:2008 IEC61000-4-8:2009 IEC61000-4-11:2004

This equipment is intended to be operated in all countries.

This declaration is made by ALLNET Computersysteme GmbH Maistraße 2 82110 Germering Germany

Germering, 03.01.2013

Wolfgang Marcus Bauer