



KGS-2423

Web Management Interface

User's Manual



DOC.111205

TRADEMARKS

Ethernet is a registered trademark of Xerox Corp.

Vitesse Switch Software. Copyright (c) 2002-2009

Vitesse Semiconductor Corporation "Vitesse". All Rights Reserved.

Unpublished rights reserved under the copyright laws of the United States of America, other countries and international treaties. Permission to use, copy, store and modify, the software and its source code is granted. Permission to integrate into other products, disclose, transmit and distribute the software in an absolute machine readable format (e.g. HEX file) is also granted. The software may only be used in products utilizing the Vitesse switch products.

(C) 2011 KTI Networks Inc. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation or transformation) without permission from KTI Networks Inc.

KTI Networks Inc. reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of KTI Networks Inc. to provide notification of such revision or change.

For more information, contact:

United States KTI Networks Inc.
P.O. BOX 631008
Houston, Texas 77263-1008

Phone: 713-2663891
Fax: 713-2663893
E-mail: kti@ktinet.com
URL: <http://www.ktinet.com/>

International Fax: 886-2-26983873
E-mail: kti@ktinet.com.tw
URL: <http://www.ktinet.com.tw/>

Table of Contents

1. Web Management	9
1.1 Start Browser Software and Making Connection	9
1.2 Login to the Switch Unit	9
1.3 Main Management Menu	11
2. Configuration	13
2.1 System	13
2.1.1 Information	13
2.1.2 IP & Time	14
2.1.3 IPv6 & Time	15
2.1.4 NTP	16
2.2 Ports.....	17
2.3 Security	19
2.3.1 Switch	19
2.3.1.1 Uers	19
2.3.1.2 Privilege Levels	21
2.3.1.3 Auth Method.....	22
2.3.1.4 SSH.....	23
2.3.1.5 HTTPS	23
2.3.1.6 Access Management Configuration	24
2.3.1.7 SNMP	25
2.3.1.7.1 System	25
2.3.1.7.2 Communities	28
2.3.1.7.3 Users.....	29
2.3.1.7.4 Groups	31
2.3.1.7.5 Views	32
2.3.1.7.6 Accesses.....	33
2.3.2 Network	34
2.3.2.1 Limit Control.....	34
2.3.2.2 NAS.....	37
2.3.2.3 ACL	47
2.3.2.3.1 Ports.....	47

2.3.2.3.2 Rate Limiters	49
2.3.2.3.3 Access Control Lists.....	49
2.3.2.4 DHCP	52
2.3.2.4.1 Snooping.....	52
2.3.2.4.2 Relay	53
2.3.2.5 IP Source Guard	55
2.3.2.5.1 Configuration.....	55
2.3.2.5.2 Static Table	56
2.3.2.6 ARP Inspection	57
2.3.2.6.1 Configuration.....	57
2.3.2.6.2 Static Table	58
2.3.3 AAA	59
2.4 Aggregation.....	61
2.4.1 Static	61
2.4.2 LACP	63
2.5 Spanning Tree	64
2.5.1 Bridge Settings.....	64
2.5.2 MSTI Mapping.....	66
2.5.3 MSTI Priorities	67
2.5.4 CIST Ports	68
2.5.5 MSTI Ports	69
2.6 IGMP Snooping.....	72
2.6.1 Basic Configuration.....	72
2.6.2 VLAN Configuration	73
2.6.3 Port Group Filtering.....	74
2.7 MVR	75
2.8 LLDP	76
2.8.1 LLDP	76
2.8.2 LLDP-MED	79
2.9 PoE	85
2.10 MAC Table	87
2.10.1 Static MAC Address Configuration.....	88

2.11 VLANs.....	89
2.11.1 VLAN Membership.....	89
2.11.2 VLAN Port Configuration.....	91
2.12 Private VLANs.....	93
2.13 Voice VLAN.....	94
2.13.1 Configuration.....	94
2.13.2 OUI.....	96
2.14 QoS.....	97
2.14.1 Ports.....	97
2.14.2 DSCP Remarking.....	99
2.14.4 QoS Control List.....	100
2.14.5 Rate Limiters.....	102
2.14.6 Storm Control.....	103
2.14.7 Wizard.....	104
2.14.7.1 Wizard – Port Policies.....	105
2.14.7.2 Wizard – Typical Network Application Rules.....	106
2.14.7.3 Wizard – ToS Precedence Mapping.....	107
2.14.7.4 Wizard – VLAN Tag Priority Mapping.....	108
2.15 Mirroring.....	109
2.16 UPnP.....	111
2.17 Stack.....	112
2.17.1 Assigning Switch ID.....	112
2.17.2 Master Switch Election in a Stack.....	114
3. Monitor.....	115
3.1 System.....	115
3.1.1 Information.....	115
3.1.2 CPU Load.....	116
3.1.3 Log.....	117
3.1.4 Detailed Log.....	118
3.2 Ports.....	119
3.2.1 State.....	119
3.2.2 Traffic Overview.....	121

3.2.3 QoS Statistics	122
3.2.4 Detailed Statistics.....	123
3.3 Security	125
3.3.1 Access Management Statistics	125
3.3.2 Network.....	125
3.3.2.1 Port Security	125
3.3.2.1.1 Switch	126
3.3.2.1.2 Port	127
3.3.2.2 NAS.....	128
3.3.2.2.1 Switch	128
3.3.2.2.2 Port	130
3.3.2.3 ACL Status.....	134
3.3.2.4 DHCP	135
3.3.2.4.1 Snooping Statistics	135
3.3.2.4.2 Relay Statistics	136
3.3.2.5 ARP Inspection	137
3.3.2.6 IP Source Guard	138
3.3.3 AAA.....	139
3.3.3.1 RADIUS Overview.....	139
3.3.3.2 RADIUS Details	140
3.4 LACP.....	143
3.4.1 System Status.....	144
3.4.2 Port Status	145
3.4.3 Port Statistics.....	146
3.5 Spanning Tree	147
3.5.1 Bridge Status	147
3.5.2 Port Status	149
3.5.3 Port Statistics.....	150
3.6 IGMP Snooping.....	151
3.7 MVR	152
3.8 LLDP	152
3.8.1 Neighbors.....	152

3.8.2 LLDP-MED Neighbors.....	153
3.8.3 PoE	157
3.8.4 Port Statistics	158
3.9 PoE	160
3.10 MAC Table	161
3.11 VLAN.....	162
3.11.1 VLAN Membership.....	162
3.11.2 VLAN Port	163
3.12 Stack.....	165
4. Diagnostics	167
4.1 SFP DDM.....	167
4.2 Ping.....	168
4.3 Ping6.....	169
5. Maintenance.....	170
5.1 Reset Device.....	170
5.2 Factory Defaults	171
5.3 Software Upload	171
5.4 Configuration.....	171
Glossary	173

1. Web Management

The switch features an http server which can serve the management requests coming from any web browser software over TCP/IP network.

Web Browser

Compatible web browser software with JAVA script support

Microsoft Internet Explorer 4.0 or later

Netscape Communicator 4.x or later

Set IP Address for the System Unit

Before the switch can be managed from a web browser software, make sure a unique IP address is configured for the switch.

1.1 Start Browser Software and Making Connection

Start your browser software and enter the IP address of the switch unit to which you want to connect. The IP address is used as URL for the browser software to search the device.

URL: <http://xxx.xxx.xxx.xxx/>

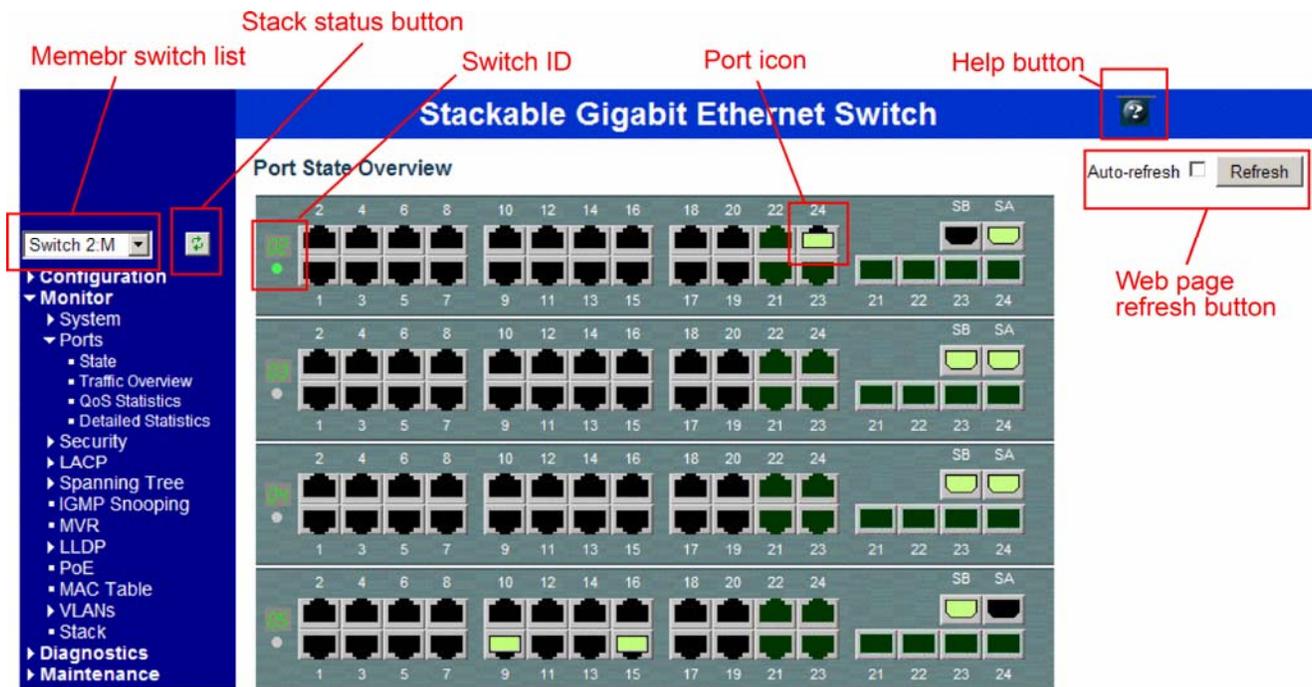
Factory default [IP address](#): 192.168.0.2

1.2 Login to the Switch Unit

When browser software connects to the switch unit successfully, a Login screen is provided for you to login to the device as the left display below:



The switch stack will accept more than one successful management connection at the same time. A switch stack image is displayed as follows after a successful login.



Page components

- Member switch list
- Menu in blue block
- Stack status button
- Switch ID display
- Stack
- Port icon
- Refresh buttons
- Help button

Description

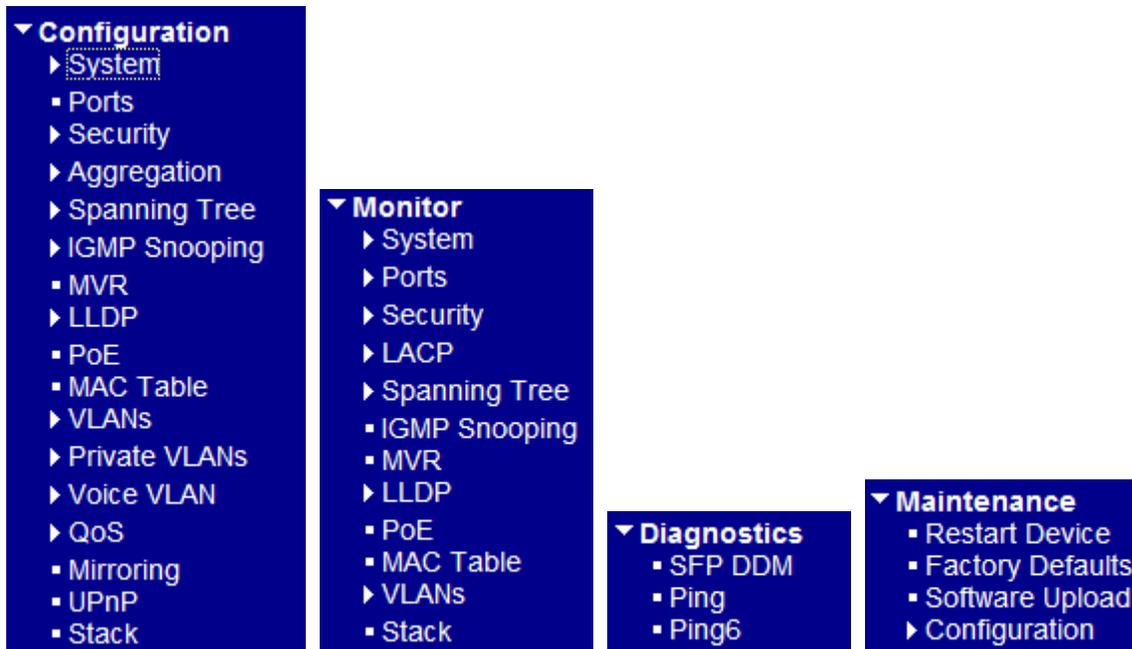
- List for target member switch selection for management operation
- Menu list for web management
- Button to refresh the status of stack connection between members
- Display the switch ID and master LED of the associated switch unit
- Stack image
- Display port link status and click to display port details
- Buttons to refresh the current whole web page
- Pop-up information window for the current management contents

1.3 Main Management Menu

Main Menu:



Sub-menus:



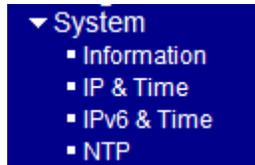
Configuration

System	Switch information, IP configuration, SNTP setting, and Password setting
Ports	Port operation related configuration, frame size, and power saving control
Security	Switch & UI authentication configuration, Port access security control
Aggregation	Static and LACP port link aggregation related configuration
Spanning Tree	STP bridge, MSTI and CIST configuration
IGMP Snooping	IGMP basic and port configuration
MVR	Multicast VLAN Registration (MVR) configuration
LLDP	LLDP configuration
PoE	Power over Ethernet configuration
MAC Table	MAC address learning settings and static MAC address port configuration
VLANs	VLAN groups and VLAN port-related configuration
Private VLANs	PVLAN groups and port isolation configuration
Voice VLAN	Voice VLAN configuration
QoS	QoS port ingress, egress and QCL configuration, Port rate control, QCL wizard

Mirroring	Port mirroring settings
UPnP	Universal Plug and Play configuration
Stack	Switch stack configuration
<u>Monitor</u>	
System	System information and system log information
Ports	Port link status, traffic statistics, QoS statistics
Security	Switch & UI authentication, Port access security status
LACP	LACP system and port status
Spanning Tree	Bridge status, Port status and RSTP/STP/MSTP statistics
IGMP Snooping	IGMP groups learned, Router ports, Statistics
MVR	Multicast VLAN Registration (MVR) status
LLDP	LLDP neighbors information, Port statistics
PoE	Power over Ethernet status
MAC Table	Display of MAC address table
VLAN	Display VLAN membership and VLAN port status
Stack	Stack status
<u>Diagnostics</u>	
SFP DDM	SFP DDM information
Ping	ICMP ping utility
Ping6	ICMPv6 ping utility
<u>Maintenance</u>	
Restart Device	Command to reboot the switch
Factory Defaults	Command to restore the switch with factory default settings
Software Upload	Command to update the switch firmware
Configuration	Command to save or upload the system configuration

2. Configuration

2.1 System



2.1.1 Information

System Information Configuration

System Contact	<input type="text"/>
System Name	<input type="text"/>
System Location	<input type="text"/>
System Timezone Offset (minutes)	<input type="text" value="0"/>

Configuration	Description
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.
System Timezone Offset	Provide the time zone offset relative to UTC/GMT. The offset is given in minutes east of GMT. Valid range: -720 to 720 minutes.

<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

Note:

1. It is suggested to give each switch unit a system name as an alternative unique identification beside IP

address.

2. The system Name, Contact, and Location settings are also used as [SNMP](#) MIBs.

2.1.2 IP & Time

IP Configuration

	Configured	Current
DHCP Client	<input type="checkbox"/>	<input type="button" value="Renew"/>
IP Address	<input type="text" value="192.168.0.179"/>	192.168.0.179
IP Mask	<input type="text" value="255.255.255.0"/>	255.255.255.0
IP Router	<input type="text" value="0.0.0.0"/>	0.0.0.0
VLAN ID	<input type="text" value="1"/>	1
DNS Server	<input type="text" value="0.0.0.0"/>	0.0.0.0

IP DNS Proxy Configuration

DNS Proxy

Configuration	Description
DHCP Client	Enable the DHCP client by checking this box.
IP Address	Provide the IP address of this switch unit.
IP Mask	Provide the IP mask of this switch unit.
IP Router	Provide the IP address of the default router for this switch unit.
VLAN ID	Provide the managed VLAN ID. The allowed range is 1 through 4095.
DNS Server	Provide the IP address of the DNS Server.
DNS Proxy	When DNS proxy is enabled, the switch will relay DNS requests to the current configured DNS server and reply as a DNS resolver to the client device on the network.

<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.
<input type="button" value="Renew"/>	Click to renew DHCP . This button is only available if DHCP is enabled.

Note:

1. 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.

2. The IP addresses should be in dotted decimal notation.

2.1.3 IPv6 & Time

IPv6 Configuration

	Configured	Current
Auto Configuration	<input type="checkbox"/>	
Address	::192.168.0.2	::192.168.0.2 Link-Local Address: fe80::240:f6ff:fee4:1002
Prefix	96	96
Router	::	::
VLAN ID	1	1

Configuration	Description
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 separates 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 also used a following legally IPv4 address. For example, '::192.1.2.34'.
Prefix	Provide the IPv6 Prefix of this switch. The allowed range is 1 through 128.
Gateway	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 separates 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 also used a following legally IPv4 address. For example, '::192.1.2.34'.
VLAN ID	Provide the managed VLAN ID. The allowed range is 1 through 4095.

<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

2.1.4 NTP

NTP Configuration

Mode	Disabled
Server 1	
Server 2	
Server 3	
Server 4	
Server 5	

Configuration	Description
Mode	Indicates the NTP mode operation. Possible modes are: <i>Enabled</i> : Enable NTP mode operation. When enable NTP mode operation, the agent forward and to transfer NTP messages between the clients and the server when they are not on the same subnet domain. <i>Disabled</i> : Disable NTP mode operation.
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 separates 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 also used a following legally IPv4 address. For example, ':::192.1.2.34'.
<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

2.2 Ports

Port Configuration for Switch 1

Port	Link	Speed		Flow Control			Maximum Frame	Excessive Collision Mode	Power Control
		Current	Configured	Current Rx	Current Tx	Configured			
1	Down	Down	Auto	X	X	<input type="checkbox"/>	9600	Discard	Disabled
2	Down	Down	Auto	X	X	<input type="checkbox"/>	9600	Discard	Disabled
3	Down	Down	Auto	X	X	<input type="checkbox"/>	9600	Discard	Disabled
4	Down	Down	Auto	X	X	<input type="checkbox"/>	9600	Discard	Disabled
5	Down	Down	Auto	X	X	<input type="checkbox"/>	9600	Discard	Disabled
6	Down	Down	Auto	X	X	<input type="checkbox"/>	9600	Discard	Disabled
7	Down	Down	Auto	X	X	<input type="checkbox"/>	9600	Discard	Disabled
8	Down	Down	Auto	X	X	<input type="checkbox"/>	9600	Discard	Disabled
9	Down	Down	Auto	X	X	<input type="checkbox"/>	9600	Discard	Disabled
10	Down	Down	Auto	X	X	<input type="checkbox"/>	9600	Discard	Disabled

Configuration	Description
---------------	-------------

Port	The port number associated to this configuration row
------	--

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

Speed - Current	The current link speed of the port.
-----------------	-------------------------------------

Speed - Configured	Select any available link speed for the given switch port.
--------------------	--

Speed	
Current	Configured
Down	Auto
Down	Disabled
Down	Auto
Down	1Gbps FDX
Down	100Mbps FDX
Down	100Mbps HDX
Down	10Mbps FDX
Down	10Mbps HDX

Disabled: disables the switch port operation.

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

1Gbps FDX: selects auto-negotiation 1000Mbps and full duplex

100Mbps FDX: selects fixed 100Mbps and full duplex

100Mbps HDX: selects fixed 100Mbps and half duplex

10Mbps FDX: selects fixed 10Mbps and full duplex

10Mbps HDX: selects fixed 10Mbps and half duplex

Flow Control – Current Rx	Whether pause frames on the port are obeyed
---------------------------	---

Flow Control – Current Tx	Whether pause frames on the port are transmitted
---------------------------	--

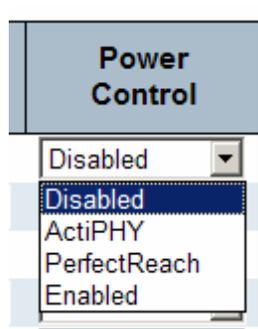
Flow Control – Configured	Click to enable flow control for fixed speed settings.
---------------------------	--

When “Auto” Speed is selected for a port, this selection indicates the flow control capability that is advertised to the link partner.

Maximum Frame Enter the maximum frame size allowed for the switch port, including FCS.
The allowed range is 1518 bytes to 9600 bytes.

Excessive Collision Mode Configure port transmission collision behavior.
Discard: Discard frame after 16 collisions (default).
Restart: Restart back-off algorithm after 16 collisions.

Power Control The Configured column allows for changing the power savings mode parameters per port.



Disabled: All power savings mechanisms are disabled.

ActiPHY: Link down power savings is enabled.

PerfectReach: Link up power savings is enabled.

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

Save	Click to save the 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.

2.3 Security



2.3.1 Switch



2.3.1.1 Users

Users Configuration

Username	Privilege Level
admin	15

Add new user

Configuration	Description
Username	The name identifying the user.
Privilege Level	The privilege level for the user.
Add new user	Click to add a new user.

Add User

User Settings	
Username	<input type="text"/>
Password	<input type="password"/>
Password (again)	<input type="password"/>
Privilege Level	1 <input type="button" value="▼"/>

Save Reset Cancel

Configuration	Description
---------------	-------------

Username	The name identifying the user
Password	The password of the user
Password (again)	Re-enter the configured password.
Privilege Level	The privilege level for the user.

<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.
<input type="button" value="Cancel"/>	Click to go back to Users Configuration.

2.3.1.2 Privilege Levels

Privilege Levels Configuration

Group Name	Privilege levels			
	Configuration Read-only	Configuration/Execute Read-write	Status/Statistics Read-only	Status/Statistics Read-write
Aggregation	5	10	5	10
Debug	15	15	15	15
Diagnostics	5	10	5	10
IGMP_Snooping	5	10	5	10
IP	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
LLDP-MED	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
SNMP	5	10	5	10
Security	5	10	5	10
Spanning_Tree	5	10	5	10
Stack	5	10	1	10
System	5	10	1	10
UPnP	5	10	5	10
VLANs	5	10	5	10
Voice_VLAN	5	10	5	10

Save Reset

Configuration

Description

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 privilege level group has an authorization 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).

Save

Click to save the changes.

Reset

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

2.3.1.3 Auth Method

Authentication Method Configuration

Client	Authentication Method	Fallback
console	local	<input type="checkbox"/>
telnet	local	<input type="checkbox"/>
ssh	local	<input type="checkbox"/>
web	local	<input type="checkbox"/>

Save Reset

Configuration

Description

Client

Access method to the switch – [telnet](#), [ssh](#), web, console

Authentication Method

Authentication 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.

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 something else than 'none' or 'local'.

<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

2.3.1.4 SSH

SSH Configuration

Mode	Disabled ▾
------	------------

Save	Reset
------	-------

Configuration	Description
Mode	Indicates the SSH mode operation. Possible modes are: Enabled: Enable SSH mode operation. Disabled: Disable SSH mode operation.

<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

2.3.1.5 HTTPS

HTTPS Configuration

Mode	Disabled ▾
Automatic Redirect	Disabled ▾

Save	Reset
------	-------

Configuration	Description
Mode	Indicates the HTTPS mode operation. Possible modes are: Enabled: Enable HTTPS mode operation. Disabled: Disable HTTPS mode operation.
Automatic Redirect	Indicates the HTTPS redirect mode operation. Automatic redirect web browser to HTTPS during HTTPS mode enabled. Possible modes are: Enabled: Enable HTTPS redirect mode operation.

Disabled: Disable HTTPS redirect mode operation.

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

2.3.1.6 Access Management Configuration

Access Management Configuration

Mode

Delete Start IP Address End IP Address HTTP/HTTPS SNMP TELNET/SSH

Add new entry

Save Reset

Configuration	Description
Mode	Indicates the access management mode operation. Possible modes are: <i>Enabled:</i> Enable access management mode operation. <i>Disabled:</i> 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 the host can access the switch from HTTP/HTTPS interface that the host IP address matched the entry.
SNMP	Indicates the host can access the switch from SNMP interface that the host IP address matched the entry.
TELNET/SSH	Indicates the host can access the switch from TELNET/SSH interface that the host IP address matched the entry.

Add new entry	Click to add a new access management entry.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.1.7 SNMP

- ▼ SNMP
 - System
 - Communities
 - Users
 - Groups
 - Views
 - Accesses

2.3.1.7.1 System

SNMP System Configuration

Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

SNMP Trap Configuration

Trap Mode	Disabled
Trap Version	SNMP v1
Trap Community	public
Trap Destination Address	
Trap Destination IPv6 Address	::
Trap Authentication Failure	Enabled
Trap Link-up and Link-down	Enabled
Trap Inform Mode	Disabled
Trap Inform Timeout (seconds)	1
Trap Inform Retry Times	5

Save Reset

System Configuration Description

Mode	Indicates the SNMP mode operation. Possible modes are: Enabled: Enable SNMP mode operation. Disabled: Disable SNMP mode operation.
Version	Indicates the SNMP supported version. Possible versions are:

SNMP v1: Set SNMP supported version 1.

SNMP v2c: Set SNMP supported version 2c.

SNMP v3: 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 ~ 255 , and the allowed content is the ASCII characters from 33 to 126. <i>Note: This field only suits when SNMP version is setting SNMPv1 or SNMPv2c. If SNMP version is setting SNMPv3, the community string will 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 use to restrict source subnet.</i>
Write Community	Indicates the community write-access string to permit access to SNMP agent. The allowed string length is 0 ~ 255 , and the allowed content is the ASCII characters from 33 to 126. <i>Note: This field only suits when SNMP mode version setting SNMPv1 or SNMPv2c. If SNMP version is setting SNMPv3, the community string will 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 use to restrict source subnet.</i>
Engine ID	Indicates the SNMPv3 engine ID. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

Trap Configuration	Description
Trap Mode	Indicates the SNMP trap mode operation. Possible modes are: Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation.
Trap Version	Indicates the SNMP trap supported version. Possible versions are: SNMP v1: Set SNMP trap supported version 1. SNMP v2c: Set SNMP trap supported version 2c. SNMP v3: Set SNMP trap supported version 3.
Trap Community	Indicates the community access string when send SNMP trap packet. The allowed string length is 0 ~ 255 , and the allowed content is the 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

separates 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 also used a following legally IPv4 address. For example, '::192.1.2.34'.

- Trap Authentication Failure Indicates the SNMP entity is permitted to generate authentication failure traps. Possible modes are:
Enabled: 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:
Enabled: 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:
Enabled: Enable SNMP trap inform mode operation.
Disabled: Disable SNMP trap inform mode operation.
- Trap Inform Timeout Indicates the SNMP trap inform timeout (seconds). The allowed range is **0 ~ 2147**.
- Trap Inform Retry Times Indicates the SNMP trap inform retry times. The allowed range is **0 ~ 255**.
- Trap Probe Security Engine ID Available for SNMP v3, indicates the SNMP trap probe security engine ID mode of operation. Possible values are:
Enabled: 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 Available for SNMP v3, 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 between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed.
- Trap Security Name Available for SNMP v3, 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.

Save

Click to save the changes.

Reset

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

2.3.1.7.2 Communities

Delete	Community	Source IP	Source Mask
<input type="checkbox"/>	public	0.0.0.0	0.0.0.0
<input type="checkbox"/>	private	0.0.0.0	0.0.0.0
Delete		0.0.0.0	0.0.0.0

Configuration	Description
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 the ASCII characters from 33 to 126. The community string will treat 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 use to restrict source subnet when combined with source mask.
Source Mask	Indicates the SNMP access source address mask.

Click to add a new community entry as shown below.

Delete		0.0.0.0	0.0.0.0
--------	--	---------	---------

<input type="button" value="Delete"/>	Click to cancel the new entry.
<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

2.3.1.7.3 Users

SNMPv3 Users Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="checkbox"/>	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

Add new user

Save

Reset

Configuration	Description
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 between 10 and 64 hexadecimal digits, 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 usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID 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 the ASCII characters from 33 to 126.
Security Level	Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv: None authentication and none privacy. Auth, NoPriv: Authentication and none privacy. Auth, Priv: Authentication and privacy. The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
Authentication Protocol	Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are: None: None authentication protocol. MD5: An optional flag to indicate that this user using MD5 authentication protocol. SHA: An optional flag to indicate that this user using 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 pass 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 the ASCII characters from 33 to 126.

Privacy Protocol

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

None: None privacy protocol.

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

Privacy Password

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

Click to add a new SNMPv3 user entry as shown below.

Click to cancel the new entry.

Click to save the changes.

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

2.3.1.7.4 Groups

SNMPv3 Groups Configuration

Delete	Security Model	Security Name	Group Name
<input type="checkbox"/>	v1	public	default_ro_group
<input type="checkbox"/>	v1	private	default_rw_group
<input type="checkbox"/>	v2c	public	default_ro_group
<input type="checkbox"/>	v2c	private	default_rw_group
<input type="checkbox"/>	usm	default_user	default_rw_group

Add new group

Save

Reset

Configuration

Description

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 the 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 the ASCII characters from 33 to 126.

Add new group

Click to add a new SNMPv3 group entry as shown below.

Delete

v1

public

Delete

Click to cancel the new entry.

Save

Click to save the changes.

Reset

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

2.3.1.7.5 Views

SNMPv3 Views Configuration

Delete	View Name	View Type	OID Subtree
<input type="checkbox"/>	default_view	included ▼	.1

Add new view

Save

Reset

Configuration	Description
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 the ASCII characters from 33 to 126.
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. General, if a view entry's view type is 'excluded', it should be exist another view entry which view type is 'included' and it's OID sub-tree 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(*).

Add new view

Click to add a new SNMPv3 view entry as shown below.

Delete	<input type="text"/>	included ▼	<input type="text"/>
--------	----------------------	------------	----------------------

Delete

Click to cancel the new entry.

Save

Click to save the changes.

Reset

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

2.3.1.7.6 Accesses

SNMPv3 Accesses Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="checkbox"/>	default_ro_group	any	NoAuth, NoPriv	default_view ▼	None ▼
<input type="checkbox"/>	default_rw_group	any	NoAuth, NoPriv	default_view ▼	default_view ▼

Add new access

Save

Reset

Configuration	Description
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 the ASCII characters from 33 to 126.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: any : Accepted any security model (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 : None authentication and none privacy. Auth, NoPriv : Authentication and none 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 the 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 the ASCII characters from 33 to 126.

Add new access

Click to add a new SNMPv3 view entry as shown below.

Delete	default_ro_group ▼	any ▼	NoAuth, NoPriv ▼	None ▼	None ▼
--------	--------------------	-------	------------------	--------	--------

Delete

Click to cancel the new entry.

Save

Click to save the changes.

Reset

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

2.3.2 Network

- ▼ Network
 - Limit Control
 - NAS
 - ▶ ACL
 - ▶ DHCP
 - ▶ IP Source Guard
 - ▶ ARP Inspection

2.3.2.1 Limit Control

Port Limit Control Configuration

System Configuration (Stack Global)

Mode	Disabled
Aging Enabled	<input type="checkbox"/>
Aging Period	3600 seconds

Port Configuration for Switch 2

Port	Mode	Limit	Action	State	Reopen
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Disabled	4	None	Disabled	Reopen
5	Disabled	4	None	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen
9	Disabled	4	None	Disabled	Reopen
10	Disabled	4	None	Disabled	Reopen
11	Disabled	4	None	Disabled	Reopen
12	Disabled	4	None	Disabled	Reopen
13	Disabled	4	None	Disabled	Reopen
14	Disabled	4	None	Disabled	Reopen
15	Disabled	4	None	Disabled	Reopen
16	Disabled	4	None	Disabled	Reopen
17	Disabled	4	None	Disabled	Reopen
18	Disabled	4	None	Disabled	Reopen
19	Disabled	4	None	Disabled	Reopen
20	Disabled	4	None	Disabled	Reopen
21	Disabled	4	None	Disabled	Reopen
22	Disabled	4	None	Disabled	Reopen
23	Disabled	4	None	Disabled	Reopen
24	Disabled	4	None	Disabled	Reopen

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 four different as described below. The Limit Control module is one of a range of modules that utilizes a lower-layer module, the Port Security module, which manages MAC addresses learned on the port.

Configuration	Description
Mode	Indicates if Limit Control is globally enabled or disabled on the switch stack. 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 Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the 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	The port number for 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 stack 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 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 stack or elect a new master switch,
- 2) Disable and re-enable Limit Control on the port or the stack,
- 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".

[Reopen](#)

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.

[Save](#)

Click to save the changes.

[Reset](#)

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

2.3.2.2 NAS

This page allows you to configure the [IEEE 802.1X](#) and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the Authentication configuration page.

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 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 the 802.1X authentication.

Network Access Server Configuration

System Configuration (Stack Global)

Mode	Disabled	
Reauthentication Enabled	<input type="checkbox"/>	
Reauthentication Period	3600	seconds
EAPOL Timeout	30	seconds
Age Period	300	seconds
Hold Time	10	seconds
RADIUS-Assigned QoS Enabled	<input type="checkbox"/>	
RADIUS-Assigned VLAN Enabled	<input type="checkbox"/>	
Guest VLAN Enabled	<input type="checkbox"/>	
Guest VLAN ID	1	
Max. Reauth. Count	2	
Allow Guest VLAN if EAPOL Seen	<input type="checkbox"/>	

Port Configuration for Switch 2

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
1	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
7	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
8	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
9	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
10	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
11	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
12	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
13	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
14	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
15	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
16	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
17	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
18	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
19	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
20	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
21	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
22	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
23	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
24	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize

Save Reset

System Configuration Description

- Mode** Indicates if NAS is globally enabled or disabled on the switch stack. 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 [Age 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 between retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 255 seconds. This has no effect for MAC-based

ports.

Age 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 a 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→Security→AAA" page) - the client is put on hold in the Un-authorized state. The hold timer does not count during an on-going authentication. In MAC-based Auth. mode, the 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 for that port. When unchecked, RADIUS-server assigned QoS Class is disabled for 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 (see RADIUS-Assigned VLAN Enabled below for a detailed description). The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned VLAN is enabled for that port. When unchecked, RADIUS-server assigned VLAN is disabled for 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 for 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

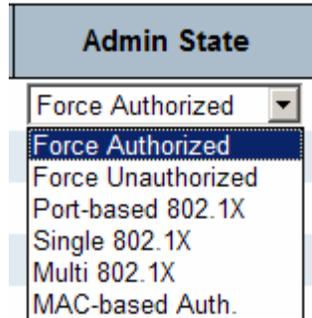
The number of times that the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1: 255].

Allow Guest VLAN if EAPOL Seen

The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port. The value can only be changed if the Guest VLAN option is

globally enabled.

Port Configuration	Description
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: In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Multi 802.1X variant. Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC

table using the Port Security module.

In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.

The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

MAC-based Auth.: Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

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

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

Limit Control functionality.

RADIUS-Assigned QoS Enabled

When RADIUS-Assigned QoS is both globally enabled and enabled (checked) for a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

This option is only available for single-client modes, i.e.

- Port-based 802.1X
- Single 802.1X

RADIUS attributes used in identifying a QoS Class:

Refer to the written documentation for a description of the RADIUS attributes needed in order to successfully identify a QoS Class. The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.

Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

- All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '3', which translates into the desired QoS Class in the range [0; 3].

RADIUS-Assigned VLAN Enabled

When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

This option is only available for single-client modes, i.e.

- Port-based 802.1X
- Single 802.1X

For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show that 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-ID attributes 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-ID does 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 that 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 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 to 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.

Save

Click to save the changes.

Reset

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

2.3.2.3 ACL

- ▼ ACL
 - Ports
 - Rate Limiters
 - Access Control List

2.3.2.3.1 Ports

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. The settings relate to the currently selected stack unit, as reflected by the page header.

ACL Ports Configuration for Switch 2

Port	Policy ID	Action	Rate Limiter ID	Port Copy	Shutdown	Counter
1	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
2	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
3	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
4	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
5	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
6	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
7	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
8	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
9	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
10	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
11	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
12	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
13	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
14	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
15	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
16	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
17	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
18	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
19	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
20	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
21	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
22	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
23	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0
24	1 ▼	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	0

Save Reset

Configuration	Description
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 <i>1 ~ 8</i> . The default value is 1.
Action	Select whether forwarding is permitted (" <i>Permit</i> ") or denied (" <i>Deny</i> "). The default value is "Permit".
Rate Limiter ID	Select which rate limiter to apply to this port. The allowed values are <i>Disabled</i> or the values <i>1 ~ 15</i> . The default value is " <i>Disabled</i> ".
Port Copy	Select which port frames are copied to. The allowed values are <i>Disabled</i> or a specific port number. The default value is " <i>Disabled</i> ".
Shutdown	Specify the port shut down operation of this port. The allowed values are: <i>Enabled</i> : If a frame is received on the port, the port will be disabled. <i>Disabled</i> : Port shut down is disabled. The default value is "Disabled".
Counter	Counts the number of frames that match this ACE.
<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.
<input type="button" value="Clear"/>	Click to clear the counters.

2.3.2.3.2 Rate Limiters

ACL Rate Limiter Configuration

Rate Limiter ID	Rate (pps)
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	1

Save Reset

Configuration	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
Rate	The rate unit is packet per second (pps), configure the rate as <i>1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K</i> . The 1 kpps is actually 1024 pps.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.2.3.3 Access Control Lists

Access Control List Configuration

Auto-refresh Refresh Clear Remove All

Ingress Port	Frame Type	Action	Rate Limiter	Port Copy	Logging	Shutdown	Counter
+							

Configuration	Description
Ingress Port	Indicates the ingress port of the ACE. Possible values are:

	<p>Any: The ACE will match any ingress port.</p> <p>Policy: The ACE will match ingress ports with a specific policy.</p> <p>Port: The ACE will match a specific ingress port.</p>
Frame Type	<p>Indicates the frame type of the ACE. Possible values are:</p> <p>Any: The ACE will match any frame type.</p> <p>EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.</p> <p>ARP: The ACE will match ARP/RARP frames.</p> <p>IPv4: The ACE will match all IPv4 frames.</p> <p>IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.</p> <p>IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.</p> <p>IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.</p> <p>IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.</p>
Action	<p>Indicates the forwarding action of the ACE.</p> <p>Permit: Frames matching the ACE may be forwarded and learned.</p> <p>Deny: Frames matching the ACE are dropped.</p>
Rate Limiter	<p>Indicates the rate limiter number of the ACE. The allowed range is 1 ~ 15. When “Disabled” is displayed, the rate limiter operation is disabled.</p>
Port Copy	<p>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.</p>
Logging	<p>Indicates the logging operation of the ACE. Possible values are:</p> <p>Enabled: Frames matching the ACE are stored in the System Log.</p> <p>Disabled: Frames matching the ACE are not logged.</p> <p>Please note that the System Log memory size and logging rate is limited.</p>
Shutdown	<p>Indicates the port shut down operation of the ACE. Possible values are:</p> <p>Enabled: If a frame matches the ACE, the ingress port will be disabled.</p> <p>Disabled: Port shut down is disabled for the ACE.</p>
Counter	<p>The counter indicates the number of times the ACE was hit by a frame.</p>
Auto-refresh	<p>Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.</p>

ACE modification buttons:

-  Inserts a new ACE before the current row.
-  Edits the ACE.
-  Moves the ACE up the list.
-  Moves the ACE down the list.

(X)

Deletes the ACE.

(+)

The lowest plus sign adds a new entry at the bottom of the list of ACL.

Refresh

Click to refresh the page; any changes made locally will be undone.

Clear

Click to clear the counters.

Remove All

Click to remove all ACEs.

Remark: The maximum number of ACEs is 128.

2.3.2.4 DHCP

- ▼ DHCP
 - Snooping
 - Relay

2.3.2.4.1 Snooping

DHCP Snooping Configuration

Stack Global Settings

Snooping Mode	Disabled ▼
	Disabled
	Enabled

Port Mode Configuration for Switch 2

Port	Mode
1	Trusted ▼
2	Trusted ▼
3	Trusted ▼
4	Trusted ▼
5	Trusted ▼
6	Trusted ▼
7	Trusted ▼
8	Trusted ▼
9	Trusted ▼
10	Trusted ▼
11	Trusted ▼
12	Trusted ▼
13	Trusted ▼
14	Trusted ▼
15	Trusted ▼
16	Trusted ▼
17	Trusted ▼
18	Trusted ▼
19	Trusted ▼
20	Trusted ▼
21	Trusted ▼
22	Trusted ▼
23	Trusted ▼
24	Trusted ▼

Save	Reset
------	-------

Configuration	Description
Snooping Mode	Indicates the DHCP snooping mode operation. Possible modes are: Enabled: Enable DHCP snooping mode operation. When enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed 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 sources of the DHCP message. Untrusted: Configures the port as untrusted sources of the DHCP message.
<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

2.3.2.4.2 Relay

DHCP Relay Configuration

Relay Mode	Disabled
Relay Server	0.0.0.0
Relay Information Mode	Disabled
Relay Information Policy	Replace

Replace

Keep

Drop

Configuration	Description
Relay Mode	Indicates the DHCP relay mode operation. Possible modes are: Enabled: Enable DHCP relay mode operation. When enable DHCP relay mode operation, the agent forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain. And the DHCP broadcast message won't flood for security considered. 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 on the same subnet domain.
Relay Information Mode	Indicates the DHCP relay information mode option operation. Possible modes are: Enabled: Enable DHCP relay information mode operation. When enable DHCP relay information mode operation, the agent insert specific information (option 82) into a

DHCP message when forwarding to DHCP server and remove it from a DHCP message when transferring to DHCP client. It only works under DHCP relay operation mode enabled.

Disabled: Disable DHCP relay information mode operation.

Relay Information Policy Indicates the DHCP relay information option policy. When enable DHCP relay information mode operation, if agent receives a DHCP message that already contains relay agent information. It will enforce the policy. And it only works under DHCP relay information operation mode enabled. Possible policies are:

Replace: Replace the original relay information when receive a DHCP message that already contains it.

Keep: Keep the original relay information when receive a DHCP message that already contains it.

Drop: Drop the package when receive a DHCP message that already contains relay information.

Save

Click to save the changes.

Reset

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

2.3.2.5 IP Source Guard

- ▼ IP Source Guard
 - Configuration
 - Static Table

2.3.2.5.1 Configuration

IP Source Guard Configuration

Stack Global Settings

Mode

Port Mode Configuration for Switch 2

Port	Mode	Max Dynamic Clients
1	Disabled	Unlimited
2	Disabled	0
3	Disabled	1
4	Disabled	2
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited
7	Disabled	Unlimited
8	Disabled	Unlimited
9	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
23	Disabled	Unlimited
24	Disabled	Unlimited

Configuration	Description
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 can be learned on given ports. This value can be 0, 1, 2 and unlimited. If the port mode is enabled and the value of max dynamic client is equal 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.
<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

2.3.2.5.2 Static Table

Static IP Source Guard Table for Switch 2

Delete	Port	VLAN ID	IP Address	IP Mask
<input type="button" value="Delete"/>	1 ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>

Configuration	Description
<input type="button" value="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.
IP Mask	It can be used for calculating the allowed network with IP address.
<input type="button" value="Add new entry"/>	Click to add a new entry to the Static IP Source Guard table. Specify the Port, VLAN ID, IP address, and IP Mask for the new entry. Click "Save".
<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

2.3.2.6 ARP Inspection

- ▼ ARP Inspection
 - Configuration
 - Static Table

2.3.2.6.1 Configuration

ARP Inspection Configuration

Stack Global Settings

Mode

Port Mode Configuration for Switch 2

Port	Mode
1	<input type="text" value="Disabled"/>
2	<input type="text" value="Disabled"/>
3	<input type="text" value="Disabled"/>
4	<input type="text" value="Disabled"/>
5	<input type="text" value="Disabled"/>
6	<input type="text" value="Disabled"/>
7	<input type="text" value="Disabled"/>
8	<input type="text" value="Disabled"/>
9	<input type="text" value="Disabled"/>
10	<input type="text" value="Disabled"/>
11	<input type="text" value="Disabled"/>
12	<input type="text" value="Disabled"/>
13	<input type="text" value="Disabled"/>
14	<input type="text" value="Disabled"/>
15	<input type="text" value="Disabled"/>
16	<input type="text" value="Disabled"/>
17	<input type="text" value="Disabled"/>
18	<input type="text" value="Disabled"/>
19	<input type="text" value="Disabled"/>
20	<input type="text" value="Disabled"/>
21	<input type="text" value="Disabled"/>
22	<input type="text" value="Disabled"/>
23	<input type="text" value="Disabled"/>
24	<input type="text" value="Disabled"/>

Configuration	Description
Stack Mode	Enable the Global ARP Inspection or disable the Global ARP Inspection.
Port Mode	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.
<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

2.3.2.6.2 Static Table

Static ARP Inspection Table for Switch 2

Delete	Port	VLAN ID	MAC Address	IP Address
<input type="button" value="Delete"/>	1 ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>

Configuration	Description
<input type="button" value="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.
MAC Address	Allowed Source MAC address in ARP request packets.
IP Address	Allowed Source IP address.
<input type="button" value="Add new entry"/>	Click to add a new entry to the Static ARP table. Specify the Port, VLAN ID, IP address, and MAC address for the new entry. Click "Save".
<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

2.3.3 AAA

Authentication Server Configuration

Common Server Configuration

Timeout	<input type="text" value="15"/>	seconds
Dead Time	<input type="text" value="300"/>	seconds

RADIUS Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="1812"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="1812"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="1812"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="1812"/>	<input type="text"/>
5	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="1812"/>	<input type="text"/>

RADIUS Accounting Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="1813"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="1813"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="1813"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="1813"/>	<input type="text"/>
5	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="1813"/>	<input type="text"/>

TACACS+ Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="49"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="49"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="49"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="49"/>	<input type="text"/>
5	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="49"/>	<input type="text"/>

Common Server	Description
---------------	-------------

Timeout

The Timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server. If the server does not reply within this timeframe, we will consider it to be dead and continue with the next enabled server (if any).

RADIUS servers are using the [UDP](#) protocol, which is unreliable by design. In order

to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.

Dead Time

The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

RADIUS Authentication Server Configuration

#	The RADIUS authentication server number for which the configuration applies
Enabled	Enable the server by checking this box.
IP Address(Hostname)	The IP address of the server expressed in dotted decimal notation .
Port	The UDP port to use on the server. If the port is set to zero (0), the default port (1812) is used for the server.
Secret	The secret - up to 29 characters long - shared between the server and the switch unit.

RADIUS Accounting Server Configuration

#	The RADIUS accounting server number for which the configuration applies
Enabled	Enable the server by checking this box.
IP Address(Hostname)	The IP address of the server expressed in dotted decimal notation .
Port	The UDP port to use on the server. If the port is set to zero (0), the default port (1812) is used for the server.
Secret	The secret - up to 29 characters long - shared between the server and the switch unit.

TACACS+ Authentication Server Configuration

#	The TACACS+ authentication server number for which the configuration applies
Enabled	Enable the server by checking this box.
IP Address(Hostname)	The IP address of the server expressed in dotted decimal notation .
Port	The UDP port to use on the server. If the port is set to zero (0), the default port (1812) is used for the server.
Secret	The secret - up to 29 characters long - shared between the server and the switch unit.

<input type="button" value="Save"/>	Click to save the changes.
-------------------------------------	----------------------------

<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.
--------------------------------------	---

2.4 Aggregation

The Port Link Aggregation function can combine multiple physical switched ports, called “Aggregation Group” into one logical port. It allows making connection between two switches using more than one physical links to increase the connection bandwidth between two switches. Two aggregation modes, “Static” and “LACP” are supported.

- ▼ Aggregation
 - Static
 - LACP

2.4.1 Static

Aggregation Mode Configuration

Stack Global Settings

Hash Code Contributors	
Source MAC Address	<input checked="" type="checkbox"/>
Destination MAC Address	<input type="checkbox"/>
IP Address	<input checked="" type="checkbox"/>
TCP/UDP Port Number	<input checked="" type="checkbox"/>

Aggregation Group Configuration for Switch 2

		Port Members																							
Locality	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
	Normal	<input checked="" type="checkbox"/>																							
Global	1	<input type="checkbox"/>																							
Global	2	<input type="checkbox"/>																							
Local	1	<input type="checkbox"/>																							
Local	2	<input type="checkbox"/>																							
Local	3	<input type="checkbox"/>																							
Local	4	<input type="checkbox"/>																							
Local	5	<input type="checkbox"/>																							
Local	6	<input type="checkbox"/>																							
Local	7	<input type="checkbox"/>																							
Local	8	<input type="checkbox"/>																							
Local	9	<input type="checkbox"/>																							
Local	10	<input type="checkbox"/>																							
Local	11	<input type="checkbox"/>																							
Local	12	<input type="checkbox"/>																							

Save Reset

Global Configuration **Description**

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

Locality	Indicates the aggregation group type. This field is only valid for stackable switches. Global: The group members may reside on different units in the stack. The device supports two 8-port global aggregations. Local: The group members reside on the same unit. Each local aggregation may consist of up to 16 members.
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.

Click to save the changes.

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

*Note:**The maximum number of global groups is 2. The number of member ports is up to 8.**The maximum number of local groups is 12. The number of member ports is up to 16.*

2.4.2 LACP

LACP Port Configuration

Port	LACP Enabled	Key	Role
1	<input type="checkbox"/>	Auto <input type="text"/>	Active <input type="text"/>
2	<input type="checkbox"/>	Auto <input type="text"/>	Active <input type="text"/>
3	<input type="checkbox"/>	Auto <input type="text"/>	Active <input type="text"/>
4	<input type="checkbox"/>	Auto <input type="text"/>	Active <input type="text"/>
5	<input type="checkbox"/>	Auto <input type="text"/>	Active <input type="text"/>
6	<input type="checkbox"/>	Auto <input type="text"/>	Active <input type="text"/>
7	<input type="checkbox"/>	Auto <input type="text"/>	Active <input type="text"/>
8	<input type="checkbox"/>	Auto <input type="text"/>	Active <input type="text"/>
9	<input type="checkbox"/>	Auto <input type="text"/>	Active <input type="text"/>
10	<input type="checkbox"/>	Auto <input type="text"/>	Active <input type="text"/>
11	<input type="checkbox"/>	Auto <input type="text"/>	Active <input type="text"/>
12	<input type="checkbox"/>	Auto <input type="text"/>	Active <input type="text"/>
13	<input type="checkbox"/>	Auto <input type="text"/>	Active <input type="text"/>
14	<input type="checkbox"/>	Auto <input type="text"/>	Active <input type="text"/>
15	<input type="checkbox"/>	Auto <input type="text"/>	Active <input type="text"/>
16	<input type="checkbox"/>	Auto <input type="text"/>	Active <input type="text"/>

Configuration	Description
Port	The port number for which the associated row configuration applies
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 . Auto: set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Specific: 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 link partner (speak if spoken to).
<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

Note: LLAG means Local Link aggregation Group. GLAG means Global Link aggregation Group.

2.5 Spanning Tree

This section is used to set configuration for supporting Spanning Tree protocols including [STP](#), [RSTP](#), and MSTP.

- ▼ Spanning Tree
 - Bridge Settings
 - MSTI Mapping
 - MSTI Priorities
 - CIST Ports
 - MSTI Ports

2.5.1 Bridge Settings

STP Bridge Configuration

Basic Settings

Protocol Version	MSTP
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	<input style="width: 100%;" type="text"/>

Save

Reset

Basic Configuration	Description
Protocol Version	The STP protocol version setting Valid values: <i>STP, RSTP, MSTP</i>
Forward Delay	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values: <i>4 ~ 30 seconds</i>
Max Age	The maximum age of the information transmitted by the Bridge when it is the Root Bridge Valid values: <i>6 ~ 40 seconds (Max Age must be $\leq (FwdDelay-1)*2$)</i>
Maximum Hop Count	It defines how many bridges a root bridge can distribute its BPDU information. This

defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region.

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: *1 ~ 10 BPDU's per second*

Advanced Configuration

Edge Port BPDU Filtering Check to configure a port *explicitly* 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 that has to pass before a port in the *error-disabled* state can be enabled.

Valid values: *30 ~ 86400 seconds (24 hours)*

Click to save the changes.

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

2.5.2 MSTI Mapping

MSTI Configuration

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name	00-40-f6-e9-10-cf
Configuration Revision	0

MSTI Mapping	
MSTI	VLANs Mapped
MST1	
MST2	
MST3	
MST4	
MST5	
MST6	
MST7	

Configuration	Description
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 <i>0</i> ~ <i>65535</i> .

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 VLAN's mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to <i>one</i> MSTI. An unused MSTI should just be left empty. (i.e. not having any VLANs mapped to it.)

Save

Click to save the changes.

Reset

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

2.5.3 MSTI Priorities

MSTI Configuration

MSTI Priority Configuration	
MSTI	Priority
CIST	128
MST1	128
MST2	128
MST3	128
MST4	128
MST5	128
MST6	128
MST7	128

Save Reset

Configuration

Description

MSTI

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

Priority

Controls the bridge priority. Lower numerical 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*.

Save

Click to save the changes.

Reset

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

2.5.4 CIST Ports

STP CIST Ports Configuration

CIST Aggregated Ports Configuration										
Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
-	<input checked="" type="checkbox"/>	Auto		128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True

CIST Normal Ports Configuration										
Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
1	<input checked="" type="checkbox"/>	Auto		128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
2	<input checked="" type="checkbox"/>	Auto		128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
3	<input checked="" type="checkbox"/>	Auto		128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
4	<input checked="" type="checkbox"/>	Auto		128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
5	<input checked="" type="checkbox"/>	Auto		128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
6	<input checked="" type="checkbox"/>	Auto		128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
7	<input checked="" type="checkbox"/>	Auto		128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
8	<input checked="" type="checkbox"/>	Auto		128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
9	<input checked="" type="checkbox"/>	Auto		128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
10	<input checked="" type="checkbox"/>	Auto		128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
11	<input checked="" type="checkbox"/>	Auto		128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
12	<input checked="" type="checkbox"/>	Auto		128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

Configuration

Description

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 <i>Auto</i> setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the <i>Specific</i> setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values: <i>1 to 200000000</i>
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
AdminEdge	Controls whether the <i>operEdge</i> flag should start as being set or cleared. (The initial <i>operEdge</i> state when a port is initialized). <i>operEdge: Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transitioning to the forwarding state is faster for edge ports (having operEdge true) than for other ports.</i>
AutoEdge	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 influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as **Root Guard**.

Restricted TCN

If enabled, 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 persistent incorrectly 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 is the physical link state for the attached LANs transitions frequently.

BPDU Guard

If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port *Edge* status does not affect 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 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.

Save

Click to save the changes.

Reset

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

Note: This configuration applies to physical and Link Aggregation ports.

2.5.5 MSTI Ports

A MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured and applicable for 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.

MSTI Port Configuration

Select MSTI

MST1

- MST1
- MST2
- MST3
- MST4
- MST5
- MST6
- MST7

Configuration	Description
MSTI	Select an MSTI for pop-up configuration.
<input type="button" value="Get"/>	Click to pop-up configuration page.

MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost	Priority
-	Auto <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>

MSTI Normal Ports Configuration

Port	Path Cost	Priority
1	Auto <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>
2	Auto <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>
3	Auto <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>
4	Auto <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>
5	Auto <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>
6	Auto <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>
7	Auto <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>
8	Auto <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>
9	Auto <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>
10	Auto <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>
11	Auto <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>
12	Auto <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>
13	Auto <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="v"/>

Configuration	Description (Example with MSTI1)
Port	The switch port number of the corresponding STP CIST (and MSTI) port.
Path Cost	Controls the path cost incurred by the port. The <i>Auto</i> setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the <i>Specific</i> setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values: <i>1 ~ 20000000</i>
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

2.6 IGMP Snooping

- ▼ IGMP Snooping
 - Basic Configuration
 - VLAN Configuration
 - Port Group Filtering

2.6.1 Basic Configuration

IGMP Snooping Configuration

Stack Global Settings

Global Configuration	
Snooping Enabled	<input type="checkbox"/>
Unregistered IPMC Flooding enabled	<input type="checkbox"/>
Leave Proxy Enabled	<input type="checkbox"/>

Port Related Configuration for Switch 2

Port	Router Port	Fast Leave	Throttling
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
11	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
12	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
13	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
14	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
15	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
16	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
17	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
18	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
19	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
20	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
21	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
22	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
23	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
24	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼

Save Reset

Global Configuration Description

Snooping Enabled	Enable the Global IGMP Snooping.
Unregistered IPMC Flooding enabled	Enable unregistered IPMC traffic flooding.

Port Configuration Description

Port	The port number for which the row configuration applies
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.
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.

<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

2.6.2 VLAN Configuration

IGMP Snooping VLAN Configuration

Start from VLAN with entries per page.

VLAN ID	Snooping Enabled	IGMP Querier
1	<input type="checkbox"/>	<input type="checkbox"/>

VLAN Configuration Description

Start from VLAN	Select range of VLAN table entries.
VLAN ID	The VLAN ID of the entry.
Snooping Enabled	Enable the per-VLAN IGMP Snooping.
IGMP Querier	Enable the IGMP Querier in the VLAN. The Querier will send out if no Querier received in 255 seconds after IGMP Querier Enabled. Each Querier's interval is 125 second, and it will stop act as an IGMP Querier if received any Querier from other devices.

<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.
--	---



Click to display the first page.



Click to display the last page.



Click to save the changes.



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

2.6.3 Port Group Filtering

IGMP Snooping Port Group Filtering Configuration for Switch 2

Delete	Port	Filtering Groups
Delete	1 ▼	<input type="text"/>

Configuration

Description

<input type="button" value="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.
<input type="button" value="Add 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".
<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

2.7 MVR

MVR Configuration

Stack Global Settings

MVR Mode	Disabled ▾
VLAN ID	100

Port Configuration for Switch 2

Port	Mode	Type	Immediate Leave
1	Disabled ▾	Receiver ▾	Disabled ▾
2	Disabled ▾	Receiver ▾	Disabled ▾
3	Disabled ▾	Receiver ▾	Disabled ▾
4	Disabled ▾	Receiver ▾	Disabled ▾
5	Disabled ▾	Receiver ▾	Disabled ▾
6	Disabled ▾	Receiver ▾	Disabled ▾
7	Disabled ▾	Receiver ▾	Disabled ▾
8	Disabled ▾	Receiver ▾	Disabled ▾
9	Disabled ▾	Receiver ▾	Disabled ▾
10	Disabled ▾	Receiver ▾	Disabled ▾
11	Disabled ▾	Receiver ▾	Disabled ▾
12	Disabled ▾	Receiver ▾	Disabled ▾
13	Disabled ▾	Receiver ▾	Disabled ▾
14	Disabled ▾	Receiver ▾	Disabled ▾
15	Disabled ▾	Receiver ▾	Disabled ▾
16	Disabled ▾	Receiver ▾	Disabled ▾
17	Disabled ▾	Receiver ▾	Disabled ▾
18	Disabled ▾	Receiver ▾	Disabled ▾
19	Disabled ▾	Receiver ▾	Disabled ▾
20	Disabled ▾	Receiver ▾	Disabled ▾
21	Disabled ▾	Receiver ▾	Disabled ▾
22	Disabled ▾	Receiver ▾	Disabled ▾
23	Disabled ▾	Receiver ▾	Disabled ▾
24	Disabled ▾	Receiver ▾	Disabled ▾

Save | Reset

Configuration

Description

MVR Mode	Enable/Disable the Global MVR.
VLAN ID	Specify the Multicast VLAN ID.
Mode	Enable MVR on the port.
Type	Specify the MVR port type on the port.
Immediate Leave	Enable the fast leave on the port

Save

Click to save the changes.

Reset

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

2.8 LLDP

- ▼ LLDP
 - LLDP
 - LLDP-MED

2.8.1 LLDP

LLDP Configuration

LLDP Parameters

Tx Interval	<input type="text" value="30"/>	seconds
Tx Hold	<input type="text" value="3"/>	times
Tx Delay	<input type="text" value="2"/>	seconds
Tx Reinit	<input type="text" value="2"/>	seconds

LLDP Port Configuration for Switch 2

Port	Mode	CDP aware	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
1	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
2	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
3	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
4	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
5	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
6	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
7	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
8	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
9	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
10	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
11	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
12	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
13	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
14	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
15	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
16	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
17	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
18	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
19	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
20	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
21	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
22	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
23	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
24	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				

Global Configuration	Description
Tx Interval	<p>The switch is periodically transmitting LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value.</p> <p>Valid values: 5 – 32768 seconds</p>
Tx Hold	<p>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.</p> <p>Valid values: 2 – 10 times</p>
Tx Delay	<p>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.</p> <p>Valid values: 1 – 8192 seconds</p>
Tx Reinit	<p>When a port is disabled, LLDP is disabled or the switch is rebooted a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization.</p> <p>Valid values: 1 – 10 seconds</p>
Port Configuration	
Port	The switch port number of the logical LLDP port.
Mode	<p>Select LLDP mode.</p> <p>Rx only: The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.</p> <p>Tx only: The switch will drop LLDP information received from neighbors, but will send out LLDP information.</p> <p>Disabled: The switch will not send out LLDP information, and will drop LLDP information received from neighbors.</p> <p>Enabled: The switch will send out LLDP information, and will analyze LLDP information received from neighbors.</p>
CDP Aware	<p>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 for the port is enabled.</p> <p>Only CDP TLVs that can be mapped into a corresponding field in the LLDP neighbors table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frame are not shown in the LLDP statistic. Only). CDP TLVs are mapped into LLDP neighbors table as shown below.</p>

CDP TLV "Device ID" is mapped into the LLDP "Chassis ID" field.

CDP TLV "Address" is mapped into the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table.

CDP TLV "Port ID" is mapped into the LLDP "Port ID" field.

CDP TLV "Version and Platform" is mapped into the LLDP "System Description" field.

Both the CDP and LLDP supports "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors table.

If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch.

Note: When CDP awareness for a port is disabled the CDP information isn't removed immediately, but will be removed when the hold time is exceeded.

Optional TLV

Port Descr	When checked the "port description" is included in LLDP information transmitted.
Sys Name	When checked the "system name" is included in LLDP information transmitted.
Sys Descr	When checked the "system description" is included in LLDP information transmitted.
Sys Capa	When checked the "system capability" is included in LLDP information transmitted.
Mgmt Addr	When checked the "management address" is included in LLDP information transmitted.

Click to save the changes.

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

2.8.2 LLDP-MED

LLDPMED Configuration

Fast Start Repeat Count

Fast start repeat count

Coordinates Location

Latitude degrees Longitude degrees Altitude Meters Map Datum

Civic Address Location

Country code	<input type="text"/>	State	<input type="text"/>	County	<input type="text"/>
City	<input type="text"/>	City district	<input type="text"/>	Block (Neighborhood)	<input type="text"/>
Street	<input type="text"/>	Leading street direction	<input type="text"/>	Trailing street suffix	<input type="text"/>
Street suffix	<input type="text"/>	House no.	<input type="text"/>	House no. suffix	<input type="text"/>
Landmark	<input type="text"/>	Additional location info	<input type="text"/>	Name	<input type="text"/>
Zip code	<input type="text"/>	Building	<input type="text"/>	Apartment	<input type="text"/>
Floor	<input type="text"/>	Room no.	<input type="text"/>	Place type	<input type="text"/>
Postal community name	<input type="text"/>	P.O. Box	<input type="text"/>	Additional code	<input type="text"/>

Emergency Call Service

Emergency Call Service

Policies

Delete	Policy Id	Application Type	Tag	VLAN ID	L2 Priority	DSCP
Delete	0	Voice	Tagged	1	0	0

Add new policy

Policy Port Configuration for Switch 2

Save Reset

Configuration	Description
Fast start repeat count	The number of times the fast start transmission is repeated. The recommended value is 4 times, giving that 4 LLDP frames with a 1 second interval will be transmitted, when a LLDP frame with new information is received.

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 <i>North</i> of the equator or <i>South</i> of the equator.
Longitude	Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either <i>East</i> of the prime meridian or <i>West</i> 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 used for the coordinates given in this Option
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

Country code The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
State National subdivisions (state, canton, region, province, prefecture).
County County, parish, gun (Japan), district.
City City, township, shi (Japan) - Example: Copenhagen
City district City division, borough, city district, ward, chou (Japan)
Block (Neighborhood) Neighborhood, 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 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.

[Add New Policy](#) Click to configure a new policy.

Policies

Delete	Policy Id	Application Type	Tag	VLAN ID	L2 Priority	DSCP
Delete	0	Voice	Tagged	1	0	0

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 policies that shall be mapped to the specific ports.

Application Type Intended use of the application types:

1. **Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. **Voice Signaling** (conditional) - for use in network topologies that require a different policy for the voice signaling 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 Signaling** (conditional) - for use in network topologies that require a

different policy for the guest voice signaling 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**

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 Signaling** (conditional) - for use in network topologies that require a separate policy for the video signaling 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 behavior 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.

Port Policies Configuration

Port	The port number for which the configuration applies.
Policy Id	The set of policies that shall apply for a given port The set of policies is selected by checkmarking the checkboxes that corresponds to the policies

<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

Civic Address Location

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

Emergency Call Service

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

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:

1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control / Signaling (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.

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.

2.9 PoE

Power Over Ethernet Configuration

Power Over Ethernet Stack Configuration

Reserved Power determined by	<input type="radio"/> Class	<input checked="" type="radio"/> Allocation	<input type="radio"/> LLDP-MED
Power Management Mode	<input type="radio"/> Actual Consumption	<input checked="" type="radio"/> Reserved Power	

Power Supply Configuration for Switch 2

Primary Power Supply [W]	<input type="text" value="100"/>
--------------------------	----------------------------------

Ethernet Port Configuration for Switch 2

Port	PoE Mode	Priority	Maximum Power [W]
1	PoE+	Low	15.4
2	Disabled	Low	15.4
3	PoE	Low	15.4
4	PoE+	Low	15.4
5	PoE+	Low	15.4
6	PoE+	Low	15.4
7	PoE+	Low	15.4
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	15.4
22	PoE+	Low	15.4
23	PoE+	Low	15.4
24	PoE+	Low	15.4

Save	Reset
------	-------

Configuration	Description
Reserved Power determined by	<p>There are three modes for configuring how the ports/PDs may reserve power.</p> <p>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.</p> <p>Class mode: In this mode each port automatic determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Three different port classes exist and one for 4, 7 and 15.4 Watts. In this mode the Maximum Power fields have no effect.</p> <p>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</p> <p>For all modes: If a port uses more power than the reserved power for the port, the port is shut down.</p>
Power Management Mode	<p>There are 2 modes for configuring when to the ports are shut down.</p> <p>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.</p> <p>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.</p>
Primary Power Supply	For being able to determine the amount of power the PD may use, it must be defined what amount of power the primary power source can deliver.
Local Port	This is the logical port number for this row.
PoE Mode	<p>The PoE Mode represents the PoE operating mode for the port.</p> <p>Disabled: PoE disabled for the port.</p> <p>PoE: Enables PoE IEEE 802.3af (Class 4 PDs limited to 15.4W)</p> <p>PoE+: Enables PoE+ IEEE 802.3at (Class 4 PDs limited to 30W)</p>
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 device 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.

Save

Click to save the changes.

Reset

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

2.10 MAC Table

MAC Address Table Configuration

Stack Aging Configuration

Disable Automatic Aging	<input type="checkbox"/>
Age Time	300 seconds

MAC Table Learning for Switch 2

	Port Members																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Auto	<input checked="" type="radio"/>																							
Disable	<input type="radio"/>																							
Secure	<input type="radio"/>																							

Static MAC Table Configuration for Switch 2

			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

Add new static entry

Save

Reset

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

Aging Configuration	Description
---------------------	-------------

Disable Automatic Aging	Check to disable aging for MAC address entries.
-------------------------	---

Aging Time	Configure aging time by entering a value here in seconds
------------	--

Valid values: *10 to 1000000 seconds*

Port MAC Table Learning

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.*

Click to configure a new static MAC address entry in the [MAC table](#).

Click to save the changes.

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

2.10.1 Static MAC Address Configuration

Static MAC Table Configuration

			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
Delete	1	00-00-00-00-00-00	<input type="checkbox"/>																							

Static MAC Table Configuration

[VLAN ID](#) The [VLAN ID](#) for the static MAC address entry.

MAC Address The MAC address for the entry.

Port Members Check to indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

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

Click to configure a new static MAC address entry in the MAC table.

2.11 VLANs

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.

2.11.1 VLAN Membership

VLAN Membership Configuration

Refresh |<< >>

Start from VLAN with entries per page.

		Port Members																							
Delete	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
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>																							

Add new entry

Save Reset

Configuration	Description
Start from VLAN	Select range of VLAN table entries.
Delete	Check to delete a VLAN entry. The entry will be deleted on the switch unit during the next Save.
VLAN ID	Indicates the ID of this particular VLAN.
Port Members	A row of check boxes for each port is displayed for each VLAN ID. To include a port in a VLAN, check the box. To remove or exclude the port from the VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Add new entry	Click to add a new VLAN entry. An empty row is added to the table, and the VLAN can be configured as needed.
Refresh	Click to refresh the page; any changes made locally will be undone.
<<	Click to display the first page.
>>	Click to display the last page.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Adding a New VLAN entry

		Port Members																							
Delete	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
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>																							
Delete	<input type="text" value="0"/>	<input type="checkbox"/>																							

Configuration	Description
VLAN ID	Enter VLAN ID for the new VLAN entry. Legal values: <i>1 through 4095</i>
Port Members	A row of check boxes for each port is displayed for each VLAN ID. To include a port in a VLAN, check the box. To remove or exclude the port from the VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
<input type="button" value="Delete"/>	Click to delete the new VLAN row.
<input type="button" value="Add new VLAN"/>	Click to add another new VLAN ID.
<input type="button" value="Save"/>	Click to save the new VLAN row.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

2.11.2 VLAN Port Configuration

VLAN Port Configuration for Switch

Port	VLAN Aware	Ingress Filtering	Frame Type	Port VLAN	
				Mode	ID
1	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
2	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
3	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
4	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
5	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
6	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
7	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
8	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
9	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
10	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
11	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
12	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
13	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
14	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
15	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
16	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
17	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
18	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
19	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
20	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
21	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
22	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
23	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1
24	<input type="checkbox"/>	<input type="checkbox"/>	All ▼	Specific ▼	1

Configuration	Description
Port	This is the logical port number for this row.
VLAN Aware	Enable VLAN awareness for a port by checking the box. This parameter affects VLAN ingress processing. If VLAN awareness is enabled: the tag is removed from tagged frames received on the port. Furthermore, VLAN tagged frames are classified to the VLAN ID in the tag. If VLAN awareness is disabled, all frames are classified to the Port VLAN ID and tags are not removed. By default, VLAN awareness is disabled (no checkmark).
Ingress Filtering	Enable ingress filtering for 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 frames. This parameter affects VLAN ingress processing. All: all frames are accepted. (Default) Tagged: Only tagged frames are accepted. Untagged frames received on the port are discarded.
Port VLAN Mode	Configures the Port VLAN Mode. This parameter affects VLAN ingress and egress processing. None: 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. Specific: (the default value) 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: <i>The port must be a member of the same VLAN as the Port VLAN ID.</i>
<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

2.12 Private VLANs

▼ Private VLANs ▪ Port Isolation

A **Private VLAN** is a VLAN which contains switched ports that are restricted, such that they can only communicate with a given "uplink", or called "Promiscuous port". The restricted ports are called "Isolated ports". Each private VLAN typically contains many isolated ports, and a single uplink. The uplink will typically be a switched port (or link aggregation group) connected to a router, firewall, server, provider network, or similar central resource.

Types of Ports in a private VLAN

- Promiscuous:** Usually connects to a router – a type of a port which is allowed to send and receive frames from any other port on the VLAN.
- Isolated:** This type of port is only allowed to communicate with Promiscuous ports. Isolated ports are not allowed to communicate to each other. This type of ports usually connects to hosts.

By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1. A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

Port Isolation Configuration for Switch 2

Port Number																							
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
<input type="checkbox"/>																							

A port member of a [VLAN](#) can be isolated to other isolated ports on [Private VLAN](#).

Configuration	Description
Port Numbers	A check box is provided for each port of a private VLAN. When checked, set the port to be isolation port in a private VLAN. When unchecked, set the port to be promiscuous port in a private VLAN. By default, port isolation is disabled for all ports.
<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

2.13 Voice VLAN

- ▼ Voice VLAN
 - Configuration
 - OUI

2.13.1 Configuration

Voice VLAN Configuration

Stack Global Settings

Mode	Disabled
VLAN ID	1000
Age Time	86400 seconds
Traffic Class	High

Port Configuration for Switch 2

Port	Mode	Security
1	Disabled	Disabled
2	Disabled	Disabled
3	Disabled	Disabled
4	Disabled	Disabled
5	Disabled	Disabled
6	Disabled	Disabled
7	Disabled	Disabled
8	Disabled	Disabled
9	Disabled	Disabled
10	Disabled	Disabled
11	Disabled	Disabled
12	Disabled	Disabled
13	Disabled	Disabled
14	Disabled	Disabled
15	Disabled	Disabled
16	Disabled	Disabled
17	Disabled	Disabled
18	Disabled	Disabled
19	Disabled	Disabled
20	Disabled	Disabled
21	Disabled	Disabled
22	Disabled	Disabled
23	Disabled	Disabled
24	Disabled	Disabled

Save Reset

The Voice VLAN feature enables the voice traffic forwarding on the Voice VLAN, then the switch can

classifying and scheduling to network traffic. It is recommended there are 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 VLAN ID correctly. It should be configured through its own GUI.

Configuration	Description
Mode	Indicates the Voice VLAN mode operation. We must disable MSTP feature before enabling Voice VLAN. It can avoid the conflict of ingress filter. 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 conflict configuration if the value equal management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.
Age Time	Indicates the Voice VLAN secure learning age time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware age time. The actual age time will be situated in the [age_time; 2 * age_time] interval.
Traffic Class	Indicates the Voice VLAN traffic class. All traffic on Voice VLAN will apply this class.
Port Mode	Indicates the Voice VLAN port mode. When the port mode isn't disabled, we must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filter. Possible port modes are: Disabled: Disjoin from Voice VLAN. Auto: Enable auto detect mode. It detects whether there is VoIP phone attached on the specific port and configures the Voice VLAN members automatically. Forced: Forced join to Voice VLAN.
Port Security	Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephone MAC addresses in 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.
<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

2.13.2 OUI

Voice VLAN OUI Table

Delete	Telephony OUI	Description
<input type="checkbox"/>	00-01-e3	Siemens AG phones
<input type="checkbox"/>	00-03-6b	Cisco phones
<input type="checkbox"/>	00-0f-e2	H3C phones
<input type="checkbox"/>	00-60-b9	Philips and NEC AG phones
<input type="checkbox"/>	00-d0-1e	Pingtel phones
<input type="checkbox"/>	00-e0-75	Polycom phones
<input type="checkbox"/>	00-e0-bb	3Com phones

Add new entry

Save

Reset

Configuration

Description

Delete

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

Telephony OUI

An 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. The allowed string length is 0 to 32.

Add new entry

Click to add a new OUI entry

<input type="checkbox"/>	00-e0-bb	3Com phones
Delete	<input type="text"/>	<input type="text"/>

Delete

Click to delete an OUI entry

Save

Click to save the changes.

Reset

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

2.14 QoS

- ▼ QoS
 - Ports
 - DSCP Remarking
 - QoS Control List
 - Rate Limiters
 - Storm Control
 - Wizard

Frames can be classified by 4 different QoS classes: *Low*, *Normal*, *Medium*, and *High*.

The classification is controlled by a [QCL](#) that is assigned to each port. A QCL consists of an ordered list of up to 12 [QCEs](#). Each QCE can be used to classify certain frames to a specific QoS class.

This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 [DSCP](#) or [Tag Priority](#). Frames not matching any of the QCEs are classified to the default QoS class for the port.

2.14.1 Ports

Port QoS Configuration

Number of Classes

Ingress Configuration				Egress Configuration				
Port	Default Class	QCL #	Tag Priority	Queuing Mode	Queue Weighted			
					Low	Normal	Medium	High
1	Low	1	0	Strict Priority	1	2	4	8
2	Low	1	0	Strict Priority	1	2	4	8
3	Normal	1	0	Strict Priority	1	2	4	8
4	High	1	0	Strict Priority	1	2	4	8
5	Low	1	0	Strict Priority	1	2	4	8
6	Low	1	0	Strict Priority	1	2	4	8
7	Low	1	0	Strict Priority	1	2	4	8
8	Low	1	0	Strict Priority	1	2	4	8
9	Low	1	0	Strict Priority	1	2	4	8
10	Low	1	0	Strict Priority	1	2	4	8
11	Low	1	0	Strict Priority	1	2	4	8
12	Low	1	0	Strict Priority	1	2	4	8
13	Low	1	0	Strict Priority	1	2	4	8
14	Low	1	0	Strict Priority	1	2	4	8

Configuration	Description
Number of Classes	Configure the number of traffic classes as "1", "2", or "4". The default value is "4".
Ingress Configuration	
Port	The logical port for the settings contained in the same row.
Default Class	Configure the default QoS class for the port, that is, the QoS class for frames not matching any of the QCEs in the QCL.
QCL #	Select which QCL to use for the port.
Tag Priority	Select the default tag priority for this port when adding a Tag to the untagged frames.
Egress Configuration	
Queuing Mode	Select which Queuing mode for this port. <i>Strict Priority:</i> High class queue is served first always till it is empty <i>Weighted:</i> The queues are served based on the weight ratios set below.
Queue Weighted	Setting Queue weighted (Low:Normal:Medium:High) if the "Queuing Mode" is "Weighted".
- Low	Weight of <i>Low</i> Class
- Normal	Weight of <i>Normal</i> Class
- Medium	Weight of <i>Medium</i> Class
- High	Weight of <i>High</i> Class
<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

2.14.2 DSCP Remarking

The DSCP value of incoming frames will be changed according to its mapping queue once this packet is transmitted by the egress port.

DSCP Remarking Configuration for Switch 2

Port	DSCP Remarking Mode	DSCP Queue Mapping			
		Low	Normal	Medium	High
1	Disabled ▾	CS1 ▾	CS2 ▾	CS3 ▾	CS4 ▾
2	Disabled ▾	Best Effort	CS2 ▾	CS3 ▾	CS4 ▾
3	Disabled ▾	CS1	CS2 ▾	CS3 ▾	CS4 ▾
4	Disabled ▾	CS2	CS2 ▾	CS3 ▾	CS4 ▾
5	Disabled ▾	CS3	CS2 ▾	CS3 ▾	CS4 ▾
6	Disabled ▾	CS4	CS2 ▾	CS3 ▾	CS4 ▾
7	Disabled ▾	CS5	CS2 ▾	CS3 ▾	CS4 ▾
8	Disabled ▾	CS6	CS2 ▾	CS3 ▾	CS4 ▾
9	Disabled ▾	CS7	CS2 ▾	CS3 ▾	CS4 ▾
10	Disabled ▾	Expedite Forward	CS2 ▾	CS3 ▾	CS4 ▾
11	Disabled ▾	CS1 ▾	CS2 ▾	CS3 ▾	CS4 ▾
12	Disabled ▾	CS1 ▾	CS2 ▾	CS3 ▾	CS4 ▾
13	Disabled ▾	CS1 ▾	CS2 ▾	CS3 ▾	CS4 ▾
14	Disabled ▾	CS1 ▾	CS2 ▾	CS3 ▾	CS4 ▾
15	Disabled ▾	CS1 ▾	CS2 ▾	CS3 ▾	CS4 ▾
16	Disabled ▾	CS1 ▾	CS2 ▾	CS3 ▾	CS4 ▾

Save

Reset

Configuration

Description

Port	The logical port for the settings contained in the same row.
DSCP Remarking Mode	If the QoS remarking mode is set to enabled, it should be with this DSCP remarking/correction function according to RFC2474 on this port.
DSCP Queue Mapping	Configure the mapping table between the queue and its DSCP value that is used for DSCP remarking if the DSCP value of incoming packets is not specified in RCF2474. Best Effort = DSCP (0) CS1 = DSCP (8) CS2 = DSCP (16) CS3 = DSCP (24) CS4 = DSCP (32) CS5 = DSCP (40) CS6 = DSCP (48)

CS7 = DSCP (56)

Expedite Forward = DSCP (46)

Save

Click to save the changes.

Reset

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

2.14.4 QoS Control List

QoS Control List Configuration

QCL # 

QCE Type	Type Value	Traffic Class	
			

Configuration	Description
QCL #	Select a QCL to display a table that lists all the QCEs for that particular QCL.
	You can modify each QCE in the table using the following buttons:
	Inserts a new QCE before the current row.
	Edits the QCE.
	Moves the QCE up the list.
	Moves the QCE down the list.
	Deletes the QCE.
	The lowest plus sign adds a new entry at the bottom of the list of QCL.

QCE Configuration

QCE Type	Ethernet Type 
Ethernet Type Value	0x FFFF
Traffic Class	LOW 

Save Reset Cancel

QCE Type	Specifies which frame field the QCE processes to determine the QoS class of the frame. The following QCE types are supported: <u>Ethernet Type</u> : The Ethernet Type field. If frame is tagged, this is the Ethernet Type
----------	--

that follows the tag header.

VLAN ID: VLAN ID. Only applicable if the frame is VLAN tagged.

TCP/UDP Port: IPv4 TCP/UDP source/destination port.

DSCP: IPv4 and IPv6 DSCP.

ToS: The 3 precedence bit in the ToS byte of the IPv4/IPv6 header (also known as DS field).

Tag Priority: [User Priority](#). Only applicable if the frame is VLAN tagged or priority tagged.

Type Value

Indicates the value according to its QCE type.

Traffic Class

The QoS class associated with the QCE.

Save

Click to save the changes.

Reset

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

Cancel

Click to return to previous page.

2.14.5 Rate Limiters

Rate Limit Configuration

Port	Policer Enabled	Policer Rate	Policer Unit	Shaper Enabled	Shaper Rate	Shaper Unit
1	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
2	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
3	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
7	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
8	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
9	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
10	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
11	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
12	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
13	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps

Configuration	Description
Port	The logical port for the settings contained in the same row.
Policer Enabled	Enable or disable the port policer. The default value is "Disabled".
Policer Rate	Configure the rate for the port policer. The default value is "500". This value is restricted to 500-1000000 when the "Policer Unit" is "kbps", and it is restricted to 1-1000 when the "Policer Unit" is "Mbps"
Policer Unit	Configure the unit of measure for the port policer rate as kbps or Mbps. The default value is "kbps".
Shaper Enabled	Enable or disable the port shaper. The default value is "Disabled".
Shaper Rate	Configure the rate for the port shaper. The default value is "500". This value is restricted to 500-1000000 when the "Policer Unit" is "kbps", and it is restricted to 1-1000 when the "Policer Unit" is "Mbps".
Shaper Unit	Configure the unit of measure for the port shaper rate as kbps or Mbps . The default value is "kbps".
<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

2.14.6 Storm Control

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 rate is 2^n , where n is equal to or less than 15, or "No Limit". The unit of the rate can be either pps (packets per second) or kpps (kilo-packets per second). The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch.

Note: Frames, which are sent to the CPU of the switch are always limited to approximately 4 kpps. For example, broadcasts in the management VLAN are limited to this rate. The management VLAN is configured on the IP setup page.

Storm Control Configuration

Frame Type	Status	Rate (pps)
Unicast	<input type="checkbox"/>	1
Multicast	<input type="checkbox"/>	1
Broadcast	<input type="checkbox"/>	1

Configuration	Description
Frame Type	The settings in a particular row apply to the frame type listed here: unicast, multicast, or broadcast.
Status	Enable or disable the storm control status for the given frame type.
Rate	The rate unit is packet per second (pps), configure the rate as 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K , or 1024K . The 1 kpps is actually 1024 pps.

<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

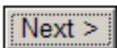
2.14.7 Wizard

Welcome to the QCL Configuration Wizard!

Please select an action:

- Set up Port Policies**
Group ports into several types according to different QCL policies.
- Set up Typical Network Application Rules**
Set up the specific QCL for different typical network application quality control.
- Set up ToS Precedence Mapping**
Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets.
- Set up VLAN Tag Priority Mapping**
Set up the traffic class mapping to the user priority value (3 bits) when receiving VLAN tagged packets.

To continue, click Next.



This handy wizard helps you set up a [QCL](#) quickly.

2.14.7.1 Wizard – Port Policies

QCL ID	Port Members																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	<input checked="" type="radio"/>																							
2	<input type="radio"/>																							
3	<input type="radio"/>																							
4	<input type="radio"/>																							
5	<input type="radio"/>																							
6	<input type="radio"/>																							
7	<input type="radio"/>																							
8	<input type="radio"/>																							
9	<input type="radio"/>																							
10	<input type="radio"/>																							
11	<input type="radio"/>																							
12	<input type="radio"/>																							
13	<input type="radio"/>																							
14	<input type="radio"/>																							

Configuration	Description
QCL ID	Frames that hit this QCE are set to match this specific QCL.
Port Members	A row of radio buttons for each port is displayed for each QCL ID. To include a port in a QCL member, click the radio button.

<input type="button" value="Cancel Wizard"/>	Click to cancel the wizard.
<input type="button" value=" < Back"/>	Click to go back to the previous wizard step.
<input type="button" value=" Next >"/>	Click to continue the wizard.

Finished !

The QCL configuration wizard is finished, and the new configuration is ready for use.

Click Finish to get more information.
Click Wizard Again to start the wizard again.

2.14.7.2 Wizard – Typical Network Application Rules

Set up Typical Network Application Rules

Set up the specific QCL for different typical network application quality control by selecting the network application type for your rule:

o Audio and Video

QuickTime 4 Server MSN Messenger Phone Yahoo Messenger Phone Napster Real Audio

o Games

Blizzard Battlenet (Diablo2 and StarCraft) Fighter Ace II Quake2 Quake3 MSN Game Zone

o User Definition

Ethernet Type VLAN ID TCP/UDP Port DSCP

Configuration	Description
Audio and Video	Indicates the common servers that apply to the specific QCE . The common servers are: <i>QuickTime 4 Server, MSN Messenger Phone, Yahoo Messenger Phone, Napster, Real Audio.</i>
Games	Indicates the common games that apply to the specific QCE.
User Definition	Indicates the user definition that applies to the specific QCE. The user definitions are: <u>Ethernet Type</u> : Specify the Ethernet Type filter for this QCE. The allowed range is <i>0x600 to 0xFFFF</i> . <u>VLAN ID</u> : VLAN ID filter for this QCE. The allowed range is <i>1 to 4095</i> . <u>UDP/TCP Port</u> : Specify the TCP/UDP port filter for this QCE. The allowed range is <i>0 to 65535</i> . <u>DSCP</u> : Specify the DSCP filter for this QCE. The allowed range is <i>0 to 63</i> .
<input type="button" value="Cancel Wizard"/>	Click to cancel the wizard.
<input type="button" value=" < Back"/>	Click to go back to the previous wizard step.
<input type="button" value=" Next >"/>	Click to continue the wizard.

2.14.7.3 Wizard – ToS Precedence Mapping

Set up ToS Precedence Mapping

Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets.

QCL ID	1 ▾
ToS Precedence 0 Class	Low ▾
ToS Precedence 1 Class	Low ▾
ToS Precedence 2 Class	Low ▾
ToS Precedence 3 Class	Low ▾
ToS Precedence 4 Class	Low ▾
ToS Precedence 5 Class	Low ▾
ToS Precedence 6 Class	Low ▾
ToS Precedence 7 Class	Low ▾

Cancel Wizard

< Back

Next >

This wizard is used to set up the traffic class mapping to the precedence part of [ToS](#) (3 bits) when receiving IPv4/IPv6 packets.

Configuration	Description
QCL ID	Select the QCL ID to which this QCE applies.
ToS Precedence Class	Select a traffic class of Low, Normal, Medium, or High to apply to the QCE.
Cancel Wizard	Click to cancel the wizard.
< Back	Click to go back to the previous wizard step.
Next >	Click to continue the wizard.

2.14.7.4 Wizard – VLAN Tag Priority Mapping

Set up VLAN Tag Priority Mapping

Set up the traffic class mapping to the user priority value (3 bits) when receiving VLAN tagged packets.

QCL ID	1
Tag Priority 0 Class	Normal
Tag Priority 1 Class	Low
Tag Priority 2 Class	Low
Tag Priority 3 Class	Normal
Tag Priority 4 Class	Medium
Tag Priority 5 Class	Medium
Tag Priority 6 Class	High
Tag Priority 7 Class	High

Cancel Wizard

< Back

Next >

Configuration	Description
QCL ID	Select the QCL ID to which this QCE applies.
VLAN Priority Class	Select a traffic class of Low, Normal, Medium, or High to apply to the QCE.
Cancel Wizard	Click to cancel the wizard.
< Back	Click to go back to the previous wizard step.
Next >	Click to continue the wizard.

2.15 Mirroring

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

Stack Global Settings

Port to mirror to	Disabled
Switch to mirror to	Switch 2

Mirror Port Configuration for Switch 2

Port	Mode
1	Disabled
2	Disabled
3	Enabled
4	Rx only
	Tx only
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
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

Save	Reset
------	-------

Configuration	Description
Port to mirror to	Port to mirror is also known as the mirror port . Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored to this port. Disabled disables mirroring.
Port	The logical port for the settings contained in the same row.
Mode	Select one of the following mirror modes. Rx only: Frames received at this port are mirrored to the mirror port . Frames transmitted are not mirrored. Tx only: Frames transmitted from this port are mirrored to 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 to the mirror port .
<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

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

2.16 UPnP

UPnP Configuration

Mode	Disabled ▾
TTL	4
Advertising Duration	100

Save	Reset
------	-------

Configuration	Description
Mode	Indicates the UPnP operation mode. Possible modes are: Enabled: Enable UPnP mode operation. Disabled: Disable UPnP mode operation. When the mode is enabled, two ACEs are added automatically to trap UPnP related packets to CPU. The ACEs are automatically removed when the mode is disabled.
TTL	The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 255.
Advertising Duration	The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive a 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
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.17 Stack

Stack Configuration

Delete	Stack Member	Switch ID	Master		Switch Type
			Capable	Priority	
<input type="checkbox"/>	00-40-f6-e4-11-02	2 ▼	Yes	2 ▼	KGS-2423
<input type="checkbox"/>	00-40-f6-e4-13-02	3 ▼	Yes	2 ▼	KGS-2423
<input type="checkbox"/>	00-40-f6-e4-14-02	4 ▼	Yes	2 ▼	KGS-2423
<input type="checkbox"/>	00-40-f6-e4-12-02	5 ▼	Yes	2 ▼	KGS-2423
<input type="checkbox"/>	00-40-f6-e4-10-02	1	-	-	

Start Master Election

Configuration	Description
Delete	Check to delete this switch from the stack configuration.
Stack Member	The MAC address of the switch
Switch ID	The Switch ID (1-16) assigned to a switch
Master Capable	Indicates whether a switch is capable of being master.
Master Priority	The priority that the switch has in the master election process. The smaller the priority, the more likely the switch will become master during the master election process.
Switch Type	The product name of the switch
Start Master Election	By checking this option, the "Save" operation will also start the master election process.

<input type="button" value="Save"/>	Click to save the changes.
<input type="button" value="Reset"/>	Click to reset to default values.

2.17.1 Assigning Switch ID

Assigning and Swapping Switch IDs

When a switch is added to the stack, a Switch ID is automatically assigned to the switch. The automatic SID assignment can be modified by choosing a different Switch ID on the Stack Configuration page. This method allows Switch IDs to be assigned so that it is easier for the user to remember the ID of each switch.

The Switch IDs of two switches can be swapped by simply interchanging the values in the Switch ID column. Changing Switch IDs does not result in any interruption of the stack operation.

Removing a Switch from the Stack

When a switch is removed from the stack, the configuration for the switch is preserved, and the switch still appears on the Stack Configuration page. If the configuration of the switch is not to be transferred to another switch, then the configuration may be deleted by choosing Delete, followed by "Save".

Replacing a Switch

If a switch is to be replaced with another switch (for example, replacing failing hardware), the following procedure must be used to assign the configuration of the failing switch to the new hardware:

1. Remove the failing switch from the stack. For example, assume that the failing switch had Switch ID 3.
2. Insert the new switch into the stack. The new switch is assigned an unused Switch ID.
3. To remove the automatic switch ID assignment, choose "Delete", followed by "Save". The new switch is then shown with Switch ID set to "-".
4. To assign the configuration of Switch ID 3 to the new hardware, simply choose 3 in the Switch ID column and click "Save". The new hardware has now taken over the configuration of the failing hardware.

General Switch ID Assignment Rules

When assigning Switch IDs to the devices in the stack, you must note the following:

- ✓ Switches with assigned IDs can be changed to use any other switch ID (possibly by swapping Switch ID with another active switch).
- ✓ When swapping two Switch IDs, the devices will retain their (own) configuration.
- ✓ Switches without an assigned Switch ID can only be assigned to any *unused* ID.
- ✓ When assigning a Switch ID of an inactive switch to a new switch, the new switch will inherit the former's configuration (see "Replacing a Switch" above).
- ✓ Deleting a switch will remove any configuration pertaining to it.
- ✓ Deleting an *active* switch will leave it with an unassigned Switch ID until rebooted or manually assigning a Switch ID.

2.17.2 Master Switch Election in a Stack

Within a managed stack, *one* master switch (or just "master") must be elected. Any switch not being master is a slave switch (or just "slave").

To elect a master, the following criteria are evaluated sequentially:

1. If any switch already claims to have been master for more than 30 seconds, then that switch will become master.
2. If multiple switches claim to have been master for more than 30 seconds, then the switch which has been master for the longest period of time will become master.
3. The switch with the smallest master priority.
4. The switch with the smallest MAC address.

The above algorithm ensures that once a master has been elected and has been master for more than 30 seconds, it will remain master. However in some cases the user may want to enforce a new master election. This is done by clicking "**Start Master Election**", followed by "**Save**". This causes the first two criteria to be ignored, thereby basing master election only on master priority and MAC address. When master election is enforced, the first two criteria are ignored for a period of 10-15 seconds. On the Stack State Monitor web page, this is shown by "Reelect" being set to "Yes" for one of the switches in the stack.

3. Monitor

- ▼ **Monitor**
 - ▶ System
 - ▶ **Ports**
 - ▶ Security
 - ▶ LACP
 - ▶ Spanning Tree
 - IGMP Snooping
 - MVR
 - ▶ LLDP
 - PoE
 - MAC Table
 - ▶ VLANs
 - Stack

3.1 System

- ▼ **System**
 - Information
 - CPU Load
 - Log
 - Detailed Log

3.1.1 Information

System Information

Auto-refresh [Refresh](#)

System	
Contact	
Name	
Location	
Hardware	
MAC Address	00-40-f6-e4-11-02
Time	
System Date	1970-01-01 16:38:17 +0000
System Uptime	0d 16:38:17

Switch ID	Software Version
2	v1.0116
3	v1.0116
4	v1.0116
5	v1.0116

This page gives an example of one stack composed of four switches.

Status Information **Description**

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.
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.
Switch ID	The switch ID.
Software Version	The software version of the switch
Software Date	The date when the switch software was produced.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.

3.1.2 CPU Load

This page displays the CPU load, using a 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 plug-in installed to support SVG.



3.1.3 Log

System Log Information for Switch 2

Auto-refresh

Refresh

Clear

|<<

<<

>>

>>|

Level

The total number of entries is 10 for the given level.

Start from ID with entries per page.

ID	Level	Time	Message
1	Info	-	Switch just made a cool boot.
2	Info	1970-01-01 00:00:03 +0000	Link up on switch 2, port 25
3	Info	1970-01-01 00:00:05 +0000	Link up on switch 3, port 26
4	Info	1970-01-01 00:00:06 +0000	Link up on switch 3, port 25
5	Info	1970-01-01 00:00:07 +0000	Link up on switch 5, port 26
6	Info	1970-01-01 00:00:08 +0000	Link up on switch 5, port 22
7	Info	1970-01-01 00:00:10 +0000	Link up on switch 5, port 9
8	Info	1970-01-01 00:00:11 +0000	Link up on switch 4, port 11
9	Info	1970-01-01 00:00:11 +0000	Link up on switch 4, port 25
10	Info	1970-01-01 00:00:11 +0000	Link up on switch 4, port 26

Configuration

Description

ID	The ID (≥ 1) of the system log entry.
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.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to Updates the system log entries, starting from the current entry ID.
<input type="button" value="Clear"/>	Flushes all system log entries.
<input type="button" value=" <<"/>	Updates the system log entries, starting from the first available entry ID.
<input type="button" value="<<"/>	Updates the system log entries, ending from the last entry currently displayed.
<input type="button" value=">>"/>	Updates the system log entries, starting from the last entry currently displayed.
<input type="button" value=">> "/>	Updates the system log entries, ending at the last entry currently displayed.

3.1.4 Detailed Log

Detailed System Log Information for Switch 2

ID	<input type="text" value="1"/>
----	--------------------------------

Message

Level	Info
Time	-
Message	Switch just made a cool boot.

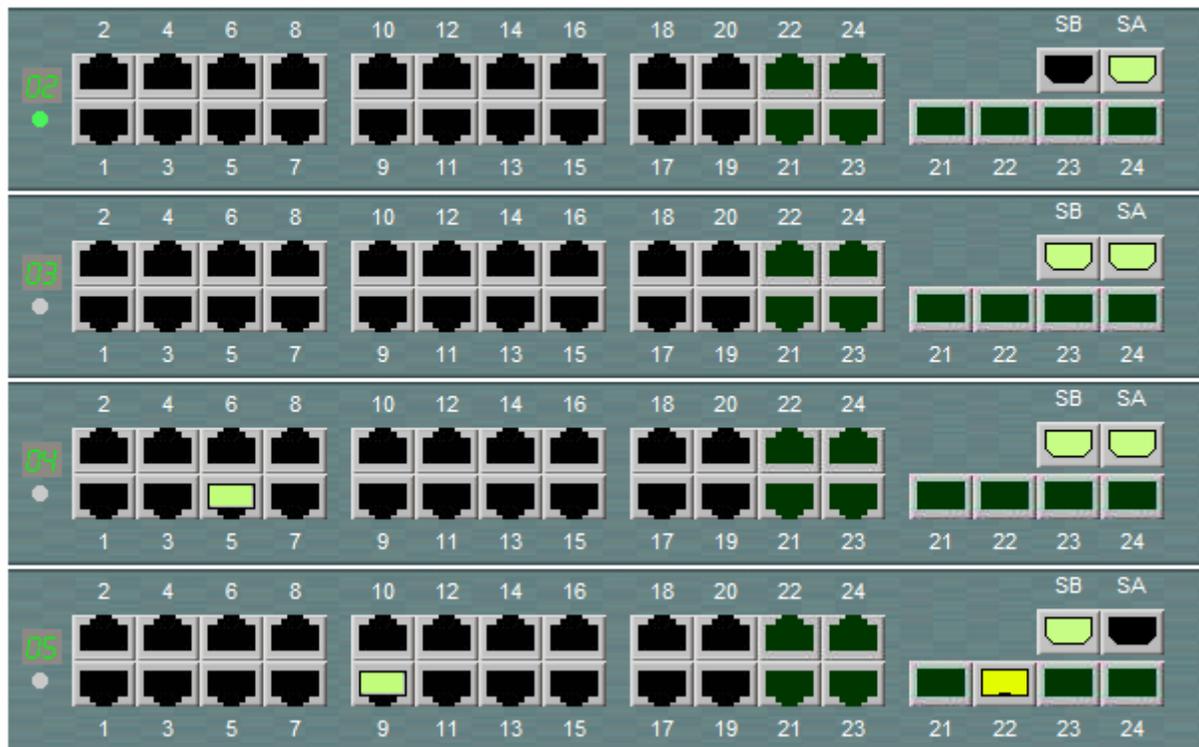
Configuration	Description
ID	The ID (≥ 1) of the system log entry.
Message	The message of the system log entry.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to Updates the system log entries, starting from the current entry ID.
<input type="button" value="Clear"/>	Flushes all system log entries.
<input type="button" value=" <<"/>	Updates the system log entries, starting from the first available entry ID.
<input type="button" value="<<"/>	Updates the system log entries, ending from the last entry currently displayed.
<input type="button" value=">>"/>	Updates the system log entries, starting from the last entry currently displayed.
<input type="button" value=">> "/>	Updates the system log entries, ending at the last entry currently displayed.

3.2 Ports



3.2.1 State

Port State Overview



An image of the stack is displayed. The switch ID is displayed on the left side of each switch. All link-up ports are displayed in green color.

Status	Description
Port Icon	Click the port icon to display its detailed statistics. Example of Port 22 of Switch ID 5:

Detailed Port Statistics for Switch 5 Port 22

Port 22 Auto-refresh Refresh

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	23000
Rx Octets	0	Tx Octets	3346778
Rx Unicast	0	Tx Unicast	43
Rx Multicast	0	Tx Multicast	3455
Rx Broadcast	0	Tx Broadcast	19502
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	0	Tx 64 Bytes	6176
Rx 65-127 Bytes	0	Tx 65-127 Bytes	10401
Rx 128-255 Bytes	0	Tx 128-255 Bytes	3571
Rx 256-511 Bytes	0	Tx 256-511 Bytes	2851
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	1
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Low	0	Tx Low	22995
Rx Normal	0	Tx Normal	0
Rx Medium	0	Tx Medium	0
Rx High	0	Tx High	5
Receive Error Counters		Transmit Error Counters	
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		
Power Over Ethernet Status			
PD class	0	Power Used	0 [W]
Power Requested	0 [W]	Current Used	0 [mA]
Power Allocated	0 [W]	Priority	Low

Auto-refresh

Check this box to enable an automatic refresh of the page at regular intervals.

Click to refresh the page; any changes made locally will be undone.

Click to clear all statistic counters.

3.2.2 Traffic Overview

Port Statistics Overview for Switch 5

Auto-refresh

Port	Packets		Bytes		Errors		Drops		Filtered
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	2653	46433	169792	6798553	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0
22	0	46429	0	6797740	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0
25	53761	5253	8065523	836880	0	0	0	0	1666
26	0	0	0	0	0	0	0	0	0

Configuration	Description
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
Receive/Transmit	The number of received and transmitted packets per port.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.
<input type="button" value="Clear"/>	Click to flush all counters.

3.2.3 QoS Statistics

Queuing Counters for Switch 5

Auto-refresh

Port	Low Queue		Normal Queue		Medium Queue		High Queue	
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	48267	0	0	0	0	2760	5
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
18	0	0	0	0	0	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	0	0	0	0	0
22	0	48252	0	0	0	0	0	5
23	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0
25	49997	39	0	0	0	0	5899	5428
26	0	0	0	0	0	0	0	0

An example of Switch ID 5 is displayed.

Configuration	Description
Port	The logical port for the settings contained in the same row.
Low Queue	There are 4 QoS queues per port with strict or weighted queuing scheduling. This is the lowest priority queue.
Normal Queue	This is the normal priority queue of the 4 QoS queues.
Medium Queue	This is the medium priority queue of the 4 QoS queues.
High Queue	This is the highest priority queue of the 4 QoS queues.
Receive/Transmit	The number of received and transmitted packets per port.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.
<input type="button" value="Clear"/>	Click to flush all counters.

3.2.4 Detailed Statistics

Detailed Port Statistics for Switch 5 Port 22

Port 22 Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	23000
Rx Octets	0	Tx Octets	3346778
Rx Unicast	0	Tx Unicast	43
Rx Multicast	0	Tx Multicast	3455
Rx Broadcast	0	Tx Broadcast	19502
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	0	Tx 64 Bytes	6176
Rx 65-127 Bytes	0	Tx 65-127 Bytes	10401
Rx 128-255 Bytes	0	Tx 128-255 Bytes	3571
Rx 256-511 Bytes	0	Tx 256-511 Bytes	2851
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	1
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Low	0	Tx Low	22995
Rx Normal	0	Tx Normal	0
Rx Medium	0	Tx Medium	0
Rx High	0	Tx High	5
Receive Error Counters		Transmit Error Counters	
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		
Power Over Ethernet Status			
PD class	0	Power Used	0 [W]
Power Requested	0 [W]	Current Used	0 [mA]
Power Allocated	0 [W]	Priority	Low

Configuration Description

Receive Total and Transmit Total

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

Receive and Transmit Size Counters

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

Receive and Transmit Queue Counters

Number of packets received and transmitted by the input and output queues.

Receive Error Counters

Rx Drops	Number of frames dropped due to lack of receive buffers or egress congestion.
Rx CRC/Alignment	Number of frames received with CRC or alignment errors.
Rx Undersize	Number of short ¹ frames received with valid CRC.
Rx Oversize	Number of long ² frames received with valid CRC.

Rx Fragments	Number of short ¹ frames received with invalid CRC.
Rx Jabber	Number of long ² frames received with invalid CRC.
Rx Filtered	Number of received frames filtered by the forwarding process.

Transmit Error Counters

Tx Drops	Number of frames dropped due to output buffer congestion.
Tx Late/Exc. Coll.	Number of frames dropped due to excessive or late collisions.

Power Over Ethernet Status

Power Used	The Power Used shows how much power the PD currently is using.
Power Requested	The Power Requested shows the requested amount of power the PD wants to reserve.
Current Used	The Power Used shows how much current the PD currently is using.
Power Allocated	The Power Allocated shows the amount of power the switch has allocated for the PD.
Priority	The Priority shows the port's priority configured by the user.

Port #	Select the logical port for the displayed statistics
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.
<input type="button" value="Clear"/>	Click to flush all counters.

Note:

¹ *Short frames are frames that are smaller than 64 bytes.*

² *Long frames are frames that are longer than the configured maximum frame length for this port.*

3.3 Security

- Security
 - Access Management Statistics
 - Network
 - AAA

3.3.1 Access Management Statistics

Access Management Statistics Auto-refresh Refresh Clear

Interface	Receive Packets	Allow Packets	Discard Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

Statistics	Description
Interface	The interface that allowed remote host can access the switch.
Receive Packets	The received packets number from the interface under access management mode is enabled.
Allow Packets	The allowed packets number from the interface under access management mode is enabled.
Discard Packets	The discarded packets number from the interface under access management mode is enabled.
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.
Clear	Click to flush all counters.

3.3.2 Network

- Network
 - Port Security
 - NAS
 - ACL Status
 - DHCP
 - ARP Inspection
 - IP Source Guard

3.3.2.1 Port Security

- Port Security
 - Switch
 - Port

3.3.2.1.1 Switch

Port Security Switch Status

Auto-refresh

Refresh

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
DHCP Snooping	D
Voice VLAN	V

Port Status for Switch 2

Port	Users	State	MAC Count	
			Current	Limit
1	----	Disabled	-	-
2	----	Disabled	-	-
3	----	Disabled	-	-
4	----	Disabled	-	-
5	----	Disabled	-	-
6	----	Disabled	-	-
7	----	Disabled	-	-
8	----	Disabled	-	-
9	----	Disabled	-	-
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	-	-

User Module Legend Description

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 Description

Port	The port number for which the status applies. Click the port number to see the status for this particular port.
Users	Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.
State	Shows the current state of the port. It can take one of four values: 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 (-). Indicates the number of currently learned MAC addresses (forwarding as well as blocked) on the port. If no user modules are enabled on the port, a dash (-) will be shown.

Auto-refresh Check this box to enable an automatic refresh of the page at regular intervals.
 Click to refresh the page; any changes made locally will be undone.

3.3.2.1.2 Port

Port Security Port Status for Switch 4 Port 5 Port 5 Auto-refresh

MAC Address	VLAN ID	State	Time of Adding	Age/Hold
No MAC addresses attached				

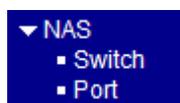
Port Status	Description
--------------------	--------------------

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 Adding	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.

Port #	Select the logical port for the displayed statistics
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.

Note: Port security configuration is set via "Configuration" -> "Security" -> "Network" -> "Limit Control" operation. Refer to section 2.3.2.1.

3.3.2.2 NAS



3.3.2.2.1 Switch

Network Access Server Switch Status for Switch 4

Auto-refresh Refresh

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled				
2	Force Authorized	Globally Disabled				
3	Force Authorized	Globally Disabled				
4	Force Authorized	Globally Disabled				
5	Force Authorized	Globally Disabled				
6	Force Authorized	Globally Disabled				
7	Force Authorized	Globally Disabled				
8	Force Authorized	Globally Disabled				
9	Force Authorized	Globally Disabled				
10	Force Authorized	Globally Disabled				
11	Force Authorized	Globally Disabled				
12	Force Authorized	Globally Disabled				
13	Force Authorized	Globally Disabled				
14	Force Authorized	Globally Disabled				
15	Force Authorized	Globally Disabled				
16	Force Authorized	Globally Disabled				
17	Force Authorized	Globally Disabled				
18	Force Authorized	Globally Disabled				
19	Force Authorized	Globally Disabled				
20	Force Authorized	Globally Disabled				
21	Force Authorized	Globally Disabled				
22	Force Authorized	Globally Disabled				
23	Force Authorized	Globally Disabled				
24	Force Authorized	Globally Disabled				

Status	Description
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.
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. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.

3.3.2.2.2 Port

NAS Statistics for Switch 2 Port 2

Port 2 ▾

Auto-refresh

Refresh

Clear

Port State

Admin State	Port-based 802.1X
Port State	Unauthorized
QoS Class	
Port VLAN ID	

Port Counters

Receive EAPOL Counters		Transmit EAPOL Counters	
Total	0	Total	4
Response ID	0	Request ID	4
Responses	0	Requests	0
Start	0		
Logoff	0		
Invalid Type	0		
Invalid Length	0		
Receive Backend Server Counters		Transmit Backend Server Counters	
Access Challenges	0	Responses	0
Other Requests	4		
Auth. Successes	0		
Auth. Failures	0		
Last Supplicant Info			
MAC Address			
VLAN ID			
Version			0
Identity			

EAPOL frame counters are available for the following administrative states:

- ✓ Force Authorized
- ✓ Force Unauthorized
- ✓ Port-based 802.1X
- ✓ Single 802.1X
- ✓ Multi 802.1X

The backend (RADIUS) frame counters are available for the following administrative states:

- ✓ Port-based 802.1X
- ✓ Single 802.1X
- ✓ Multi 802.1X
- ✓ MAC-based Auth.

The information about the last supplicant/client that attempted to authenticate is available for the following administrative states:

- ✓ Port-based 802.1X
- ✓ Single 802.1X
- ✓ Multi 802.1X
- ✓ MAC-based Auth.

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

- ✓ Multi 802.1X
- ✓ MAC-based Auth.

Status	Description
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.

EAPOL Port Counter	Description
Rx Total	The number of valid EAPOL frames of any type that have been received by the switch.
Rx Response ID	The number of valid EAPOL Response Identity frames that have been received by the switch.
Rx Responses	The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.
Rx Start	The number of EAPOL Start frames that have been received by the switch.
Rx Logoff	The number of valid EAPOL Logoff frames that have been received by the switch.
Rx Invalid Type	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
Rx Invalid Length	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
Tx Total	The number of EAPOL frames of any type that have been transmitted by the switch.

Tx Request ID	The number of EAPOL Request Identity frames that have been transmitted by the switch.
Tx Requests	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.

Backend Server Counter	Description
-------------------------------	--------------------

Rx Access Challenges	<p>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. Indicate that the backend server has communication with the switch.</p> <p>MAC-based: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).</p>
Rx Other Requests	<p>802.1X-based: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicate that the backend server chose an EAP-method.</p> <p>MAC-based: Not applicable.</p>
Rx Auth. Successes	<p>802.1X- and MAC-based: Counts the number of times that the switch receives a success indication. Indicate that the supplicant/client has successfully authenticated to the backend server.</p>
Rx Auth. Failures	<p>802.1X- and MAC-based: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.</p>
Tx Responses	<p>802.1X-based: Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted.</p> <p>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.</p>

Last Supplicant/Client Info	Description
------------------------------------	--------------------

MAC Address	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	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

Description

Selected Counters

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

- Multi 802.1X
- MAC-based Auth.

Attached MAC Addresses **Description**

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).

Port #

Select the logical port for the displayed statistics

Auto-refresh

Check this box to enable an automatic refresh of the page at regular intervals.

Click to refresh the page; any changes made locally will be undone.

Clear

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.

Clear All

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.

Clear This

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.

3.3.2.3 ACL Status

ACL Status for Switch 2

User	Ingress Port	Frame Type	Action	Rate Limiter	Port Copy	CPU	CPU Once	Counter	Conflict
No entries									

Combined Auto-refresh Refresh

- Combined
- Static
- IP Source Guard
- ARP Inspection
- UPnP
- DHCP
- Conflict

Status	Description
User	Indicates the ACL user.
Ingress Port	Indicates the ingress port of the ACE. Possible values are: Any: The ACE will match any ingress port. Policy: The ACE will match ingress ports with a specific policy. 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.

Action	<p>IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.</p> <p>Indicates the forwarding action of the ACE.</p> <p>Permit: Frames matching the ACE may be forwarded and learned.</p> <p>Deny: Frames matching the ACE are dropped.</p>
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 15. When “Disabled” is displayed, the rate limiter operation is disabled.
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.
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.
[Combined]	Select the ACL status from the drop down list.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.

3.3.2.4 DHCP

- ▼ DHCP
 - Snooping Statistics
 - Relay Statistics

3.3.2.4.1 Snooping Statistics

DHCP Snooping Port Statistics for Switch 2 Port 1

Port 1 Auto-refresh

Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0

Counters	Description
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.

Port #	Select the logical port for the displayed statistics
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.
<input type="button" value="Clear"/>	Click to flush all counters.

3.3.2.4.2 Relay Statistics

DHCP Relay Statistics

Auto-refresh

Server Statistics

Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0

Client Statistics

Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option
0	0	0	0	0	0	0

Server Counters	Description
Transmit to Server	The packets number that relayed from client to server.
Transmit Error	The packets number that errors sending packets to clients.
Receive from Server	The packets number that received packets from server.
Receive Missing Agent Option	The packets number that received packets without agent information options.
Receive Missing Circuit ID	The packets number that received packets which the Circuit ID option was missing.

Receive Missing Remote ID The packets number that received packets which Remote ID option was missing.
 Receive Bad Circuit ID The packets number that the Circuit ID option did not match known circuit ID.
 Receive Bad Remote ID The packets number that the Remote ID option did not match known Remote ID.

Client Counters	Description
Transmit to Client	The packets number that relayed packets from server to client.
Transmit Error	The packets number that error sending packets to servers.
Receive from Client	The packets number that received packets from server.
Receive Agent Option	The packets number that received packets with relay agent information option.
Replace Agent Option	The packets number that replaced received packets with relay agent information option.
Keep Agent Option	The packets number that kept received packets with relay agent information option.
Drop Agent Option	The packets number that dropped received packets with relay agent information option.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.
<input type="button" value="Clear"/>	Click to flush all counters.

3.3.2.5 ARP Inspection

Dynamic ARP Inspection Table for Switch 2 Auto-refresh

Start from , VLAN , MAC address and IP address with entries per page.

Port	VLAN ID	MAC Address	IP Address
No more entries			

Navigating the ARP Inspection Table

Each page shows up to 999 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 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.

Button	Description
--------	-------------

Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.
<input type="button" value="Clear"/>	Click to flush all counters.
<input type="button" value=" <<"/>	Click to update the table starting from the first entry.
<input type="button" value=">>"/>	Click to update the table starting with the entry after the last entry currently displayed

3.3.2.6 IP Source Guard

Dynamic IP Source Guard Table for Switch 2 Auto-refresh

Start from , VLAN and IP address and IP Mask with entries per page.

Port	VLAN ID	IP Address	IP Mask
No more entries			

Navigating the IP Source Guard Table

Each page shows up to 999 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", "IP address" and "IP mask" 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 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.

Button	Description
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.
<input type="button" value="Clear"/>	Click to flush all counters.
<input type="button" value=" <<"/>	Click to update the table starting from the first entry.
<input type="button" value=">>"/>	Click to update the table starting with the entry after the last entry currently displayed

3.3.3 AAA

- ▼ AAA
 - RADIUS Overview
 - RADIUS Details

3.3.3.1 RADIUS Overview

RADIUS Authentication Server Status Overview

Auto-refresh Refresh

#	IP Address	Status
1	0.0.0.0:1812	Disabled
2	0.0.0.0:1812	Disabled
3	0.0.0.0:1812	Disabled
4	0.0.0.0:1812	Disabled
5	0.0.0.0:1812	Disabled

RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0:1813	Disabled
2	0.0.0.0:1813	Disabled
3	0.0.0.0:1813	Disabled
4	0.0.0.0:1813	Disabled
5	0.0.0.0:1813	Disabled

Status	Description
--------	-------------

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.
Status	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.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.

3.3.3.2 RADIUS Details

RADIUS Authentication Statistics for Server #1 (0.0.0.0:1812) Auto-refresh

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
State		Disabled	
Round-Trip Time		0 ms	

RADIUS Accounting Statistics for Server #1 (0.0.0.0:1813)

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
State		Disabled	
Round-Trip Time		0 ms	

Authentication Server Description

Server #	Select a RADIUS server number.
Rx Access Accepts	RFC4670 name: radiusAuthClientExtAccessAccepts The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx Access Rejects	RFC4670 name: radiusAuthClientExtAccessRejects The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx Access Challenges	RFC4670 name: radiusAuthClientExtAccessChallenges The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx Malformed Access Responses	RFC4670 name: radiusAuthClientExtMalformedAccessResponses The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
Rx Bad Authenticators	RFC4670 name: radiusAuthClientExtBadAuthenticators The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx Unknown Types	RFC4670 name: radiusAuthClientExtUnknownTypes The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Rx Packets Dropped	RFC4670 name: radiusAuthClientExtPacketsDropped The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Tx Access Requests	RFC4670 name: radiusAuthClientExtAccessRequests The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Tx Access Retransmissions	RFC4670 name: radiusAuthClientExtAccessRetransmissions The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Tx Pending Requests	RFC4670 name: radiusAuthClientExtPendingRequests The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
Tx Timeouts	RFC4670 name: radiusAuthClientExtTimeouts

The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

State

Shows the state of the server. It takes one of the following values:

Disabled: The selected server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Round-Trip Time

RFC4670 name: radiusAuthClientExtRoundTripTime

The time interval (measured in milliseconds) is between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

Accounting Server	Description
Rx Responses	RFC4670 name: radiusAccClientExtResponses The number of RADIUS packets (valid or invalid) received from the server.
Rx Malformed Responses	RFC4670 name: 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	RFC4670 name: radiusAcctClientExtBadAuthenticators The number of RADIUS packets containing invalid authenticators received from the server.
Rx Unknown Types	RFC4670 name: radiusAccClientExtUnknownTypes The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx Packets Dropped	RFC4670 name: radiusAccClientExtPacketsDropped The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.

Tx Requests	RFC4670 name: radiusAccClientExtRequests The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx Retransmissions	RFC4670 name: radiusAccClientExtRetransmissions The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx Pending Requests	RFC4670 name: radiusAccClientExtPendingRequests The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.
Tx Timeouts	RFC4670 name: radiusAccClientExtTimeouts The number of accounting timeouts to the server After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
State	Shows the state of the server. It takes one of the following values: Disabled: The selected server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAccClientExtRoundTripTime The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.
<input type="button" value="Clear"/>	Click to clear all counters.

3.4 LACP

- ▼ LACP
 - System Status
 - Port Status
 - Port Statistics

3.4.1 System Status

LACP System Status

Auto-refresh

Aggr ID	Partner System ID	Partner Key	Last Changed	Local Ports
<i>No ports enabled or no existing partners</i>				

Configuration	Description
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	Show which ports are a part of this aggregation for this switch/stack. The format is: " Switch ID :Port".
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.

3.4.2 Port Status

LACP Status for Switch 2 Auto-refresh Refresh

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port
1	No	-	-	-	-
2	No	-	-	-	-
3	No	-	-	-	-
4	No	-	-	-	-
5	No	-	-	-	-
6	No	-	-	-	-
7	No	-	-	-	-
8	No	-	-	-	-
9	No	-	-	-	-
10	No	-	-	-	-
11	No	-	-	-	-
12	No	-	-	-	-
13	No	-	-	-	-
14	No	-	-	-	-
15	No	-	-	-	-
16	No	-	-	-	-
17	No	-	-	-	-
18	No	-	-	-	-
19	No	-	-	-	-
20	No	-	-	-	-
21	No	-	-	-	-
22	No	-	-	-	-
23	No	-	-	-	-
24	No	-	-	-	-

Status	Description
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. IDs 1 and 2 are GLAGs while IDs 3-14 are LLAGs.
Partner System ID	The partners System ID (MAC address).
Partner Port	The partners port number connected to this port.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.

3.4.3 Port Statistics

LACP Statistics for Switch 2 Auto-refresh

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
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

Configuration	Description
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.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.
<input type="button" value="Clear"/>	Click to clear all counters.

3.5 Spanning Tree

- ▼ Spanning Tree
 - Bridge Status
 - Port Status
 - Port Statistics

3.5.1 Bridge Status

STP Bridges

Auto-refresh

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	80:00-00:40:F6:E9:10:CF	80:00-00:40:F6:E9:10:CF	-	0	Steady	-

Configuration	Description
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 <i>root</i> port role.
Root Cost	Root Path Cost. For the Root Bridge this 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 for this Bridge instance.
Topology Change Last	The time since last Topology Change occurred.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.

STP Detailed Bridge Status

Auto-refresh

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	80:00-00:40:F6:E4:11:02
Root ID	80:00-00:40:F6:E4:11:02
Root Cost	0
Root Port	-
Regional Root	80:00-00:40:F6:E4:11:02
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	0
Topology Change Last	-

CIST Ports & Aggregations State

Switch ID	Port	Port ID	Role	State	Path Cost	Edge	Point2Point	Uptime
No ports or aggregations active								

Status

Description

Bridge Instance	The Bridge instance - CIST, MST1, ...
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 <i>root</i> port role.
Root Cost	Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
Regional Root	The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. <i>(For the CIST instance only)</i>
Internal Root Cost	The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. <i>(For the CIST instance only)</i>
Topology Flag	The current state of the Topology Change Flag for this Bridge instance.
Topology Change Count	The number of times where the topology-change flag has been set (during a one-second interval).
Topology Last	The time passed since the Topology Flag was last set.

Physical Ports & Aggregations State

Switch ID	The Switch ID of the logical port.
Port	The switch port number of the logical STP port.
Port ID	The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port.
Role	The current STP port role. The port role can be one of the following values:

AlternatePort, BackupPort, RootPort, DesignatedPort.

State	The current STP port state. The port state can be one of the following values: <i>Blocking, Learning, Forwarding.</i>
Path Cost	The current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value.
Edge	The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.
Point2Point	The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transition STP state.
Uptime	The time since the bridge port was last initialized.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="checkbox"/> Refresh	Click to refresh the page; any changes made locally will be undone.

3.5.2 Port Status

STP Port Status for Switch 2

Auto-refresh

Port	CIST Role	CIST State	Uptime
2:1	Non-STP	Forwarding	-
2:2	Non-STP	Forwarding	-
2:3	Non-STP	Forwarding	-
2:4	Non-STP	Forwarding	-
2:5	Non-STP	Forwarding	-
2:6	Non-STP	Forwarding	-
2:7	Non-STP	Forwarding	-
2:8	Non-STP	Forwarding	-
2:9	Non-STP	Forwarding	-
2:10	Non-STP	Forwarding	-
2:11	Non-STP	Forwarding	-
2:12	Non-STP	Forwarding	-
2:13	Non-STP	Forwarding	-
2:14	Non-STP	Forwarding	-
2:15	Non-STP	Forwarding	-
2:16	Non-STP	Forwarding	-
2:17	Non-STP	Forwarding	-
2:18	Non-STP	Forwarding	-
2:19	Non-STP	Forwarding	-
2:20	Non-STP	Forwarding	-
2:21	Non-STP	Forwarding	-
2:22	Non-STP	Forwarding	-
2:23	Non-STP	Forwarding	-
2:24	Non-STP	Forwarding	-

Status	Description
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: <i>AlternatePort</i> , <i>BackupPort</i> , <i>RootPort</i> , <i>DesignatedPort</i> .
CIST State	The current STP port state of the CIST port. The port state can be one of the following values: <i>Blocking</i> , <i>Learning</i> , <i>Forwarding</i> .
Uptime	The time since the bridge port was last initialized.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.

3.5.3 Port Statistics

STP Statistics

Auto-refresh

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
2	75789	0	0	0	0	0	0	0	0	0

Counter	Description
Port	The switch port number of the logical RSTP 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.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.
<input type="button" value="Clear"/>	Click to clear all counters.

3.6 IGMP Snooping

IGMP Snooping Status

Auto-refresh

Refresh

Clear

Statistics

VLAN ID	Querier Status	Querier Transmit	Querier Receive	V1 Reports Receive	V2 Reports Receive	V3 Reports Receive	V2 Leave Receive
---------	----------------	------------------	-----------------	--------------------	--------------------	--------------------	------------------

IGMP Groups

VLAN ID	Groups	Port Members																							
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
No IGMP groups																									

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-

Status Description

Statistics

VLAN ID	The VLAN ID of the entry.
Querier Status	Show the Querier status is "ACTIVE" or "IDLE".
Querier Transmit	The number of Transmitted Querier.
Querier Receive	The number of Received Querier.
V1 Reports Receive	The number of Received V1 Reports.
V2 Reports Receive	The number of Received V2 Reports.
V3 Reports Receive	The number of Received V3 Reports.
V2 Leave Receive	The number of Received V2 Leave.

IGMP Groups

Groups	The present IGMP groups, Max. are 128 groups for each VLAN.
Port Members	The ports that are members of the entry.

Router Ports

Port	The port number
Status	The port is a router port or not.

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.

Clear

Click to clear all counters.

3.7 MVR

MVR Status for Switch 2

Auto-refresh

Refresh

Clear

Statistics

VLAN ID	V1 Reports Receive	V2 Reports Receive	V3 Reports Receive	V2 Leave Receive
---------	--------------------	--------------------	--------------------	------------------

Multicast Groups

		Port Members																									
VLAN ID	Groups	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
<i>No multicast groups</i>																											

Status

Description

Groups	The present multicast groups Max. are 128 groups in the multicast VLAN.
Port Members	The ports that are members of the entry.
V1 Reports Receive	The number of Received V1 Reports.
V2 Reports Receive	The number of Received V2 Reports.
V3 Reports Receive	The number of Received V3 Reports.
V2 Leave Receive	The number of Received V2 Leave.

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.

Clear

Click to clear all counters.

3.8 LLDP

- ▼ LLDP
 - Neighbors
 - LLDP-MED Neighbors
 - PoE
 - Port Statistics

3.8.1 Neighbors

LLDP Neighbor Information

Auto-refresh Refresh

Local Port	Chassis ID	Remote Port ID	System Name	Port Description	System Capabilities	Management Address
Port 3	00-40-F6-E9-22-CF	7		Port #7	Bridge(+)	192.168.0.174 (IPv4)
Port 24	00-01-C1-00-00-00	24		Port #24	Bridge(+)	192.168.0.177 (IPv4)

Status	Description										
Local Port	The port on which the LLDP frame was received.										
Chassis ID	The Chassis ID is the identification of the neighbor's LLDP frames.										
Remote Port ID	The Remote Port ID is the identification of the neighbor port.										
System Name	System Name is the name advertised by the neighbor unit.										
Port Description	Port Description is the port description advertised by the neighbor unit.										
System Capabilities	System Capabilities describes the neighbor unit's capabilities. The possible capabilities are: <table border="0"><tr><td>1. Other</td><td>2. Repeater</td></tr><tr><td>3. Bridge</td><td>4. WLAN Access Point</td></tr><tr><td>5. Router</td><td>6. Telephone</td></tr><tr><td>7. DOCSIS cable device</td><td>8. Station only</td></tr><tr><td>9. Reserved</td><td></td></tr></table> When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).	1. Other	2. Repeater	3. Bridge	4. WLAN Access Point	5. Router	6. Telephone	7. DOCSIS cable device	8. Station only	9. Reserved	
1. Other	2. Repeater										
3. Bridge	4. WLAN Access Point										
5. Router	6. Telephone										
7. DOCSIS cable device	8. Station only										
9. Reserved											
Management Address	Management Address is the neighbor unit's address that is used for higher layer entities to assist the discovery by the network management. This could for instance hold the neighbor's IP address.										
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.										
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.										

3.8.2 LLDP-MED Neighbors

LLDP-MED Neighbor Information

Auto-refresh Refresh

No LLDP-MED neighbor information found

Status	Description
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
5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

LLDP-MED Endpoint Device Definition < LLDP-MED the using service communication IP in participate and edge, network LAN 802 IEEE at located are TIA-1057, defined as Devices, Endpoint>

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. Fore-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 neighbor 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 vis 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 Signaling - for use in network topologies that require a different policy for the voice signaling 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 Signaling - for use in network topologies that require a different policy for the guest voice signaling 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 Signaling - for use in network topologies that require a separate policy for the video signaling than for the video media.

Policy

Policy

Unknown: The network policy for the specified application type is currently unknown.

Defined: The network policy is defined.

TAG

TAG is indicating 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 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).

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.

3.8.3 PoE

LLDP Neighbor Power Over Ethernet Information for Switch 2

Auto-refresh

Local Port	Power Type	Power Source	Power Priority	Maximum Power
------------	------------	--------------	----------------	---------------

Status	Description
Local Port	The port for this switch on which the LLDP frame was received.
Type	The Type represents whether the device is a Power Sourcing Entity (PSE) or Power Device (PD). If the Type is unknown it is represented as " <i>Reversed</i> ".
Source	The Source represents the power source being utilized by a PSE or PD device. If the device is a PSE device it can either run on its Primary Power Source or its Backup Power Source. If it is unknown whether the PSE device is using its Primary Power Source or its Backup Power Source it is indicated as " <i>Unknown</i> ". If the device is a PD device it can either run on its local power supply or it can use the PSE as power source. It can also use both its local power supply and the PSE. If it is unknown what power supply the PD device is using it is indicated as " <i>Unknown</i> ".
Priority	Power Priority represents the priority of the PD device, or the power priority associated with the PSE type device's port that is sourcing the power. There are three levels of power priority. The three levels are: Critical, High and Low. If the power priority is unknown it is indicated as " <i>Unknown</i> ".
Power	The Power Value contains a numerical value that indicates the maximum power in watts required by a PD device from a PSE device, or the minimum power a PSE device is capable of sourcing over a maximum length cable based on its current configuration. The maximum allowed value is 102.3 W. If the device indicates value higher than 102.3 W, it is represented as "reserved"
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.

3.8.4 Port Statistics

Global Counters	
Neighbor entries were last changed at - (10903 sec. ago)	
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

Auto-refresh Refresh Clear

LLDP Statistics for Switch 2

Local Counters									
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs	
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0

Global Status	Description
---------------	-------------

Neighbor entries were last changed at

Shows the time of the last entry was last deleted or added. It is also shows the time elapsed since last change was detected.

Total Neighbors Entries Added

Shows the number of new entries added since switch reboot.

Total Neighbors Entries Deleted

Shows the number of new entries deleted since switch reboot.

Total Neighbors Entries Dropped

Shows the number of [LLDP](#) frames dropped due to that the entry table was full.

Total Neighbors Entries Aged Out

Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

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 Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port links 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 TLVs received.
Age-Outs	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.
<input type="button" value="Clear"/>	Click to clear all counters.

3.9 PoE

Power Over Ethernet Status for Switch 2

Auto-refresh Refresh

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	4	30 [W]	30 [W]	27.9 [W]	508 [mA]	Low	PoE turned ON
2	1	4 [W]	4 [W]	2.3 [W]	43 [mA]	Low	PoE turned ON
3	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
4	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
5	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
6	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
7	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
8	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
9	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
10	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
11	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
12	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
13	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
14	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
15	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
16	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
17	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
18	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
19	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
20	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
21	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
22	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
23	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
24	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		34 [W]	34 [W]	30.2 [W]	551 [mA]		

MAC Table Column Description

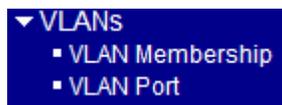
Local Port	This is the logical port number for this row.
Power Requested	The Power Requested shows the requested amount of power the PD wants to reserve.
Power Allocated	The Power Allocated shows the amount of power the switch has allocated for the PD.
Power Used	The Power Used shows how much power the PD currently is using.
Current Used	The Power Used shows how much current the PD currently is using.
Priority	The Priority shows the port's priority configured by the user.
Port Status	The Port Status shows the port's status.

Auto-refresh Check this box to enable an automatic refresh of the page at regular intervals.

Click to updates the information.

The page example shows Port 1 and Port 2 have compliant PD connected.

3.11 VLAN



3.11.1 VLAN Membership

A VLAN User is a module that uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID, UVID. Currently we support following VLAN:

- CLI/Web/SNMP: This are referred 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 in 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.

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 is selected, it shall show this information for all the VLAN Users, and this is the default. VLAN membership allows the frames Classified to the VLAN ID to be forwarded to the respective VLAN member ports.

VLAN Membership Status for User Static

VLAN ID	Port Members																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Static Auto-refresh Refresh

Static
 NAS
 MVR
 Voice VLAN
 MSTP
 Combined

Select a type of VLAN Users

Status

Description

VLAN ID

Indicates the ID of this particular VLAN.

Port Members

A row of check marks is displayed for each VLAN ID. The port with check mark is the member of the associated VLAN ID.

Auto-refresh

Check this box to enable an automatic refresh of the page at regular intervals.

Click to updates the information, starting from the current entry ID.

3.11.2 VLAN Port

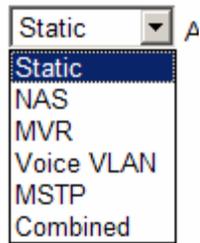
VLAN Port Status for User Static

 Auto-refresh

Port	PVID	VLAN Aware	Ingress Filtering	Frame Type	Tx Tag	UVID	Conflicts
1	1	Disabled	Disabled	All	Untag_this	1	No
2	1	Disabled	Disabled	All	Untag_this	1	No
3	1	Disabled	Disabled	All	Untag_this	1	No
4	1	Disabled	Disabled	All	Untag_this	1	No
5	1	Disabled	Disabled	All	Untag_this	1	No
6	1	Disabled	Disabled	All	Untag_this	1	No
7	1	Disabled	Disabled	All	Untag_this	1	No
8	1	Disabled	Disabled	All	Untag_this	1	No
9	1	Disabled	Disabled	All	Untag_this	1	No
10	1	Disabled	Disabled	All	Untag_this	1	No
11	1	Disabled	Disabled	All	Untag_this	1	No
12	1	Disabled	Disabled	All	Untag_this	1	No
13	1	Disabled	Disabled	All	Untag_this	1	No
14	1	Disabled	Disabled	All	Untag_this	1	No
15	1	Disabled	Disabled	All	Untag_this	1	No
16	1	Disabled	Disabled	All	Untag_this	1	No
17	1	Disabled	Disabled	All	Untag_this	1	No
18	1	Disabled	Disabled	All	Untag_this	1	No
19	1	Disabled	Disabled	All	Untag_this	1	No
20	1	Disabled	Disabled	All	Untag_this	1	No
21	1	Disabled	Disabled	All	Untag_this	1	No
22	1	Disabled	Disabled	All	Untag_this	1	No
23	1	Disabled	Disabled	All	Untag_this	1	No
24	1	Disabled	Disabled	All	Untag_this	1	No

Static ▼

Select a type of VLAN Users



Status	Description
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.
VLAN Aware	Shows the VLAN Awareness for the port. If VLAN awareness is enabled, the tag is removed from tagged frames received on the port. VLAN tagged frames are classified to the VLAN ID in the tag. If VLAN awareness is disabled, all frames are classified to the Port VLAN ID and tags are not removed.
Ingress Filtering	Show the ingress filtering for 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 of the frame, 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 behavior 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: <ol style="list-style-type: none">1. Functional Conflicts between feature.2. Conflicts due to hardware limitation.3. Direct conflict between user modules.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Refresh"/>	Click to updates the information.

3.12 Stack

Stack Topology

Auto-refresh Refresh

Stack Topology	Stand-alone
Stack Member Count	1
Last Topology Change	-
Master Switch	00-40-f6-e4-11-02
Last Master Change	-

Stack List

Stack Member	Switch ID	Product		Master		
		Name	Version	Priority	Time	Reelect
00-40-f6-e4-11-02	2	KGS-2423	v1.0118	2	0d 02:22:18	No
00-40-f6-e4-10-02	1	-	-	-	-	-
00-40-f6-e4-13-02	3	-	-	-	-	-
00-40-f6-e4-14-02	4	-	-	-	-	-
00-40-f6-e4-12-02	5	-	-	-	-	-

Master Forwarding Table

Stack Member	Switch ID	Distance		Forwarding	
		Port 25	Port 26	Port 25	Port 26
00-40-f6-e4-11-02	2	0	0	Local	Local
00-40-f6-e4-10-02	1	0	0	-	-
00-40-f6-e4-13-02	3	0	0	-	-
00-40-f6-e4-14-02	4	0	0	-	-
00-40-f6-e4-12-02	5	0	0	-	-

Status	Description
Stack Topology	Specifies the type of topology for the stack: Chain: A chain of switches, that is, no redundant forwarding paths. Ring: A ring of switches, thereby providing redundant forwarding paths. Back-to-Back: Two switches interconnected on both stacking ports.
Stack Member Count	The number of switches in the stack.
Last Topology Change	The time of the last topology change in the stack.
Master Switch	The MAC address of the current stack master switch.
Last Master Change	The time of the last master change in the stack.
Stack List	For each switch in the stack, the following information is shown: The MAC address, Switch ID , product name and version, and master election state. The master election state is normally "No". Only when a forced master election is enforced by the user, the master election state takes the value "Yes". For details about the master election

algorithm, see Stack Configuration Help.

Master Forwarding Table As the heading suggests, the information in the table is as seen from the master view. For each switch in the stack, the following information is shown: The MAC address, switch ID, distance information, and the primary forwarding path to the switch. For ring topology, a backup path is also provided.

Auto-refresh Check this box to enable an automatic refresh of the page at regular intervals.

Click to updates the information.

4. Diagnostics

- ▼ **Diagnostics**
 - SFP DDM
 - Ping
 - Ping6

4.1 SFP DDM

SFP DDM for Switch 2

Information	SFP Ports			
	21	22	23	24
Identifier	SFP transceiver	SFP transceiver	SFP transceiver	Not Applicable
Connector	LC	LC	LC	Not Applicable
SONET Compliance	Not Applicable	Not Applicable	Not Applicable	Not Applicable
GbE Compliance	1000BASE-LX	1000BASE-LX	1000BASE-SX	Not Applicable
Vendor Name	APAC Opto	KTI Networks	APAC Opto	Not Applicable
Vendor OUI	000F99	0040F6	000F99	Not Applicable
Temperature	34 (C)	37 (C)	Not Applicable	Not Applicable
Voltage	3.34 (V)	3.31 (V)	Not Applicable	Not Applicable
TX Power	-5.69 (dBm)	-5.84 (dBm)	Not Applicable	Not Applicable

Status	Description
SFP Ports	Port numbers which are equipped with SFP slot (i.e. Port 21, 22, 23 and 24).
Identifier	Identification information of the transceiver
Connector	The connector type used on the transceiver
SONET Compliance	The SONET compliance information of the transceiver
GbE Compliance	Gigabit Ethernet compliance information of the transceiver
Vendor Name	The vendor name of the transceiver
Vendor OUI	The vendor OUI of the transceiver
Temperature	The current temperature sensed currently inside the transceiver
Voltage	The working voltage sensed currently inside the transceiver
TX Power	The transmission optical power sensed currently TX power data is displayed in unit of “dBm”.

Click to updates the information.

4.2 Ping

ICMP Ping

IP Address
Ping Size

Settings	Description
IP Address	The destination IP Address
Ping Size	Payload size of the ICMP packet. Values range: 8 ~ 1400 bytes.

Click to start ping test. Five 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.

Result displayed for a failed ping test

ICMP Ping Output

```
PING server 192.168.0.215
rcvfrom: Operation timed out
Sent 5 packets, received 0 OK, 0 bad
```

Result displayed for a successful ping test

ICMP Ping Output

```
PING server 192.168.0.99
64 bytes from 192.168.0.99: icmp_seq=0, time=20ms
64 bytes from 192.168.0.99: icmp_seq=1, time=30ms
64 bytes from 192.168.0.99: icmp_seq=2, time=0ms
64 bytes from 192.168.0.99: icmp_seq=3, time=0ms
64 bytes from 192.168.0.99: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

Click to start a new ping test.

4.3 Ping6

ICMPv6 Ping

IP Address

Ping Size

Settings	Description
IP Address	The destination IPv6 Address
Ping Size	Payload size of the ICMP packet. Values range: 8 ~ 1400 bytes.
<input type="button" value="Start"/>	Click to start ping test. Five 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.

Result displayed for a failed ping test

ICMPv6 Ping Output

```
PING6 server fdec:ba98:7654:3210:adbf:bbff:2922:fff2
rcvfrom: Operation timed out
Sent 5 packets, received 0 OK, 0 bad
```

Result displayed for a successful ping test

ICMPv6 Ping Output

```
PING6 server fdec:ba98:7654:3210:adbf:bbff:2922:fff
72 bytes from fdec:ba98:7654:3210:adbf:bbff:2922:fff: icmp_seq=0, time=10ms
72 bytes from fdec:ba98:7654:3210:adbf:bbff:2922:fff: icmp_seq=1, time=10ms
72 bytes from fdec:ba98:7654:3210:adbf:bbff:2922:fff: icmp_seq=2, time=0ms
72 bytes from fdec:ba98:7654:3210:adbf:bbff:2922:fff: icmp_seq=3, time=20ms
72 bytes from fdec:ba98:7654:3210:adbf:bbff:2922:fff: icmp_seq=4, time=10ms
Sent 5 packets, received 5 OK, 0 bad
```

Click to start a new ping test.

5. Maintenance

- ▼ **Maintenance**
 - Reset Device
 - Factory Defaults
 - Software Upload
 - ▶ Configuration

5.1 Reset Device

Restart Device

Are you sure you want to perform a Restart?

You can reset the stack switch on this page. After reset, the system will boot normally as if you had powered-on the devices.

<input type="button" value="Yes"/>	<p>Click to reboot device. the message is displayed as follows.</p> <p>System restart in progress</p> <div style="border: 1px solid black; background-color: red; color: white; text-align: center; padding: 5px;">The system is now restarting.</div> <p></p> <p><i>Waiting, please stand by...</i></p>
<input type="button" value="No"/>	<p>Click to return to the Port State page without rebooting.</p>

5.2 Factory Defaults

Factory Defaults

Are you sure you want to reset the configuration to
Factory Defaults?

Yes No

Yes

Click to reboot device. "System rebooting" message is displayed as follows.

Configuration Factory Reset Done

The configuration has been reset. The new configuration is available immediately.

No

Click to return to the Port State page without rebooting.

5.3 Software Upload

This page facilitates an update of the firmware controlling the switch.

Firmware Update

Browse Upload

Browse

Click to the location of a software image

Upload

Click to start uploading.

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 reboots.

Warning: While the firmware is being updated, Web access appears to be defunct. **Do not reset or power off the device at this time** or the switch may fail to function afterwards.

5.4 Configuration

You can save/view or load the switch configuration. The configuration file is in XML format with a hierarchy of tags: Header tags: `<?xml version="1.0"?>` and `<configuration>`. These tags are mandatory and must be present at the beginning of the file.

Configuration Save

Save configuration

Save configuration

Click to start download of the configuration.

Configuration Upload

Browse

Upload

Browse

Click to the location of a configuration file

Upload

Click to start uploading configuration.

Glossary

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

A

ACE

[ACE](#) is an acronym for [A](#)ccess [C](#)ontrol [E](#)ntry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types ([Ethernet Type](#), [ARP](#), and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL

[ACL](#) is an acronym for [A](#)ccess [C](#)ontrol [L](#)ist. It is the list table of [ACE](#)s, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

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

There are 3 web-pages associated with the manual ACL configuration:

ACL|Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" web-page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.

ACL|Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - page. You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the frame gets

past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the Web page help text for each specific port property.

ACL|Rate Limiters: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES

[AES](#) is an acronym for Advanced Encryption Standard. The encryption key protocol is applied in 802.11 standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

APS

[APS](#) is an acronym for Automatic Protection Switching. This protocol is used to secure that switching is done bidirectional in the two ends of a protection group, as defined in G.8031.

Aggregation

Use multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

(Also *Port [Aggregation](#), Link Aggregation*).

ARP

[ARP](#) is an acronym for Address Resolution Protocol. It is a protocol that used to convert an [IP](#) address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known.

Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

[ARP Inspection](#) is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through DUT.

Auto-Negotiation

[Auto-negotiation](#) is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C

CC

[CC](#) is an acronym for Continuity Check. It is a [MEP](#) functionality that is able to detect loss of continuity in a network by transmitting [CCM](#) frames to a peer MEP.

CCM

[CCM](#) is an acronym for Continuity Check Message. It is a [OAM](#) frame transmitted from a

MEP to its peer MEP and used to implement [CC](#) functionality.

CDP

[CDP](#) is an acronym for [C](#)isco [D](#)iscovery [P](#)rotocol.

D

DDM

[DDM](#) is an acronym for [D](#)igital [D](#)iagnostics [M](#)onitoring. Modern optical SFP transceivers support digital diagnostics monitoring (DDM) functions according to the industry-standard SFF-8472. This feature gives the end user the ability to monitor real-time parameters of the SFP, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage.

DEI

[DEI](#) is an acronym for [D](#)rop [E](#)ligible [I](#)ndicator. It is a 1-bit field in the VLAN tag.

DES

[DES](#) is an acronym for [D](#)ata [E](#)ncryption [S](#)tandard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP

[DHCP](#) is an acronym for [D](#)ynamic [H](#)ost [C](#)onfiguration [P](#)rotocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of [DNS](#) servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

[DHCP Relay](#) is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agent's MAC address.

DHCP Snooping

[DHCP Snooping](#) is used to block intruder on the untrusted ports of DUT when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS

[DNS](#) is an acronym for Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS

[DoS](#) is an acronym for Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

Dotted Decimal Notation

[Dotted Decimal Notation](#) refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.

An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

DSCP

[DSCP](#) is an acronym for Differentiated Services Code Point. It is a field in the header of [IP](#)

packets for packet classification purposes.

E

EEE

[EEE](#) is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS

[EPS](#) Is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type

[Ethernet Type](#), or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

F

FTP

[FTP](#) is an acronym for [File Transfer Protocol](#). It is a transfer protocol that uses the Transmission Control Protocol ([TCP](#)) and provides file writing and reading. It also provides directory service and security features.

Fast Leave

IGMP 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.

H

HTTP

[HTTP](#) is an acronym for [Hypertext Transfer Protocol](#). It is a protocol that used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol ([TCP](#)) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

[HTTPS](#) is an acronym for Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure [HTTP](#) connection.

HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, [TCP/IP](#).) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

[ICMP](#) is an acronym for Internet Control Message Protocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the [PING](#) command uses ICMP to test an Internet connection.

ICMPv6

Internet Control Message Protocol version 6 (ICMPv6) is the implementation of the [ICMP](#) for Internet Protocol version 6 (IPv6) defined in RFC 4443.

IEEE 802.1X

[IEEE 802.1X](#) is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

[IGMP](#) is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IMAP

[IMAP](#) is an acronym for Internet Message Access Protocol. It is a protocol for email clients to retrieve email messages from a mail server.

IMAP is the protocol that IMAP clients use to communicate with the servers, and [SMTP](#) is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 ([POP3](#)), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP

[IP](#) is an acronym for Internet Protocol. It is a protocol used for communicating data across a internet network.

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

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

IPv6

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol ([IP](#)). It is designed to succeed the Internet Protocol version 4 (IPv4). The Internet operates by transferring data between hosts in small packets that are independently routed across networks as specified by an international communications protocol known as the Internet Protocol. IPv6 addresses have two logical parts: a 64-bit network prefix, and a 64-bit host address part. (The host address is often automatically generated from the interface MAC address.) An IPv6 address is represented by 8 groups of 16-bit hexadecimal values separated by colons (:) shown as follows: 2001:0db8:85a3:0000:0000:8a2e:0370:7334. The hexadecimal digits are case-insensitive.

IPMC

[IPMC](#) is an acronym for IP MultiCast.

IP Source Guard

[IP Source Guard](#) is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source

Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

L

LACP

LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol, allows bundling several physical ports together to form a single logical port.

LLDP

LLDP is an IEEE 802.1ab standard protocol. The Link Layer Discovery Protocol, is used for network discovery, and works by having the units in the network exchanging information with their neighbors using LLDP frames.

LLDP-MED

[LLDP-MED](#) is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LOC

[LOC](#) is an acronym for Loss Of Connectivity and is detected by a [MEP](#) and is indicating lost connectivity in the network. Can be used as a switch criteria by [EPS](#)

M

MAC Table

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

MEP

[MEP](#) is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5

[MD5](#) is an acronym for Message-Digest algorithm 5. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be

configured to mirror frames from multiple ports to a mirror port. (In this context, [mirroring](#) a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.

N

NAS

NAS is an acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is [IEEE 802.1X](#).

NetBIOS

[NetBIOS](#) is an acronym for Network Basic Input/Output System. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS

[NFS](#) is an acronym for Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP

[NTP](#) is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses [UDP](#) (datagrams) as transport layer.

O

OAM

[OAM](#) is an acronym for Operation Administration and Maintenance.

It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality.

[MEP](#) functionality like [CC](#) and [RDI](#) is based on this

Optional TLVs.

A LLDP frame contains multiple [TLVs](#)

For some [TLVs](#) it is configurable if the switch shall include the [TLV](#) in the LLDP frame.

These [TLVs](#) are known as optional [TLVs](#). If an optional [TLV](#) is disabled the corresponding information is not included in the LLDP frame.

OUI

[OUI](#) is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

P

PCP

[PCP](#) is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as [User Priority](#).

PD

[PD](#) is an acronym for Powered Device. In a [PoE](#) system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY

[PHY](#) is an abbreviation for Physical Interface Transceiver and is the device that implement the Ethernet physical layer (IEEE-802.3).

PING

[ping](#) is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.
ping uses Internet Control Message Protocol ([ICMP](#)) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

PoE

[PoE](#) is an acronym for Power Over Ethernet.

Power Over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

Policer

A [policer](#) can limit the bandwidth of received frames. It is located in front of the ingress queue.

POP3

[POP3](#) is an acronym for Post Office Protocol version 3. It is a protocol for email clients to retrieve email messages from a mail server.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some

period of time. POP can be thought of as a "store-and-forward" service.

An alternative protocol is Internet Message Access Protocol ([IMAP](#)). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol ([SMTP](#)). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

PPPoE

[PPPoE](#) is an acronym for Point-to-Point Protocol over Ethernet.

It is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks (Wikipedia).

Private VLAN

In a [private VLAN](#), communication between ports in that private [VLAN](#) is not permitted. A VLAN can be configured as a private VLAN.

PTP

[PTP](#) is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.

Q

QCE

[QCE](#) is an acronym for QoS Control Entry. It describes [QoS](#) class associated with a particular QCE ID.

There are six QCE frame types: [Ethernet Type](#), [VLAN](#), [UDP/TCP](#) Port, [DSCP](#), [TOS](#), and [Tag Priority](#). Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL

[QCL](#) is an acronym for QoS Control List. It is the list table of [QCEs](#), containing [QoS](#) control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

[QL](#) In [SyncE](#) this is the Quality Level of a given clock source. This is received on a port in a [SSM](#) indicating the quality of the clock received in the port.

QoS

[QoS](#) is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship

between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

There are 4 web-pages associated with the QoS configuration:

QoS|QoS Control List: The web page shows the QCEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one QCE even though there are more matching QCEs. The first matching QCE will give that frame a priority: Low, Normal, Medium or High. 5 different QCLs can be created, each with 8 different QCEs. You assign each port a QCL id under QoS|Ports page. The QoS counters can be viewed under Monitor|Ports|QoS statistics. There are number of parameters that can be configured with a QCE. Read the Web page help text to get further information for each of them.

QoS|Ports: The Ports QoS page is used to assign a QCL id to an ingress port. Furthermore you can assign a default class to a port and a queuing mode. Strict queuing means that the higher priority frame will always be served before a lower priority frame. Weighted priority will give each class some weight of the bandwidth.

QoS|Rate Limiters: Under this page you can configure the policer (ingress) and shaper (egress) rate for each port. See the help page for details.

QoS|Storm Control: Here you can limit the flooding in the switch, i.e. the rate you choose applies to the whole switch. Choose the mix of Unicast, Multicast and Broadcast storm control. See the help page for details.

R

RARP

[RARP](#) is an acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of [arp](#).

RADIUS

[RADIUS](#) is an acronym for Remote Authentication Dial In User Service. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RDI

[RDI](#) is an acronym for Remote Defect Indication. It is a [OAM](#) functionality that is used by a [MEP](#) to indicate defect detected to the remote peer MEP

Router Port

A router port is a port on the Ethernet switch that leads switch towards the Layer 3 multicast device.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of [STP](#): the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

SAMBA

[Samba](#) is a program running under UNIX-like operating systems that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows, IBM OS/2, and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking.

Samba can be installed on a variety of operating system platforms, including Linux, most common Unix platforms, OpenVMS, and IBM OS/2.

Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows "Neighborhood Network".

SHA

[SHA](#) is an acronym for Secure Hash Algorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper

A [shaper](#) can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP

[SMTP](#) is an acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol ([TCP](#)) and provides a mail service modeled on the [FTP](#) file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNMP

[SNMP](#) is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

[SNTP](#) is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses [UDP](#) (datagrams) as transport layer.

SPROUT

Stack Protocol using ROUting Technology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. [SPROUT](#) also calculates parameters for setting up each switch to perform shortest path forwarding within the stack.

SSID

Service Set Identifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (wikipedia).

SSH

[SSH](#) is an acronym for Secure SHell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, [TELNET](#) and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM

[SSM](#) In [SyncE](#) this is an abbreviation for Synchronization Status Message and is containing a [QL](#) indication.

STP

Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by [RSTP](#).

Switch ID

[Switch IDs](#) (1-16) are used to uniquely identify the switches within a stack. The Switch ID of each switch is shown on the display on the front of the switch and is used widely in the web pages as well as in the CLI commands.

SyncE

[SyncE](#) Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

T

TACACS+

[TACACS+](#) is an acronym for Terminal Access Controller Access Control System Plus. It is a networking protocol which provides access control for routers, network access servers and

other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority

[Tag Priority](#) is a 3-bit field storing the priority level for the 802.1Q frame.

TCP

[TCP](#) is an acronym for [T](#)ransmission [C](#)ontrol [P](#)rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol ([FTP](#)).

TELNET

[TELNET](#) is an acronym for [T](#)ELEtype [N](#)ETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol ([TCP](#)) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP

[TFTP](#) is an acronym for [T](#)rivial [F](#)ile [T](#)ransfer [P](#)rotocol. It is transfer protocol that uses the User Datagram Protocol ([UDP](#)) and provides file writing and reading, but it does not provides directory service and security features.

ToS

[ToS](#) is an acronym for [T](#)ype of [S](#)ervice. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

TLV

[TLV](#) is an acronym for Type Length Value. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

TKIP

[TKIP](#) is an acronym for Temporal Key Integrity Protocol. It used in WPA to replace WEP with a new encryption algorithm. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.

U

UDP

[UDP](#) is an acronym for User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol ([TCP](#)) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System ([DNS](#)), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol ([TFTP](#)).

UPnP

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

User Priority

[User Priority](#) is a 3-bit field storing the priority level for the 802.1Q frame.

V

VLAN

Virtual LAN: a method to restrict communication between switch ports. [VLANs](#) can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port [VLAN ID](#) 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

[VLAN ID](#) is a 12-bit field specifying the [VLAN](#) to which the frame belongs.

Voice VLAN

[Voice VLAN](#) is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

W

WEP

[WEP](#) is an acronym for Wired Equivalent Privacy. WEP is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages use radio, so are more susceptible to eavesdropping than wired networks. When introduced in 1999, WEP was intended to provide confidentiality comparable to that of a traditional wired network (Wikipedia).

WiFi

[WiFi](#) is an acronym for Wireless Fidelity. It is meant to be used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

WPA

[WPA](#) is an acronym for Wi-Fi Protected Access. It was created in response to several serious weaknesses researchers had found in the previous system , Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is specifically designed to also work with pre-WPA wireless network interface cards (through firmware upgrades), but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards (Wikipedia).

WPA-PSK

[WPA-PSK](#) is an acronym for Wi-Fi Protected Access - Pre Shared Key. WPA was designed to

enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPA-Radius

[WPA-Radius](#) is an acronym for Wi-Fi Protected Access - Radius (802.1X authentication server). WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPS

[WPS](#) is an acronym for Wi-Fi Protected Setup. It is a standard for easy and secure establishment of a wireless home network. The goal of the WPS protocol is to simplify the process of connecting any home device to the wireless network (Wikipedia).

WTR

[WTR](#) is an acronym for Wait To Restore. This is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource is done.