

MICROSENS

Product Manual | Firmware Generation 6

Version | 10.7.7a
Date | 2020-06-22

Address | MICROSENS
GmbH & Co. KG
Küferstraße 16
59067 Hamm/Germany
www.microsens.com

Classification | **MICROSENS**
PUBLICATION

Table of Contents

1. Introduction	3
2. Command Line Interface (CLI)	24
3. System Access	44
4. Access Control List (ACL)	60
5. Web Manager	68
6. Simple Network Management Protocol (SNMP)	81
7. RADIUS Servers	93
8. Network Time Protocol (NTP)	98
9. File Operations	105
10. Event Messages (Syslog, SNMP Notifications)	133
11. System Event Manager	148
12. Miscellaneous	153
13. Factory Information	160
14. System Information	166
15. Hardware Information	180
16. IP Stack	207
17. Port-specific Functions	220
18. SFP Transceiver	235
19. Power-over-Ethernet (PoE)	245
20. MAC Table	254
21. Remote Monitoring (RMON)	260
22. MSP 1000	271
23. SmartOffice	347
24. SmartOffice Controller	371
25. Wifi	404
26. Virtual LANs (VLANs)	414
27. Quality of Service (QoS)	434
28. Rapid Spanning Tree Protocol (RSTP)	445
29. Port-based Access Control	464
30. Multicast Traffic Filtering (IGMP Snooping)	484
31. Dynamic Host Configuration Protocol (DHCP)	497
32. Link Layer Discovery Protocol (LLDP)	513
33. Link Aggregation Control Protocol (LACP)	541
34. Ring	551
35. Message Queue Telemetry Transport (MQTT)	567
36. Modbus	586

37. Frequently Asked Questions	596
38. GNU General Public License v3	601
39. Disclaimer	609

1 Introduction

1.1 Scope of this Document

This document describes the detailed functionality of the firmware for MICROSENS Generation 6 switch products. It does not describe hardware specific product features.

Some of the features or functions described in this document may not be available on all products, depending on the hardware capabilities of the individual device. Please consult the product's hardware data sheet for further reference.

Network Management Platform

Most of the firmware functions can be accessed via the MICROSENS Network Management Platform (NMP), which is a separate product. The description of NMP functionality in relationship with the firmware is beyond the scope this document. Please see the NMP Manual for further reference.

1.2 Intended Audience

This document is intended as handbook for network technicians and administrators involved with the installation, administration and maintenance of MICROSENS Generation 6 products.

1.3 Supported Products

The firmware generation 6 described in this document supports the following hardware products:

Art.-No.	Description	Ports	Power
EQQ1032265	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: E2000 duplex, SM 1310nm, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
EQQ1069013	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: E2000 duplex, SM 1310nm, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
EQQ1069032	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS440200PM-48G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: ST duplex, MM 850nm, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440201PM-48G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: SC duplex, MM 850nm, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440202PM-48G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: SC duplex, SM 1300nm, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W

MS440203PM-48G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: ST duplex, SM 1300nm, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440207PM-48G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, SFP slot, Down: -	DC (44-57V) max. 80W
MS440207PMX-48G6-GT	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, horiz. mounting, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, SFP slot, Down: -	DC (44-57V) max. 80W
MS440207PMXH-48G6	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, horiz. mounting, holder for DIN-rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, SFP slot, Down: -	DC (44-57V) max. 80W
MS440208PM-48G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, Compact SFP Slot, Down: -	DC (44-57V) max. 80W
MS440208PMX-48G6-GT	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, horiz. mounting, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, Compact SFP Slot, Down: -	DC (44-57V) max. 80W
MS440208PMXH-48G6	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, horiz. mounting, holder for DIN-Rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, Compact SFP Slot, Down: -	DC (44-57V) max. 80W
MS440209PM-48G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440209PMX-48G6-GT	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, horiz. mounting, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440209PMXH-48G6	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, horiz. mounting, holder for DIN-rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS450186PM-48G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 10/100/1000B-TX, PD, RJ-45, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS450186MXH-G6+	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, horiz. mounting, holder for DIN-rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 10/100/1000B-TX, RJ-45, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS450186PMX-48G6	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, horiz. mounting, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 10/100/1000B-TX, PD, RJ-45, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W

MS450186PMX-48G6+	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal memory, PoE+, horiz. mounting, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 10/100/1000B-TX, PD, RJ-45, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS450186PMXH-48G6	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, horiz. mounting, holder for DIN-rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 10/100/1000B-TX, PD, RJ-45, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS450186PMXH-48G6+	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal memory, PoE+, horiz. mounting, holder for DIN-rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 10/100/1000B-TX, PD, RJ-45, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440210PM-48G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: ST duplex, MM 850nm, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440211PM-48G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: SC duplex, MM 850nm, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440212PM-48G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: SC duplex, SM 1300nm, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440213PM-48G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: ST duplex, SM 1300nm, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440217PM-48G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, SFP slots, Down: -	DC (44-57V) max. 80W
MS440217PMX-48G6-GT	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, vert. mounting, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, SFP slots, Down: -	DC (44-57V) max. 80W
MS440217PMXH-48G6	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, vert. mounting, holder for DIN-rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, SFP slots, Down: -	DC (44-57V) max. 80W
MS440217MX-12G6	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, vert. mounting, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 2x 100/1000B-X, SFP slots, Down: -	DC (12V) max. 10W
MS440217MXH-G6	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, vert. mounting, holder for DIN-rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 2x 100/1000B-X, SFP slots, Down: -	AC (230V) max. 10W
MS440217MXH-24G6	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, vert. mounting, holder for DIN-rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 2x 100/1000B-X, SFP slots, Down: -	DC (24V) max. 10W
MS440218PM-48G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, Compact SFP Slot, Down: -	DC (44-57V) max. 80W

MS440218PMX-48G6-GT	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, vert. mounting, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, Compact SFP Slot, Down: -	DC (44-57V) max. 80W
MS440218PMXH-48G6	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, vert. mounting, holder for DIN-Rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, Compact SFP Slot, Down: -	DC (44-57V) max. 80W
MS440219PM-48G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440219PMX-48G6-GT	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, vert. mounting, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440219PMXH-48G6	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, vert. mounting, holder for DIN-rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS450187PM-48G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 10/100/1000B-TX, PD, RJ-45, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS450187PMX-48G6	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, vert. mounting, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 10/100/1000B-TX, PD, RJ-45, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS450187PMX-48G6+	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal memory, PoE+, vert. mounting, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 10/100/1000B-TX, PD, RJ-45, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS450187PMXH-48G6	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, PoE+, vert. mounting, holder for DIN-rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 10/100/1000B-TX, PD, RJ-45, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS450187PMXH-48G6+	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal memory, PoE+, vert. mounting, holder for DIN-rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 10/100/1000B-TX, PD, RJ-45, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440200M-G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: ST duplex, MM 850nm, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS440201M-G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: SC duplex, MM 850nm, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS440202M-G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: SC duplex, SM 1300nm, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W

MS440203M-G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: ST duplex, SM 1300nm, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS440207M-G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, horiz. mounting	Local: x 10/100/1000B-TX, EEE, RJ-45, Up: 2x 100/1000B-X, SFP slot, Down: -	AC (230V) max. 10W
MS440208M-G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, Compact SFP Slot, Down: -	AC (230V) max. 10W
MS440209M-G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS450186M-G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 10/100/1000B-TX, RJ-45, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS440210M-G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: ST duplex, MM 850nm, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS440211M-G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: SC duplex, MM 850nm, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS440212M-G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: SC duplex, SM 1300nm, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS440213M-G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: ST duplex, SM 1300nm, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS440217M-G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 2x 100/1000B-X, SFP slots, Down: -	AC (230V) max. 10W
MS440218M-G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 2x 100/1000B-X, Compact SFP Slot, Down: -	AC (230V) max. 10W
MS440219M-G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS450187M-G6	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 10/100/1000B-TX, RJ-45, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS450187MXH-G6+	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, vert. mounting, holder for DIN-rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 10/100/1000B-TX, RJ-45, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS440200PM-48G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: ST duplex, MM 850nm, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440201PM-48G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: SC duplex, MM 850nm, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W

MS440202PM-48G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: SC duplex, SM 1300nm, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440203PM-48G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: ST duplex, SM 1300nm, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440207PM-48G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, SFP slot, Down: -	DC (44-57V) max. 80W
MS440207PMX-48G6+GT	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, horiz. mounting, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, SFP slot, Down: -	DC (44-57V) max. 80W
MS440207PMXH-48G6+	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, horiz. mounting, holder for DIN-rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, SFP slot, Down: -	DC (44-57V) max. 80W
MS440208PM-48G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, Compact SFP Slot, Down: -	DC (44-57V) max. 80W
MS440208PMX-48G6+GT	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, horiz. mounting, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, Compact SFP Slot, Down: -	DC (44-57V) max. 80W
MS440208PMXH-48G6+	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, horiz. mounting, holder for DIN-Rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, Compact SFP Slot, Down: -	DC (44-57V) max. 80W
MS440209PM-48G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440209PMX-48G6+GT	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, horiz. mounting, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440209PMXH-48G6+	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, horiz. mounting, holder for DIN-rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440209PMXH-24G6+	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, horiz. mounting, holder for DIN-rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	DC (24V) max. 10W

MS440210PM-48G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: ST duplex, MM 850nm, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440211PM-48G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: SC duplex, MM 850nm, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440212PM-48G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: SC duplex, SM 1300nm, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440213PM-48G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: ST duplex, SM 1300nm, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440217PM-48G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, SFP slot, Down: -	DC (44-57V) max. 80W
MS440217PMX-48G6+GT	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, vert. mounting, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, SFP slots, Down: -	DC (44-57V) max. 80W
MS440217PMXH-48G6+	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, vert. mounting, holder for DIN-rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, SFP slots, Down: -	DC (44-57V) max. 80W
MS440217MXH-G6+	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, vert. mounting, holder for DIN-rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 2x 100/1000B-X, SFP slots, Down: -	AC (230V) max. 10W
MS440217MXH-24G6+	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, vert. mounting, holder for DIN-rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 2x 100/1000B-X, SFP slots, Down: -	DC (24V) max. 10W
MS440218PM-48G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, Compact SFP Slot, Down: -	DC (44-57V) max. 80W
MS440218PMX-48G6+GT	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, vert. mounting, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, Compact SFP Slot, Down: -	DC (44-57V) max. 80W
MS440218PMXH-48G6+	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, vert. mounting, holder for DIN-Rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 2x 100/1000B-X, Compact SFP Slot, Down: -	DC (44-57V) max. 80W
MS440219PM-48G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W

MS440219PMX-48G6+GT	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, vert. mounting, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440219PMXH-48G6+	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, vert. mounting, holder for DIN-rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440219MXH-24G6+	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, vert. mounting, holder for DIN-rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	DC (24V) max. 10W
MS440219MXH-G6+	Ruggedized Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, vert. mounting, holder for DIN-rails, extended temperature range	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS445186PM-48G6+	Medical Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 10/100/1000B-TX, PoE+ PD, RJ-45, Down: 10/100/1000B-TX, PoE+ PSE, RJ-45	DC (44-57V) max. 30W
MS445207M-48G6+	Medical Micro Switch, 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 2x 100/1000B-X, SFP slot, Down: -	DC (44-57V) max. 10W
MS445207M-48G6	Medical Micro Switch, 6 ports Gigabit Eth., manageable, MicroSD card, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 2x 100/1000B-X, SFP slot, Down: -	DC (44-57V) max. 10W
MS445207M-G6+	Medical Micro Switch, 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 2x 100/1000B-X, SFP slot, Down: -	AC (230V) max. 10W
MS445207M-G6	Medical Micro Switch, 6 ports Gigabit Eth., manageable, MicroSD card, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 2x 100/1000B-X, SFP slot, Down: -	AC (230V) max. 10W
MS445209M-48G6+	Medical Micro Switch, 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 1x 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 10W
MS445209M-48G6	Medical Micro Switch, 6 ports Gigabit Eth., manageable, MicroSD card, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 1x 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 10W
MS445209M-G6+	Medical Micro Switch, 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 1x 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS445209PM-48G6+	Medical Micro Switch, 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 1x 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 10W
MS450186PM-48G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 10/100/1000B-TX, PD, RJ-45, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W

MS450187PM-48G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, PSE, RJ-45, Up: 10/100/1000B-TX, PD, RJ-45, Down: 10/100/1000B-TX, PSE, RJ-45	DC (44-57V) max. 80W
MS440200M-G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: ST duplex, MM 850nm, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS440201M-G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: SC duplex, MM 850nm, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS440202M-G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: SC duplex, SM 1300nm, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS440203M-G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: ST duplex, SM 1300nm, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS440207M-G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 2x 100/1000B-X, SFP slot, Down: -	AC (230V) max. 10W
MS440208M-G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 2x 100/1000B-X, Compact SFP Slot, Down: -	AC (230V) max. 10W
MS440209M-G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS450186M-G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, horiz. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 10/100/1000B-TX, RJ-45, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS440210M-G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: ST duplex, MM 850nm, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS440211M-G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: SC duplex, MM 850nm, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS440212M-G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: SC duplex, SM 1300nm, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS440213M-G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: ST duplex, SM 1300nm, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS440217M-G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 2x 100/1000B-X, SFP slots, Down: -	AC (230V) max. 10W
MS440218M-G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 2x 100/1000B-X, Compact SFP Slot, Down: -	AC (230V) max. 10W
MS440219M-24G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	DC (24V) max. 10W
MS440219M-G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W

MS450187M-G6+	Micro Switch 6 ports Gigabit Eth., manageable, MicroSD card + internal Flash, vert. mounting	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 10/100/1000B-TX, RJ-45, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 10W
MS450330M-G6+	Micro Switch 6 ports Fast Eth., manageable, MicroSD card + internal Flash, horiz. mounting	Local: 4x 10/100B-TX, EEE, RJ-45, Up: ST duplex, MM 1310nm, Down: 10/100B-TX, RJ-45	AC (230V) max. 10W
MS450330PM-48G6+	Micro Switch 6 ports Fast Eth., manageable, MicroSD card + internal Flash, horiz. mounting	Local: 4x 10/100B-TX, EEE, RJ-45, Up: ST duplex, MM 1310nm, Down: 10/100B-TX, RJ-45	DC (44-57V) max. 80W
MS450331M-G6+	Micro Switch 6 ports Fast Eth., manageable, MicroSD card + internal Flash, horiz. mounting	Local: 4x 10/100B-TX, EEE, RJ-45, Up: SC duplex, MM 1310nm, Down: 10/100B-TX, RJ-45	AC (230V) max. 10W
MS450331PM-48G6+	Micro Switch 6 ports Fast Eth., manageable, MicroSD card + internal Flash, horiz. mounting	Local: 4x 10/100B-TX, EEE, RJ-45, Up: SC duplex, MM 1310nm, Down: 10/100B-TX, RJ-45	DC (44-57V) max. 80W
MS450340M-G6+	Micro Switch 6 ports Fast Eth., manageable, MicroSD card + internal Flash, vert. mounting	Local: 4x 10/100B-TX, EEE, RJ-45, Up: ST duplex, MM 1310nm, Down: 10/100B-TX, RJ-45	AC (230V) max. 10W
MS450340PM-48G6+	Micro Switch 6 ports Fast Eth., manageable, MicroSD card + internal Flash, vert. mounting	Local: 4x 10/100B-TX, EEE, RJ-45, Up: ST duplex, MM 1310nm, Down: 10/100B-TX, RJ-45	DC (44-57V) max. 80W
MS450341M-G6+	Micro Switch 6 ports Fast Eth., manageable, MicroSD card + internal Flash, vert. mounting	Local: 4x 10/100B-TX, EEE, RJ-45, Up: SC duplex, MM 1310nm, Down: 10/100B-TX, RJ-45	AC (230V) max. 10W
MS450341PM-48G6+	Micro Switch 6 ports Fast Eth., manageable, MicroSD card + internal Flash, vert. mounting	Local: 4x 10/100B-TX, EEE, RJ-45, Up: SC duplex, MM 1310nm, Down: 10/100B-TX, RJ-45	DC (44-57V) max. 80W
MS453501PM-G6	Desktop Switch 6 Ports Gigabit Eth., manageable, MicroSD card, PoE	Local: 4x 10/100/1000B-TX, EEE, PoE (PSE), RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 80W
MS453501M-48G6	Desktop Switch 6 Ports Gigabit Eth., manageable, MicroSD card	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	DC (44-57V) max. 20W
MS453501PM-G6+	Desktop Switch 6 Ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE	Local: 4x 10/100/1000B-TX, EEE, PoE (PSE), RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 80W
MS453501M-48G6+	Desktop Switch 6 Ports Gigabit Eth., manageable, MicroSD card + internal Flash	Local: 4x 10/100/1000B-TX, EEE, RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	DC (44-57V) max. 80W
MS453501PM-48G6	Desktop Switch 6 Ports Gigabit Eth., manageable, MicroSD card, PoE	Local: 4x 10/100/1000B-TX, EEE, PoE (PSE), RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	DC (44-57V) max. 80W
MS453501PM-48G6+	Desktop Switch 6 Ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE	Local: 4x 10/100/1000B-TX, EEE, PoE (PSE), RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	DC (44-57V) max. 80W
MS453502PM-G6	Desktop Switch 6 Ports Gigabit Eth., manageable, MicroSD card, PoE+	Local: 4x 10/100/1000B-TX, EEE, PoE+ (PSE), RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 80W
MS453502PM-G6+	Desktop Switch 6 Ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+	Local: 4x 10/100/1000B-TX, EEE, PoE+ (PSE), RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 80W

MS453502PM-48G6	Desktop Switch 6 Ports Gigabit Eth., manageable, MicroSD card, PoE+	Local: 4x 10/100/1000B-TX, EEE, PoE+ (PSE), RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	DC (44-57V) max. 80W
MS453502PM-48G6+	Desktop Switch 6 Ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+	Local: 4x 10/100/1000B-TX, EEE, PoE+ (PSE), RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	DC (44-57V) max. 80W
MS453502PMX-48G6+	Ruggedized Desktop Switch 6 Ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+	Local: 4x 10/100/1000B-TX, EEE, PoE+ (PSE), RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	DC (44-57V) max. 80W
MS453503PM-48G6	Desktop Switch 6 Ports Gigabit Eth., manageable, MicroSD card, PoE	Local: 4x 10/100/1000B-TX, EEE, PoE (PSE), RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	DC (44-57V) max. 80W
MS453504PM-G6	Desktop Switch 6 Ports Gigabit Eth., manageable, MicroSD card, PoE+	Local: 4x 10/100/1000B-TX, EEE, PoE+ (PSE), RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 80W
MS453504PM-G6+	Desktop Switch 6 Ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+	Local: 4x 10/100/1000B-TX, EEE, PoE+ (PSE), RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	AC (230V) max. 80W
MS453504PM-48G6	Desktop Switch 6 Ports Gigabit Eth., manageable, MicroSD card, PoE+	Local: 4x 10/100/1000B-TX, EEE, PoE+ (PSE), RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	DC (44-57V) max. 80W
MS453504PM-48G6+	Desktop Switch 6 Ports Gigabit Eth., manageable, MicroSD card + internal Flash, PoE+	Local: 4x 10/100/1000B-TX, EEE, PoE+ (PSE), RJ-45, Up: 100/1000B-X, SFP slot, Down: 10/100/1000B-TX, RJ-45	DC (44-57V) max. 80W
MS650919PM	Industrial Gigabit Switch PL+, 7 Ethernet-Ports, SD card, Serial Port, I/O-Ports: 2x in, 2x out,	4x 10/100/1000B-TX, PoE+ (PSE), RJ-45, 1x 10/100/1000B-TX, PoE+ (PD), RJ-45, 2x Dual Media: 100/1000B-X, SFP slot or 10/100/1000B-TX, RJ-45, 1x USB, 2x I/O	2x DC Input 24-57VDC, redundant, max. 200W
MS650919PM-BS	Industrial Gigabit Switch PL+, 7 Ethernet-Ports, SD card, Serial Port, I/O-Ports: 2x in, 2x out, Railway, Substation	4x 10/100/1000B-TX, PoE+ (PSE), RJ-45, 1x 10/100/1000B-TX, PoE+ (PD), RJ-45, 2x Dual Media: 100/1000B-X, SFP slot or 10/100/1000B-TX, RJ-45, 1x USB, 2x I/O	2x DC Input 24-57VDC, redundant, max. 200W
MS650929PM	Industrial Gigabit Switch PL+, 7 Ethernet-Ports, SD card, Serial Port, I/O-Ports: 2x in, 2x out,	4x 10/100/1000B-TX, 2x 60W PoE+ (PSE), RJ-45, 1x 10/100/1000B-TX, PoE+ (PD), RJ-45, 2x Dual Media: 100/1000B-X, SFP slot or 10/100/1000B-TX, RJ-45, 1x USB, 2x I/O	2x DC Input 24-57VDC, redundant, max. 200W
MS652119PM	Industrial Gigabit Switch PLM, 13 Ethernet-Ports, SD card, Serial Port, I/O-Ports: 2x in, 2x out, Expansion-Bus: 1x out	8x 10/100/1000B-TX, PoE+ (PSE), RJ-45, 1x 10/100/1000B-TX, PoE+ (PD), RJ-45, 4x Dual Media: 100/1000B-X, SFP slot or 10/100/1000B-TX, RJ-45, 1x USB, 2x I/O	2x DC Input 24-57VDC, redundant, max. 200W
MS652119PM-V2	Industrial Gigabit Switch PLM, 13 Ethernet-Ports, SD card, Serial Port, I/O-Ports: 2x in, 2x out, Expansion-Bus: 1x out	8x 10/100/1000B-TX, PoE+ (PSE), RJ-45, 1x 10/100/1000B-TX, PoE+ (PD), RJ-45, 4x Dual Media: 100/1000B-X, SFP slot or 10/100/1000B-TX, RJ-45, 1x USB, 2x I/O	2x DC Input 24-57VDC, redundant, max. 240W

MS652119PM-B	Industrial Gigabit Switch PLM, 13 Ethernet-Ports, SD card, Serial Port, I/O-Ports: 2x in, 2x out, Expansion-Bus: 1x out, Railway	8x 10/100/1000B-TX, PoE+ (PSE), RJ-45, 1x 10/100/1000B-TX, PoE+ (PD), RJ-45, 4x Dual Media: 100/1000B-X, SFP slot or 10/100/1000B-TX, RJ-45, 1x USB, 2x I/O	2x DC Input 24-57VDC, redundant, max. 200W
MS652119PM-BS	Industrial Gigabit Switch PLM, 13 Ethernet-Ports, SD card, Serial Port, I/O-Ports: 2x in, 2x out, Expansion-Bus: 1x out, Railway, Substation	8x 10/100/1000B-TX, PoE+ (PSE), RJ-45, 1x 10/100/1000B-TX, PoE+ (PD), RJ-45, 4x Dual Media: 100/1000B-X, SFP slot or 10/100/1000B-TX, RJ-45, 1x USB, 2x I/O	2x DC Input 24-57VDC, redundant, max. 60W
MS652129PM	Industrial Gigabit Switch PLM, 13 Ethernet-Ports, SD card, Serial Port, I/O-Ports: 2x in, 2x out, Expansion-Bus: 1x out	8x 10/100/1000B-TX, 4x 60W PoE+ (PSE), RJ-45, 1x 10/100/1000B-TX, PoE+ (PD), RJ-45, 4x Dual Media: 100/1000B-X, SFP slot or 10/100/1000B-TX, RJ-45, 1x USB, 2x I/O	2x DC Input 24-57VDC, redundant, max. 200W
MS652159PM	Industrial Gigabit Switch PLM, 13 Ethernet-Ports, SD card, Serial Port, I/O-Ports: 2x in, 2x out, Expansion-Bus: 1x out	8x 10/100/1000B-TX, 4x 60W PoE+ (PSE), RJ-45, 1x 10/100/1000B-TX, PoE+ (PD), RJ-45, 4x Dual Media: 100/1000B-X, SFP slot or 10/100/1000B-TX, RJ-45, 1x USB, 2x I/O	1x DC Input 24-57VDC, redundant, max. 480W
MS652219M	Profi Line Modular (PLM) 6 Port Expansion Module	4x 10/100/1000B-TX, PoE+ (PSE), RJ-45, 2x Dual Media: 100/1000B-X, SFP slot or 10/100/1000B-TX, RJ-45	
MS652419M	Profi Line Modular (PLM) 12 Port Expansion Module	8x 10/100/1000B-TX, PoE+ (PSE), RJ-45, 4x Dual Media: 100/1000B-X, SFP slot or 10/100/1000B-TX, RJ-45	
MS400890MX	Ruggedized 19" Gigabit Switch PLR, 25 Ethernet-Ports, SD card, Serial Port, I/O-Ports: 2x in, 2x out	16x 10/100/1000B-TX, PoE+ (PSE), RJ-45, 1x 10/100/1000B-TX, PoE+ (PD), RJ-45, 8x Dual Media: 100/1000B-X, SFP slot or 10/100/1000B-TX, RJ-45, 1x USB, 2x I/O	2x DC Input 24-57VDC, redundant, max. 200W
MS400890MX-V2	Ruggedized 19" Gigabit Switch PLR, 25 Ethernet-Ports, SD card, Serial Port, I/O-Ports: 2x in, 2x out	16x 10/100/1000B-TX, PoE+ (PSE), RJ-45, 1x 10/100/1000B-TX, PoE+ (PD), RJ-45, 8x Dual Media: 100/1000B-X, SFP slot or 10/100/1000B-TX, RJ-45, 1x USB, 2x I/O	2x DC Input 24-57VDC, redundant, max. 240W
MS400890MX-BS	Ruggedized 19" Gigabit Switch PLR, 25 Ethernet-Ports, SD card, Serial Port, I/O-Ports: 2x in, 2x out, Railway, Substation	16x 10/100/1000B-TX, PoE+ (PSE), RJ-45, 1x 10/100/1000B-TX, PoE+ (PD), RJ-45, 8x Dual Media: 100/1000B-X, SFP slot or 10/100/1000B-TX, RJ-45, 1x USB, 2x I/O	2x DC Input 24-57VDC, redundant, max. 200W
MS400895MX	Ruggedized 19" Gigabit Switch PLR, 25 Ethernet-Ports, SD card, Serial Port, I/O-Ports: 2x in, 2x out	16x 10/100/1000B-TX, PoE+ (PSE), RJ-45, 1x 10/100/1000B-TX, PoE+ (PD), RJ-45, 8x Dual Media: 100/1000B-X, SFP slot or 10/100/1000B-TX, RJ-45, 1x USB, 2x I/O	1x DC Input 24-57VDC, redundant, max. 480W
MS425523M	NM3 Management Agent Module for MSP 1000 Platform, SNMP, Web-Server, 4 Ethernet-Ports, MicroSD card, Console Port, 2x SFP Slots	2x 10/100/1000B-TX, RJ-45, 1x RS-232 (RJ-45), 2x 100/1000B-X, SFP slot	

MS425524M	NM3+ Management Agent Module for MSP 1000 Platform, SNMP, Web-Server, 6 Ethernet-Ports, MicroSD card, Console Port, 2x SFP Slots, I/O-Ports: 2x in, 2x out	4x 10/100/1000B-TX, RJ-45, 1x RS-232 (RJ-45), 2x 100/1000B-X, SFP slot, 1x USB, 2x I/O	
MS660301M	Central Smart Lighting Controller, Mgmt, SD card, 1x GBE/FE, 24x LED RJ45, 4x Sensor RJ45, 2x Input, 2x Output	1x 10/100/1000B-TX, 24x LED RJ45, 4x Sensor RJ45, 2x Input, 2x Output	2x DC Input 54VDC, redundant, max. 1000W
MS660301M-V2	Central Smart Lighting Controller, Mgmt, SD card, 1x GBE/FE, 24x LED RJ45, 4x Sensor RJ45, 2x Input, 2x Output, Fan	1x 10/100/1000B-TX, 24x LED RJ45, 4x Sensor RJ45, 2x Input, 2x Output	2x DC Input 54VDC, redundant, max. 1000W
MS660301M-V4	Central Smart Lighting Controller, Mgmt, SD card, 3x FE Uplink, 24x LED, 2x Sensor Inputs, Fan	3x 10/100B-TX, 24x LED RJ45, 2x Sensor RJ45	1x DC Input 54VDC

1.4 Document Structure

This document describes each firmware subject in a separate section – beginning with the different ways to manage the switch (for instance: 'CLI', 'System Access', 'Web Manager', 'SNMP'), followed by the hard- and software features of the device (for instance: 'Factory', 'Hardware', 'SFPs', 'POE') and the available protocols (for instance: 'VLAN', 'QOS', 'RSTP', 'PACC').

Key Features

This section lists and describes the key features of the feature-group.

Functional Description

This section describes and explains the concept and functionality of the feature-group.

CLI Command Reference

This section lists all parameters applicable for the feature-group and gives the possible access modes ('Read Only', 'Read/Write' or 'Executable Action'). For each group the path in the CLI is provided. When navigating in the CLI, with this path from the root the individual parameter can be addressed. See 'Command Line Interface (CLI)' section of this manual for further reference.

Configuration Parameters

This section lists all configuration parameters provided by the feature-group and shows all possible values a configuration parameter can adopt as well as the object identifier (OID), which is needed to configure the parameter by SNMP. See 'Simple Network Management Protocol (SNMP)' section of this manual for further reference.

The parameters may be arranged in groups or lists. For each list the size of the index is provided.

Configuration values can be written and control the behaviour of individual features. Configuration values are stored device internally in configuration files (per feature-section). These files can be accessed for backup and restore purposes. See 'File Operations' section of this manual for further reference.

Status Parameters

This section lists all status parameters provided by the feature-group and shows all possible values a status parameter can adopt as well as the object identifier (OID), which is needed to access the parameter by SNMP. See 'Simple Network Management Protocol (SNMP)' section of this manual for further reference. Status values are read-only and refer to internal states of the device.

1.5 Default User Accounts

The following user accounts are predefined:

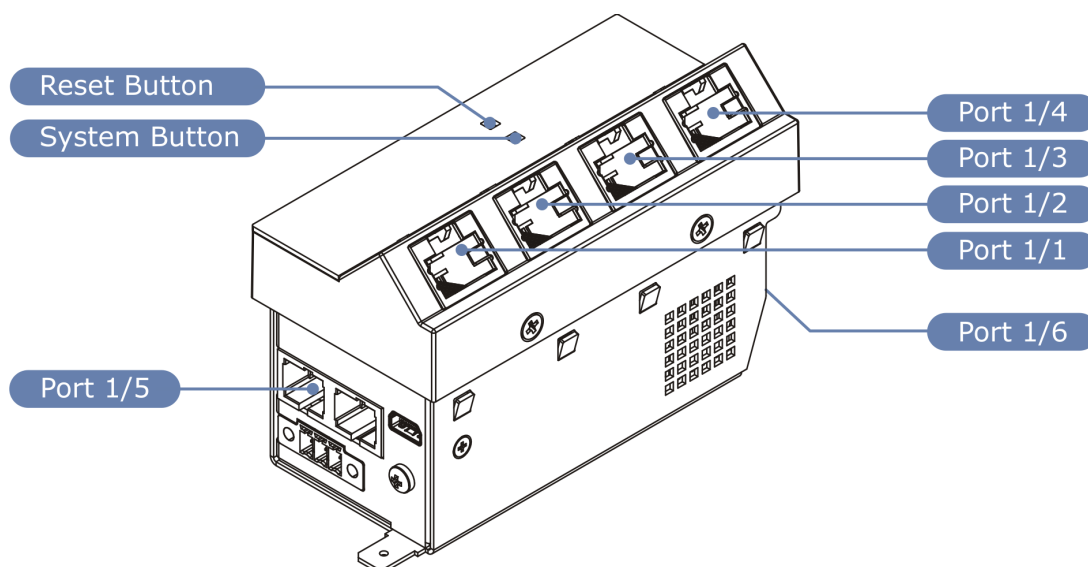
Username	Password	Access Permissions
admin	administrator	Read / Write
user	microsens	Read / Write (limited)
public	microsens	Read Only

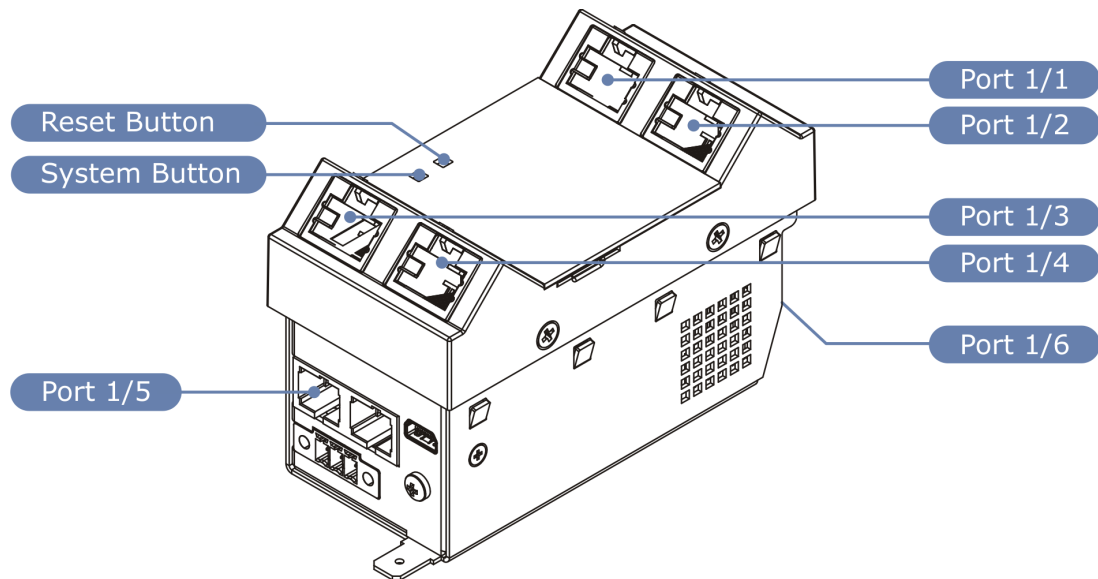
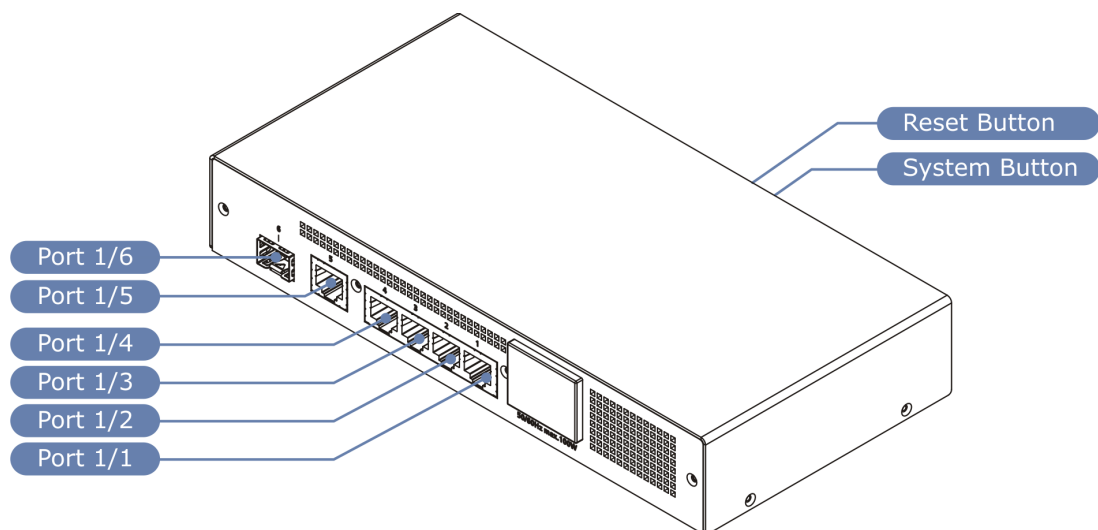
See 'System Access' section of this manual for further reference.

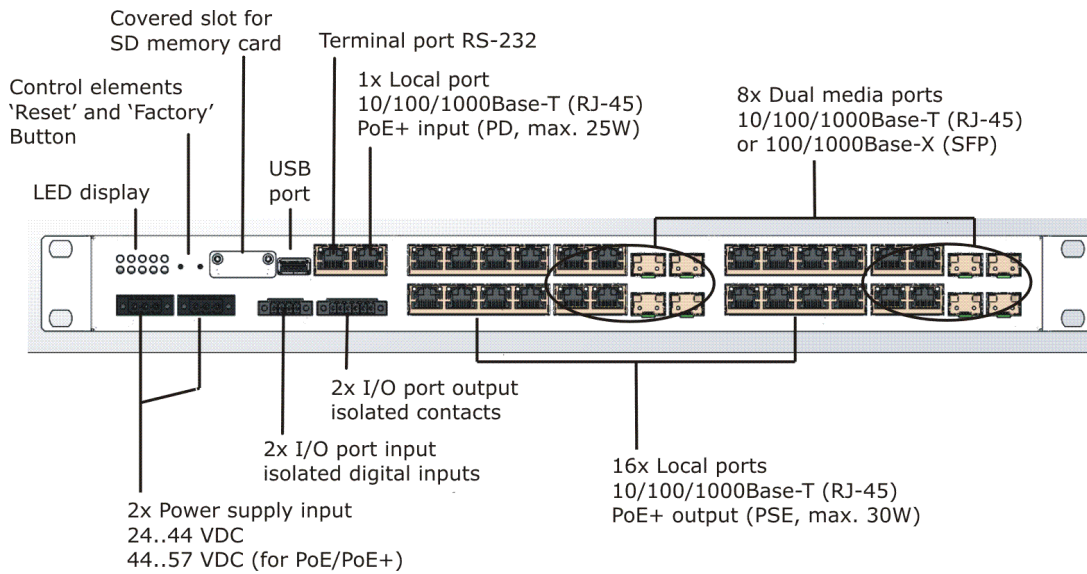
1.6 Device Interface Reference

As the firmware supports different hardware models, the following sections define the location and designations of all interfaces used by the firmware for the individual models.

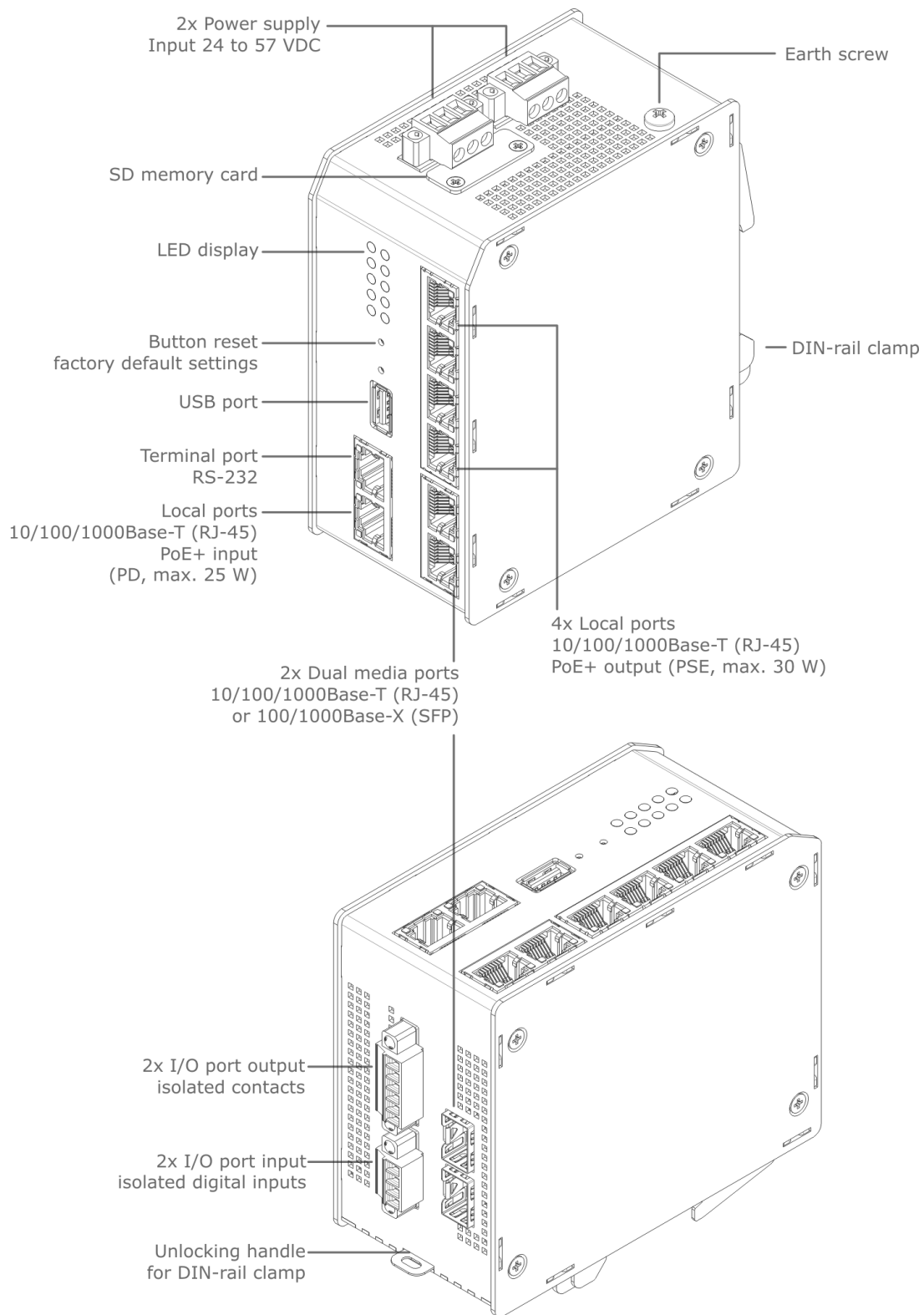
Interface definitions for Micro Switch (incl. ruggedized version), horizontal mounting:



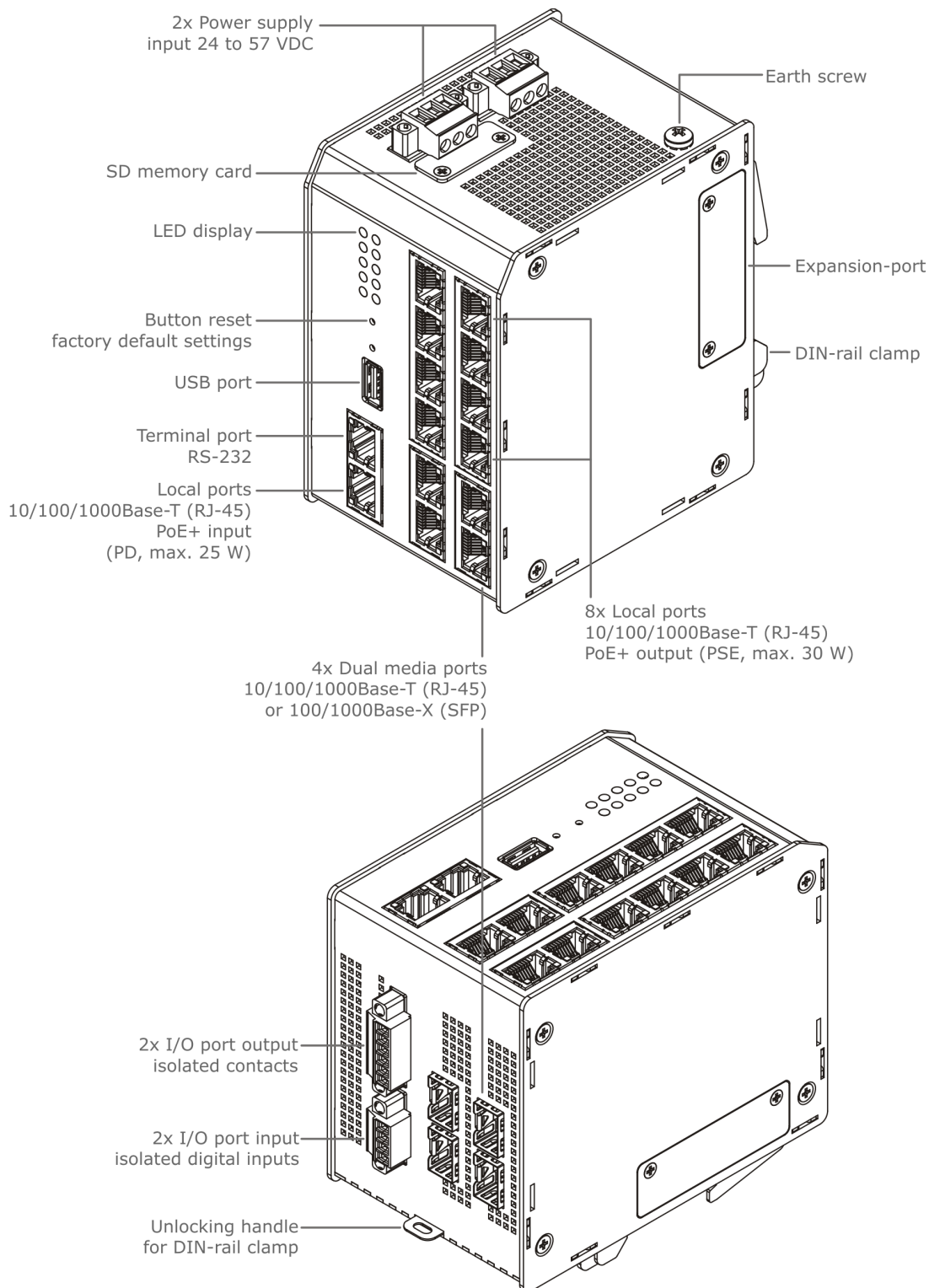
Interface definitions for Micro Switch (incl. ruggedized version), vertical mounting:**Interface definitions for Desktop Switch:**

Interface definitions for Industrial 19" Switch Profi Line Rack (PLR):

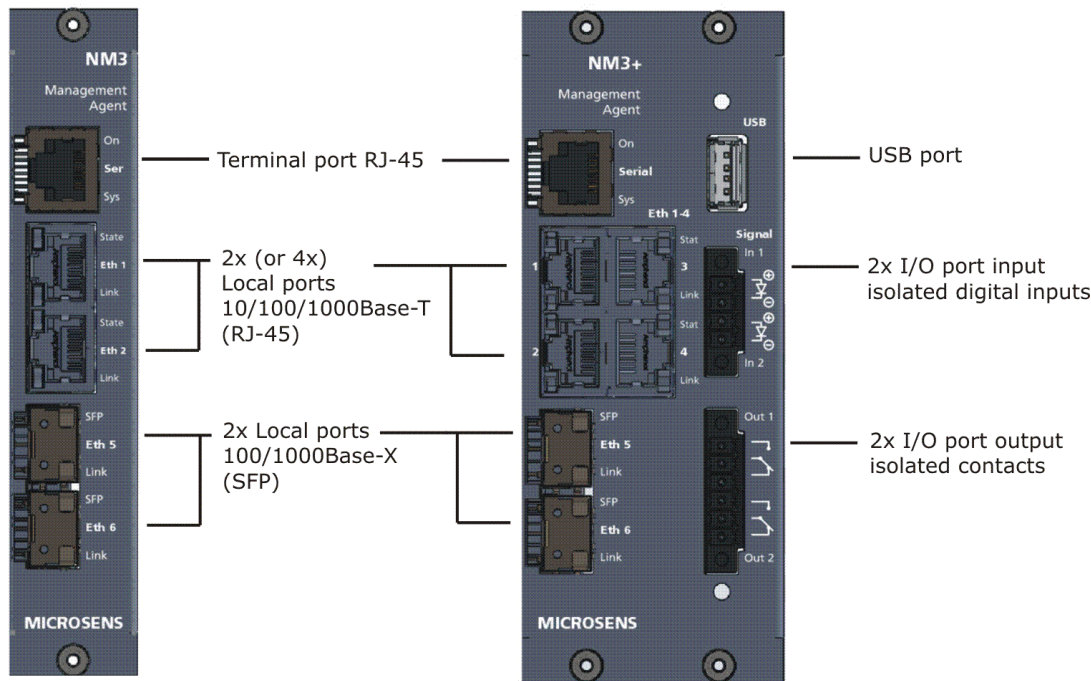
Interface definitions for Industrial Switch Profi Line + (PL+):



Interface definitions for Industrial Switch Profi Line Modular (PLM):

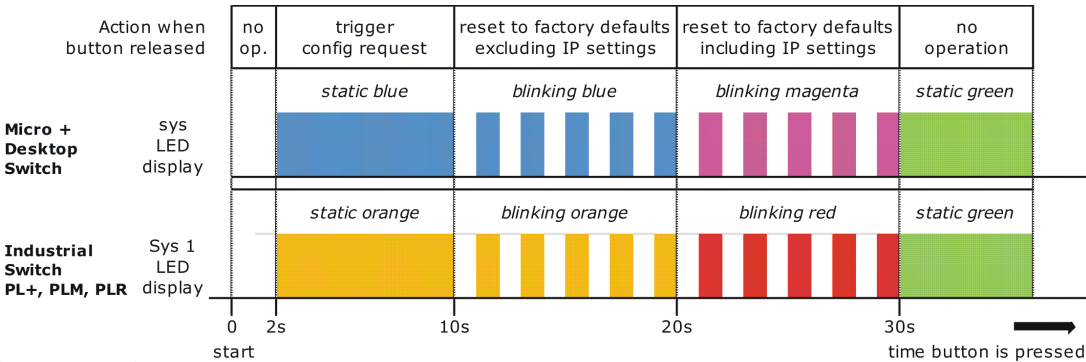


Interface definitions for MSP 1000 Network Management Agents (NM3 and NM3+):



1.7 System Button Reset Sequence

The 'System' button provides different functionalities when pressed. The 'sys' LED changes display to indicate action performed when button is released.



Duration pressed	Action performed
less than 2 sec.	No operation is performed. This minimum delay prevents accidental triggering of an action by pressing the 'System' button. The 'sys' LED remains switched off
2-10 sec.	Switch sends configuration request packet to NMP software, requesting for initialisation of IP interface. This function is only available when NMP software is running on a PC connected to the same network segment as the switch. When receiving the config request packet, a message box opens up showing the current IP settings. This function is very useful to set the initial IP stack values if the switch is unconfigured. This mode is indicated by the 'sys' LED static blue (Industrial Switch: static orange).
10-20 sec.	Switch resets the running configuration to the factory default configuration. All parameters are overwritten except the IP address settings. This mode is indicated by the 'sys' LED blinking blue (Industrial Switch: blinking orange).
20-30 sec.	Switch resets the running configuration to the factory default configuration. All parameters are overwritten including the IP address settings. This mode is indicated by the 'sys' LED blinking magenta (Industrial Switch: blinking red).
more than 30 sec.	Switch goes back to normal operation without performing any special action. This mode is indicated by the 'sys' LED static green.

1.8 Permitted / not permitted Characters

1.8.1 Generally not permitted characters

ASCII codes <32 and >126 (unless ISO 8859 is permitted)

Characters: < > ' & " „ " Â Ã (TAB)

1.8.2 Permitted characters for usage in passwords

Digits: 0-9

Letters: a-z, A-Z

Characters: # \$ % ? () ! . @ % = { } ~ + - , ^ _ (underscore) (space) in the middle

INFO: In passwords leading and subsequent blanks will be cut off and multiple blanks will be merged to one single blank.

1.8.3 Permitted characters for usage in CLI, web manager, scripting, text, strings, etc.

Digits: 0-9

Letters: a-z, A-Z

Characters: # \$ * ? () [] / \ ' @ % = { | } ~ + - ! . : ; , ^ _ (underscore) (space)

1.8.4 Support of ISO/IEC 8859-1 (Since V10.4.1):

Since Firmware version 10.4.1 German Umlaute, French Accents, etc. are supported in all user interfaces for selected descriptive parameters.

Support of ISO 8859-1 coding as follows:

ISO/IEC 8859-1

Code	...0	...1	...2	...3	...4	...5	...6	...7	...8	...9	...A	...B	...C	...D	...E	...F
0...	not used															
1...	not used															
2...	SP	!	"	#	\$	%	&	'	()	*	+	,	-	.	/
3...	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4...	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5...	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
6...	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7...	p	q	r	s	t	u	v	w	x	y	z	{		}	~	
8...	not used															
9...	not used															
A...	NBSP	í	¢	£	¥	¦	§	¨	©	ª	«	¬	SHY	®	¯	
B...	°	±	²	³	´	µ	¶	·	¸	¹	º	»	¼	½	¾	¿
C...	À	Á	Â	Ã	Ä	Å	Æ	Ç	È	É	Ê	Ë	Ì	Í	Î	Ï
D...	Ð	Ñ	Ò	Ó	Ô	Õ	Ö	×	Ø	Ù	Ú	Û	Ü	Ý	Þ	ß
E...	à	á	â	ã	ä	å	æ	ç	è	é	ê	ë	ì	í	î	ï
F...	ð	ñ	ò	ó	ô	õ	ö	÷	ø	ù	ú	û	ü	ý	þ	ÿ

Generally not permitted character

INFO: In CLI search for Keyword "\$ISO8859" to find out, which character range is permitted for an individual parameter.

2 Command Line Interface (CLI)

2.1 Key Features

Base Features

Intuitive command line interface to manage every aspect of the device. Supports wildcards and named ports as variables. Quick command entry due to auto-completion and command recall buffer. Individual console prompt string, Console inactivity timeout automatically logs out unattended terminal. Supports color displays. Online help for each parameter by typing a ?.

The command line interface (CLI) is the most direct way to manage the device. Guided operation leads the operator with just a brief learning phase. The CLI it is very convenient and quick to use. The CLI is invoked when a Telnet or SSH session is opened.

Context Sensitive Help

Type ? anywhere while editing and context sensitive help regarding the current parameter is provided.

Helps inexperienced user. No need for a handbook. All options individually explained similar to the handbook.

Offline Configuration

Offline configuration permits editing of an unlimited number of user configuration sets. These configurations may be copied, viewed, up and downloaded by file transfer protocols. Offline configurations can be made online at any time.

Offline configurations or alternate configuration permit complex setups without affecting the device operation. On completion the entire configuration changes are activated in one go. Of course direct editing with immediate effect is available too.

Comprehensive Editing

All parameter are shown and edited with the same syntax. No handbook needed for operation. Command options can be scrolled. For numbers values ranges are shown. Parameter can be written for ranges or wildcards.

Even complex settings are quickly accomplished. No need to memorize a complex syntax.

Scripting

Supports full scripting and editing of script files. A script may execute any CLI command provided the access rights are valid. Scripts may locally be edited or downloaded. A script may also be downloaded by DHCP/BOOTP function when a unit is newly connected to the network. Such script may reconfigure the device, load other scripts or even download and install a software update.

Scripts are a powerful tool to automate operation with a large number of devices that require a similar customer setup.

microScript Language

Powerful and comprehensive script language permits customized active functions which greatly increase flexibility of the product.

Special functions that in past would have required a specially made firmware can now be implemented by the customer himself or by the technical support team.

Timer Controlled Scripting

Scripts support timed single shot or cyclical invocation. Useful to implement time outs for error handling,

Simplifies exception script handling. May also be used for timed execution.

Show All Config

With the ShowAllConfig command the entire configuration can be displayed to console and simultaneously to a script file. The script can be used as backup or to configure other units. The command may also be used to display only the differences to any stored or default configuration.

The script output can be used for automation purposes for example in combination with DHCP option 66/67. The script can also form the basis for manually written scripts.

Show All Status

With the ShowAllStatus command the entire status of any parameter is displayed to console and simultaneously to a script file.

The script can be saved as backup for later reference or may be used as input to an automated test script.

Create Snapshot

Creates a snapshot of all relevant system information including all config, status, internal process details.

The snapshot file can be uploaded to support team for comprehensive analysis. This is especially helpful in a secured network, where remote access is not permitted.

Live Syslog

Syslog events can be forwarded to the active console the moment they occur. Filtering according to logging setup applies.

Unexpected events are shown on the console. Usually terminals of other products do not show events.

Telnet

A telnet session automatically invokes the cli. Telnet may be disabled in total or per user to enforce use of the more secure SSH method.

Popular terminal interface for device management. It is safeguarded by the login/password process but offers no further security.

Secure Shell (SSH)

An SSH session automatically invokes the cli. SSH may be disabled by configuration.

Terminal interface for device management. It is safeguarded by the login/password process plus the data transfer is encrypted. The use of this interface is encouraged.

Welcome Message

A customer programmable welcome message can be defined. This is shown prior to login prompt. May also be used to indicate warning to deter malicious user. Multiline output supported.

Helps to identify the proper device prior to login. May also be used to indicate warning to deter malicious user.

Umlaut Support

Support for German Umlaute, French Accents, etc. in all user interfaces for selected parameters. Supports ISO 8859-1 coding.

User defined names and information field can be written in correct spelling even if non-ASCII characters are required.

Favorites

Most often used commands can be entered as favorites and then be executed with a single key stroke (F).

Further simplifies use for frequent CLI operators.

2.2 Functional Description

2.2.1 Introduction

The command line interface (CLI) may be used to control and monitor the device. The CLI permits full access to every aspect of the device. Access to the CLI is established via the local serial port or by Telnet or SSH access via one of the Ethernet ports. The device uses a state-of-the-art data driven and XML based configuration scheme. The CLI automatically learns the available XML templates and as such can never be out of date, even should extensive firmware upgrades occur.

2.2.2 Access Control

The CLI uses a user/password scheme for access control. The same names scheme applies as used for SNMPv3. Access may be restricted to Telnet or SSH individually and for each user independently. Furthermore a view based restriction applies. A user may be allowed to see and/or modify only certain aspects of the product. All of these functions are governed by the *'management.access'* section of the configuration tree structure.

Default User Accounts

The following user accounts are predefined:

Username	Password	Access Permissions
admin	administrator	Read / Write
user	microsens	Read / Write (limited)
public	microsens	Read Only

Logout

Use *'Logout'* command to exit the CLI and close the session. There is an inactivity timer that automatically logs-off the CLI after 5 minutes (Default value).

2.2.3 Basic Operation

The CLI is started automatically upon successful login.

```
Command Line Interface (CLI) / MICROSENS GmbH / Co. KG
You are logged in as admin (id:1) from IP -
Your general access rights are: Read/Write

Type ? for help on operation and for parameter details.
>>
```

The welcome lines indicates your login name and the associated general access rights. Type '?' for a brief summary of the CLI basic operation.

The CLI is designed for convenient operation without the need to remember the various keywords. The cursor keys can be used to navigate through the options. Alternatively, typing the first letters of the keywords, the input is auto-expanded to the full word when it is clearly detected. The two modes of operation may be mixed freely as desired.

2.2.4 Cursor Operation

[*CursorRight*] shows the first keyword of the next branch in the tree.

[*CursorLeft*] steps back to the previous tree level. This deletes the entire keyword at once.

[*CursorUp/Down*] shows the keywords available at the current tree layer.

A '.' (dot) behind the keyword indicates that there is a further layer available that may be selected by [*CursorRight*]. At any time it is possible to type [*Return*]. For incomplete commands a help is displayed which lists the available keywords. Whenever possible, the CLI will display the information of all elements in that layer.

INFO: [*CursorUp*] redisplayes the last command line for further editing.

Any further [*CursorUp*] will change the last keyword. There is a recall buffer that keeps the last 10 commands. The recall buffer is accessed using the [*PageUp*] and [*PageDown*] keys.

INFO: Not every terminal supports these keys. (VT102/VT220 emulation)

Some operators prefer to type the commands in full. This mode is facilitated by setting

```
Management.CLI.auto_text_expansion = Disabled
```

Even in this mode, it is always possible to type [*CursorRight*] to auto-complete a keyword. A few examples:

User typed [*Return*] right after 'Device.' first level in the tree:

```
>>Device.
INCOMPLETE COMMAND: Type . or cursor right for next keyword level.
Add any of the following keywords:
    Factory
    System
    Hardware
    IP
    Port
    SFP
    POE
    MAC
```

```
RMON
>>
```

When on the last level before the end of the tree, typing [*Return*] displays the underlying data at once. Like in this example:

```
>>Management.CLI.
enable_telnet      : Enabled
enable_ssh         : Enabled
prompt_source      : HOSTNAME
user_prompt        : MICROSENS
colors             : Enabled
script_mode        : Disabled
auto_text_expansion : Enabled
dont_ask_questions : Disabled
inactivity_timeout : 300
num_of_clis        : 1
last_command       : Management.CLI.
Note additional tables : .recall_buffer
>>
```

INFO: Often data is grouped in tables. When data is available for display in the current tree layer, and others require more depth to execute, then the data at the current layer is shown and an indication to the other data in a further layer is made in this way: 'Note additional table: xxxx'

2.2.5 Setting Values

When a command is fully typed in, no trailing dot is displayed. Type [*Return*] to display or type '=' to set a new value.

Depending on the type of parameter, either a string or value can be entered or a list of options may be scrolled through using [*Cursor Up/Down*] keys.

2.2.6 Getting Help

At any level it is possible to retrieve help information for the currently selected layer or parameter by simply typing '?' (question mark). New lines with information are shown, then the edited line is redisplayed for further editing.

```
>>Device.IP.local_mtu ?
MTU value for locally generated data.
Default value: 1500
Range: 128-9000
>>Device.IP.local_mtu
```

This help is available even for every individual parameter item, when such items are displayed. Example:

```
>>Management.CLI.prompt_source = USER_DEFINED ?
A user defined string as defined in 'user_prompt' is used as prompt
```

```
Default value: 3
>>Management.CLI.prompt_source = USER_DEFINED
```

2.2.7 Script Mode

While the default editing is intended for human input, the CLI is fully scriptable and may be operated through command files and from scripting engines. For this purpose the CLI settings should be changed.

For script mode enter the following commands:

```
Management.CLI.auto_text_expansion = Disabled
Management.CLI.script_mode = Enabled
```

The CLI comes with an editor that permits to write CLI scripts. A CLI script may contain any command that could be written.

Note that the line editor discards wrong characters. For example the word *devixce* would be treated like *device*. The extra *x* is ignored. Likewise *devic.hardware* would fail due to the missing *e* in *device*.

INFO: When 'script_mode' is enabled, the command output is changed to reflect the required input line to set that value.

Example with script mode disabled:

```
>>Management.CLI.colors = Disabled
colors: Disabled
>>
```

The same example with script mode enabled:

```
>>Management.CLI.colors = Disabled
Management.CLI.colors = Disabled
>>
```

The output of the command can be used to set the value again. Therefore it is convenient to display what should go into the script file. Copy that output into the terminal clipboard and then paste the contents in the script editor. Then modify to taste.

Lists all available script files

To display all available script files stored on the device use the following command:

```
Management.Files.scripts.list_files
```

Execute a script file

To execute a script files use the following command:

```
RunScriptFile = filename
```

INFO: It is not required to switch the CLI configuration to 'script_mode' before executing a script. The 'RunScriptFile' command does this automatically and returns to the previously selected mode afterwards.

Comments in Script Files

Script files can contain comments for documentation and simplified understanding. A comment line must start with the character '#', all following characters are ignored until the end of the line.

```
# This is a comment line
# All text is ignored until line end
...
```

Built-in script editor

To edit a script simply use the following command. If the name does not already exist, a new file is created:

```
EditScriptFile = filename
```

This action starts the integrated MCEdit text editor. As this editor runs in full-screen mode, there may be compatibility issues with the terminal emulation used by the CLI session. For best results we recommend using 'PuTTY', which is a powerful, free Telnet and SSH client.

```

192.168.20.202 - PuTTY
/usr/local/plate.scr  [----]  0 L:[ 1+ 0  1/ 34] *(0 /1394b)  35 0x023
# Add port VLAN filter entries
Protocol.VLAN.filter_config[*].vlan_id = 101
Protocol.VLAN.filter_config[*].vlan_id = 102
Protocol.VLAN.filter_config[*].vlan_id = 103
Protocol.VLAN.filter_config[*].vlan_id = 104

# Add port membership for VLANs
Protocol.VLAN.filter_config[101].port_members = 1/1, 1/5, 1/6
Protocol.VLAN.filter_config[102].port_members = 1/2, 1/5, 1/6
Protocol.VLAN.filter_config[103].port_members = 1/3, 1/5, 1/6
Protocol.VLAN.filter_config[104].port_members = 1/4, 1/5, 1/6

# Set port VLAN mode
Protocol.VLAN.port_config[1/1].vlan_mode = ACCESS
Protocol.VLAN.port_config[1/2].vlan_mode = ACCESS
Protocol.VLAN.port_config[1/3].vlan_mode = ACCESS
Protocol.VLAN.port_config[1/4].vlan_mode = ACCESS
Protocol.VLAN.port_config[1/5].vlan_mode = TRUNK
Protocol.VLAN.port_config[1/6].vlan_mode = TRUNK

# Set port default VLAN
Protocol.VLAN.port_config[1/1].default_vlan_id = 101
Protocol.VLAN.port_config[1/2].default_vlan_id = 102
Protocol.VLAN.port_config[1/3].default_vlan_id = 103
Protocol.VLAN.port_config[1/4].default_vlan_id = 104

# Add Management VLAN settings
Protocol.VLAN.filter_config[*].vlan_id = 99
Protocol.VLAN.filter_config[99].port_members = 1/5, 1/6
Protocol.VLAN.filter_config[99].management_members = ALL
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn10Quit

```

The editor supports function keys and pull-down menus. Please see the documentation section at 'www.midnight-commander.org' for a detailed description of all functions.

Pressing 'F10' function key closes the editor and returns to normal CLI mode.

Up-/Download of script files

```

Management.Files.scripts.download_from_server =
    ftp://name:passwd@machine.domain:port/full/path/to/scriptfile

Management.Files.scripts.upload_to_server = scriptfile -u
    user:passwd ftp://ftp.upload.com/

```

These last two commands permit transfer of script files from/to external servers. There is a variety of protocols available for transfer. This includes HTTP, HTTPS, FTP, SFTP and TFTP.

For a more detailed description please refer to the detailed description of these parameter in the section 'File Operations' of this document.

INFO: Script files use UNIX-style line termination (LF). When editing and downloading scripts from a Windows environment, please use an editor program or tool to convert Windows-style (CR+LF) line termination to UNIX compatible.

Script execution via DHCP

A script file may also be transferred triggered by DHCP. The DHCP options 66/67 for Bootp may be used to inform the device of a certain host and filename. Upon initiating the DHCP function, this name is retrieved. Subsequently the file itself is automatically loaded. Upon success, the file is treated as an CLI script and an instance of the CLI will be run in background.

This script may for example contain commands to perform a configuration or even firmware download. Thus this is a very powerful tool used for rollout and maintenance.

2.2.8 List Handling with Indexes

So far only parameter have been shown that do not require an index. However, many parameters apply to a particular port or VLAN. The CLI simplifies operation here too.

An index is marked by square brackets such as in this example.

```
Protocol.VLAN.filter_config[1].alias = Any Name
```

When *auto_text_expansion* is enabled, the opening bracket is automatically displayed. This is also a hint that a value is expected. Now either type the desired index or hit [*CursorRight*], then [*CursorUp/Down*] to scroll through the available range.

Once the index is selected either way type ')' or ']' or [*Cursor Right*]. The index is completed and the next '.' (dot) is displayed. Now [*CursorUp/Down*] may be used to scroll through the following parameter.

A port range works similar to a normal index range with the exception, that a port is defined by its slot location and a port on this slot. For the installation switch or a desktop switch there is only one slot (1).

The slot becomes important when the Industrial Switch with extendable port modules is used. Here several slots with data ports exists. A typical port index looks like this: (Slot 1, Port 2)

```
Device.Port.config[1/2].speed = 1000_MBIT
```

It is possible to assign alias names to a port for convenience. When the cursor keys are used to navigate the indices, then the alias names are displayed where available.

```
# Define Alias
Device.Port.config[1/3].alias = My Name

# Alias displayed when using auto-complete function
>>Device.Port.config[1/3 ('My Name')].speed
[1/3].speed: 1000_MBIT
>>
```

The port alias name may also be used to address a port. Use double quotes to delimit the name. Blanks may appear and up to 32 characters for alias names are permitted.

```
>>Device.Port.config['My Name'].
alias : My Name
enable_port : Enabled
speed : 1000_MBIT
enable_full_duplex : Enabled
enable_auto_negotiation : Enabled
enable_flowcontrol : Enabled
enable_fefi : Disabled
```

```
enable_mdi : AUTO
>>
```

ATTENTION: All alias addressing is disabled in 'script_mode'. It is not possible to use alias addressing in scripts. Wildcards are available to view several ports at once.

Allowed options are:

- [1/*] - Display all ports on slot 1.
- [*/*] - Display all ports on all slots.

Depending on the section to display, the screen width may not be sufficient to display all elements. In such a case limit the display to only one parameter like [*/*].speed. If the list is too long, a break is displayed.

INFO: When script_mode is enabled, the screen does not stop after a full screen and content may roll off the screen. This is done so that capturing programs and scripts are easier to implement.

Adding/Removing new list entry

A new entry to a list parameter is generated by using the '*'-character (star) as index value. The following example adds a new filter entry for VLAN '101' into the VLAN filter table:

```
Protocol.VLAN.filter_config[*].vlan_id = 101
```

The field 'vlan_id' is the reference field for the index.

By leaving the reference field empty, the entry can be removed. The following example removes the VLAN filter entry for VLAN '101':

```
Protocol.VLAN.filter_config[101].vlan_id =
```

A security question is asked before the action is executed.

2.2.9 Offline Configuration

The device uses an XML file based configuration scheme. A device configuration consists of a collection of files grouped in a folder (directory).

The CLI, and other user interfaces, allow to copy, modify and transfer such configurations without affecting the running device.

Principle of Operation

Normal operation of the CLI affects the currently running and active configuration. Changes are immediately in effect.

Use *backup_to_folder* to create a user copy of the running configuration. This backed up configuration can be modified using the *OfflineConfiguration* command. This mode of operation is identified by a special prompt. Use the *OnlineConfiguration* command to return to normal live mode of operation.

Example:

```
MICROSENS>>Management.Files.configuration.backup_to_folder = MyConfig
NOTE: This will execute an action command with the following
function:
Copies running configuration to a new or existing folder. If the
folder name already exists the previous configuration is
overwritten. Syntax: backup_to_folder = my_new_config
Type y to continue, else to quit: y
executing..
Backup running configuration files to MyConfig.
ok
MICROSENS>>
MICROSENS>>OfflineConfiguration = MyConfig
You are now working on folder: MyConfig
Folder: MyConfig>>
...
Folder: MyConfig>>OnlineConfiguration
You are now working on the live configuration again.
MICROSENS>>
```

The *list*, *copy* and *delete* commands may be used as required. To activate a user configuration it must be made the running configuration. This is achieved using the *restore_from_folder* command.

The configuration is not simply replaced. Instead each individual parameter is evaluated to be valid (especially required when downloaded configurations are used). If the parameter value is changed compared to the currently running, the changes are executed and logged like every parameter change. This ensures that every change is noticed and can be traced back to the operator and time.

Please see the section 'File Operations' of this document for a more detailed description of all commands.

2.2.10 Advanced Features

Timeout

The CLI automatically logs off when unattended for a certain time. The default time out value is 5 minutes. This time can be changed and the time out may be turned off altogether. This is especially useful in lab situations.

```
Management.CLI.console_timeout = 0
```

The CLI uses the access right and views as defined in the *management.access* section of the parameter tree.

Logname

Any change here is immediately reflected and takes effect. To verify the currently active settings use the following command:

```
>>whoAmI
Your are logged in as admin with general access rights: Read / write
>>
```

Expert Mode

Before any action command that executes a function, the CLI displays a warning text and requires 'y' before execution. For experienced user this check may be disabled.

```
Management.CLI.dont_ask_questions = Enabled
```

Colors

The CLI uses colors for better readability. Help information are shown green, the prompt in yellow. Parameter values are magenta and action details may appear cyan. Errors are shown in red.

When colors are not desired or when a terminal does not support colors and strange characters appear, then colors may be turned off.

```
Management.CLI.colors = Disabled
```

Screen Size

The CLI adapts to the size of the terminal. When several columns are shown due to `[*]` wildcards, the individual fields are resized and trimmed automatically for best fit. The wider the terminal, the more data fit. When resizing the screen on the fly, simply press return on an empty line and the CLI will relearn the size.

Similarly, the line break for long lists adapts to the screen height.

2.3 CLI CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Management.						
			cli.			Command Line Interface (CLI) accessible via local terminal port, Telnet or SSH.
			enable_telnet	R/W		Enable TELNET for CLI access. Note: Disable TELNET and enable only SSH when only secure access is desired.
			enable_ssh	R/W		Enable SSH for CLI access. Note: When disabled also the SFTP file transfer server is disabled.
			prompt_source	R/W		Decides which prompt is shown.
			welcome_message	R/W		This welcome message is displayed prior to the login prompt. Use \n to enter a new line for multiline messages.
			user_prompt	R/W		User definable prompt string.
			colors	R/W		Color enhances readability but may not work with every terminal. Disable function when funny character appear.
			script_mode	R/W		When set the output will include the full command which permits to pipe the output into a script file.
			auto_text_expansion	R/W		When enabled typing characters will automatically be expanded on the command line for quicker access. This may conflict with batch file processing.
			dont_ask_questions	R/W		When enabled security questions are avoided for experienced operators.
			inactivity_timeout	R/W		An unattended CLI terminal logs off automatically after specified seconds. Use 0 to disable timeout.
			named_status_selection	R/W		When enabled dynamic status tables can comfortably be referenced by name. Otherwise a numerical index is used.
			live_help	R/W		When enabled a help text is automatically displayed while browsing through the CLI commands.
			script_tracing	R/W		This feature may be used to debug scripts and should otherwise be disabled. When enabled the program flow of a microScript or app is traced. To limit the trace to certain file(s) specify the file names in the script_filter parameter.

script_debugging	R/W	This feature may be used to debug scripts and should otherwise be disabled. When enabled possible debug messages are displayed. To limit the output to sections of interest, the debug output is filtered according to the file names specified under script_filter .
script_filter	R/W	When left blank, and debugging is enabled, all debug output is displayed. Enter a comma separated list of script file names to limit the debug output to these files.
favorites[16].		This table may be for a customized the favorites display. The commands are displayed in the entered order using the Favorites command.
command_line	R/W	Enter full command as it would be typed on the CLI console. This may also include calling scripts using RunScriptFile = file syntax.
last_instance	R	Number of times a CLI was started. Note: this value wraps at 255.
script_status.		Statistics about script file execution. Note that multiple CLI instances or command line invocations add up in the same statistics.
last_script_name	R	Name of last CLI script executed.
executed_files	R	Counts each time a CLI script is executed.
executed_commands	R	Counts each command executed within the current/last script file. The value is reset each time a script starts executing.
command_errors	R	Counts each executed command within the current/last script file that returned an error code. The value is reset each time a script starts executing.
compare_status.		Displays status results of the % operator to compare parameter or status to a set value.
last_dotstring	R	Copy of last dot_string tested.
matched	R	Displays True when the last comparision matched.
items_compared	R	Counts the number of items tested. May be more than 1 when wildcards are used.
items_different	R	Counts the number of items the were different. May be more than 0 when wildcards are used.
script_monitor[16].		Displays status results of the % operator to compare parameter or status to a set value.
state	R	Indicates if this record displays a currently running script or a history entry of a previously running script which has ended by now.
script_name	R	Name of the script

launched_by	R	Name of event or or other means of starting
cli_instance	R	Index identifying the executing cli instance
launch_time_stamp	R	Indicates the time when this record was created and the time this script was started.
run_time	R	Indicates how long the script has been executing. For history entries indicates the last run time taken.
current_file	R	Indicates the currently executed script file.
current_subroutine	R	Indicates the currently executed subroutine.
lines_executed	R	Counts how many script lines were executed.
current_line_number	R	This gives a snapshot of the currently executed line of code.
script_errors	R	In real time counts errors during script execution.
instances[256].		This table indicates how many CLI are currently running and for which operator and reason.
user_name	R	User that is logged in.
command_line	R	Displays optional command line parameter or script names that are executed by this CLI instance.
process_id	R	Indicates the process id for debugging purposes. 0 is no process.
launch_time_stamp	R	Indicates the time when this cli was started.

2.4 CLI Configuration Parameters

Group Path	General Parameters Management.CLI	
enable_telnet	Enable TELNET for CLI access. Note: Disable TELNET and enable only SSH when only secure access is desired.	
	Values	enabled, disabled
	OID	1.3.6.1.4.1.3181.10.6.3.62.1 (cliEnableTelnet)
enable_ssh	Enable SSH for CLI access. Note: When disabled also the SFTP file transfer server is disabled.	
	Values	enabled, disabled
	OID	1.3.6.1.4.1.3181.10.6.3.62.2 (cliEnableSsh)
prompt_source	Decides which prompt is shown.	
	Values	<div> <div><i>HOSTNAME</i></div> <div>The device hostname is used as prompt</div> </div> <div> <div><i>DEVICE_LOCATION</i></div> <div>The user specified device location is used as prompt</div> </div> <div> <div><i>USER_NAME</i></div> <div>The login name of the user is used as prompt</div> </div> <div> <div><i>USER_DEFINED</i></div> <div>A user defined string as defined in 'user_prompt' is used as prompt</div> </div>
	OID	1.3.6.1.4.1.3181.10.6.3.62.3 (cliPromptSource)
welcome_message	This welcome message is displayed prior to the login prompt. Use \n to enter a new line for multiline messages.	
	Value	String, max. 512 characters.
	OID	1.3.6.1.4.1.3181.10.6.3.62.4 (cliWelcomeMessage)
user_prompt	User definable prompt string.	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.3.62.5 (cliUserPrompt)
colors	Color enhances readability but may not work with every terminal. Disable function when funny character appear.	
	Values	enabled, disabled
	OID	1.3.6.1.4.1.3181.10.6.3.62.6 (cliColors)
script_mode	When set the output will include the full command which permits to pipe the output into a script file.	
	Values	enabled, disabled
	OID	1.3.6.1.4.1.3181.10.6.3.62.7 (cliScriptMode)

auto_text_expansion	<p>When enabled typing characters will automatically be expanded on the command line for quicker access. This may conflict with batch file processing.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.62.8 (cliAutoTextExpansion)</p>
dont_ask_questions	<p>When enabled security questions are avoided for experienced operators.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.62.9 (cliDontAskQuestions)</p>
inactivity_timeout	<p>An unattended CLI terminal logs off automatically after specified seconds. Use 0 to disable timeout.</p> <p>Value Number in range 0-10000</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.62.10 (cliInactivityTimeout)</p>
named_status_selection	<p>When enabled dynamic status tables can comfortably be referenced by name. Otherwise a numerical index is used.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.62.11 (cliNamedStatusSelection)</p>
live_help	<p>When enabled a help text is automatically displayed while browsing through the CLI commands.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.62.12 (cliLiveHelp)</p>
script_tracing	<p>This feature may be used to debug scripts and should otherwise be disabled. When enabled the program flow of a microScript or app is traced. To limit the trace to certain file(s) specify the file names in the script_filter parameter.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.62.13 (cliScriptTracing)</p>
script_debugging	<p>This feature may be used to debug scripts and should otherwise be disabled. When enabled possible debug messages are displayed. To limit the output to sections of interest, the debug output is filtered according to the file names specified under script_filter.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.62.14 (cliScriptDebugging)</p>
script_filter	<p>When left blank, and debugging is enabled, all debug output is displayed. Enter a comma separated list of script file names to limit the debug output to these files.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.62.15 (cliScriptFilter)</p>

2.5 CLI Status Parameters

Group Path	General Parameters Management.CLI
last_instance	<p>Number of times a CLI was started. Note: this value wraps at 255.</p> <p>Value Number in range 0-255</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.62.100 (cliLastInstance)</p>
<hr/>	
Group Path Description	script_status Management.CLI.script_status Statistics about script file execution. Note that multiple CLI instances or command line invocations add up in the same statistics.
last_script_name	<p>Name of last CLI script executed.</p> <p>Value String, max. 256 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.62.101.1.2 (scriptStatusLastScriptName)</p>
executed_files	<p>Counts each time a CLI script is executed.</p> <p>Value Number in range 0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.62.101.1.3 (scriptStatusExecutedFiles)</p>
executed_commands	<p>Counts each command executed within the current/last script file. The value is reset each time a script starts executing.</p> <p>Value Number in range 0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.62.101.1.4 (scriptStatusExecutedCommands)</p>
command_errors	<p>Counts each executed command within the current/last script file that returned an error code. The value is reset each time a script starts executing.</p> <p>Value Number in range 0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.62.101.1.5 (scriptStatusCommandErrors)</p>

Group	compare_status
Path	Management.CLI.compare_status
Description	Displays status results of the % operator to compare parameter or status to a set value.
last_dotstring	Copy of last dot_string tested. Value String, max. 256 characters. OID 1.3.6.1.4.1.3181.10.6.3.62.102.1.2 (compareStatusLastDotstring)
matched	Displays True when the last comparision matched. Values true, false OID 1.3.6.1.4.1.3181.10.6.3.62.102.1.3 (compareStatusMatched)
items_compared	Counts the number of items tested. May be more than 1 when wildcards are used. Value Number in range 0-0xFFFFFFFF OID 1.3.6.1.4.1.3181.10.6.3.62.102.1.4 (compareStatusItemsCompared)
items_different	Counts the number of items the were different. May be more than 0 when wildcards are used. Value Number in range 0-0xFFFFFFFF OID 1.3.6.1.4.1.3181.10.6.3.62.102.1.5 (compareStatusItemsDifferent)

3 System Access

3.1 Key Features

Unlimited number of Users

Three default users are created and any number of additional users may be created.

Default settings permit simple security setup. However, when desired advanced and precise access control down to parameter level can be achieved.

View Based Access Model

Access right can be precisely tailored for each user. Similar to SNMP V3 view model but applied to all user interfaces including CLI.

Default settings permit simple security setup. However, when desired advanced and precise access control down to parameter level can be achieved.

General access rights

For quick and effective rights management the general read/write privileges of a user can be selected.

Disable Insecure Interfaces

It is possible to restrict management access to secure interfaces such as HTTPS, SSH, SNMP V3
Enforce secure access policies

Interface Restrictions

For each user the permitted user interfaces can be selected.
Fine granulation of access rights

Public key encrypted passwords

For each user an access password plus an SNMP V3 password is assigned. Proper AES256 public key encrypted passwords are stored.

Secure and robust access control.

View Model for SNMP V1,V2c

The access view model may be applied to SNMP V1 or V2c access, practically creating SNMP V3 like access protection.

SNMP V3 like access protection without the complication associated with SNMP V3.

Firewall with Black and White List

Setup a dynamic list of IP addresses that may or may not gain access to the management interface. Blacklist is combined with firewall function.

Layer 3 security

TACACS+ Authentication

Users can be authenticated using central TACACS+ server. The supplied privilege levels can be mapped to any local security level.

Centralized access control. Especially useful in Cisco environment.

RADIUS access verification

Users that wish to gain system access may be authenticated via a RADIUS server instead of the locally stored names. Fallback to local is possible.

Centralized access control.

3.2 Functional Description

3.2.1 User Access

Users with individual access rights to the system information can be defined. Access rights can be fine tuned by defining user groups and views.

Adding, editing and removing of users, groups and views can be done as described in 'Command Line Interface (CLI)' section of this document.

3.2.2 Interface Selection

Each management interface can be enabled or disabled depending on the security policies required. By disabling an interface, access via the corresponding protocol is completely blocked.

3.3 Access CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Management.						
			access.			Local access control for user login authentication and element access limitation
			authentication_mode		R/W	This parameter defines against which database incoming user and password are verified.
			user[DYNAMIC].			
			name		R/W	Unique name used to login to the system regardless of the management interface used. At least 3 character are required.
			associated_groups		R/W	A user must be part of a group and inherits the rights of the groups and their views.
			general_access_rights		R/W	Limited access rights here overrule rights granted by the associated groups and their views. Use NO_ACCESS to temporarily suspend a user account.
			enable_telnet_access		R/W	Permit CLI user access via insecure telnet session or via local serial port.
			enable_ssh_access		R/W	Permit CLI user access via secure shell.
			enable_web_access		R/W	Permit user access via the web interface.
			enable_snmp_access		R/W	Permit user access via SNMP of any version. Additionally use SNMP settings to restrict to only secure SNMP v3 if desired.
			enable_nmp_access		R/W	Permit user access via the nmp network management application.
			enable_ftp_access		R/W	Permit ftp access for file transfers.

enter_password	X	Set a new authentication password which replaces the previous one. This password applies to all user access methods except SNMP. For SNMP v3 a separate set of passwords is used. Note: trailing spaces or multiple spaces in the password are automatically removed. Important when a software downgrade to a version prior 10.7.0 is intended, re-enter the admin password followed by the words: md5 before the downgrade. This stores the password compatible with older releases.
encrypted_auth_password	R/W	
snmp_v3_security_level	R/W	Defines if login authorization and/or privacy are used.
snmp_v3_auth_algorithm	R/W	Defines with which algorithm the authorization key is created and decoded.
snmp_v3_privacy_algorithm	R/W	Defines which encryption method is used security level includes privacy.
enter_snmp_v3_auth_password	X	Set a new SNMP v3 authentication password. This parameter only is required when SNMP v3 is used. This value correlates to the authorization key. No spaces are permitted and at least 8 character are required.
encrypted_snmp_auth_password	R/W	
enter_snmp_v3_privacy_password	X	Set a new encryption password. This parameter only is required when SNMP v3 user based privacy is used. If left empty, the SNMP v3 authentication password is also used for SNMP v3 privacy. No spaces are permitted and at least 8 character are required. IMPORTANT: This password must be different to the authentication password !
encrypted_snmp_privacy_password	R/W	
group[DYNAMIC].		

name	R/W	Enter a unique and descriptive name that identifies the group. At least 3 character are required.
associated_views	R/W	A list which may point to one or several views that make up this group.
view[DYNAMIC].		
name	R/W	Enter a unique and descriptive name that identifies the view. At least 3 character are required.
associated_pattern	R/W	A list which may point to one or several pattern that make up this view.
pattern[DYNAMIC].		
name	R/W	Enter a unique and descriptive name that identifies the pattern. At least 3 character are required.
dotstring	R/W	A dotstring or partial dotstring can be defined here. Note that the first keyword (device, protocol, Management,App) must not be included. Example: port (for device.port) or port.config.alias
access_rights	R/W	This defines in which way the dotstring is to be treated.
radius.		
primary_auth_server_name	R/W	Symbolic name of the RADIUS server used for authentication.
fallback_auth_server_name	R/W	Symbolic name of the RADIUS server used for authentication if the primary server is down. Leave empty when no fallback is required.
tacacs.		
primary_auth_server_name	R/W	Symbolic name of the TACACS+ server used for authentication.
fallback_auth_server_name	R/W	Symbolic name of the TACACS+ server used for authentication if the primary server is down. Leave empty when no fallback is required.

privilege_level_0_user	R/W	This maps TACACS+ privilege levels to internal access model. Level 0 is lowest privilege level. Make sure the name entered here exists as local user name.
privilege_level_1_user	R/W	This maps TACACS+ privilege levels to internal access model. Level 1 is a basic privilege level. Make sure the name entered here exists as local user name.
privilege_level_15_user	R/W	This maps TACACS+ privilege levels to internal access model. Level 15 is highest privilege level and would usually be mapped to the admin user.
restrictions[DYNAMIC].		This table may be used to restrict access to the management system. Be careful not to lock your self out.
name	R/W	Enter a unique and descriptive name that identifies the ip_address. At least 3 character are required.
mode	R/W	The associated IP address may be permitted or denied. Use UNUSED to temporarily suspend an entry.
ip_address	R/W	Enter an IP address or address range which is denied or permitted. For example, to describe a range of IP addresses from 192.168.0.1 to 192.168.255.255 you use: 192.168.0.0/16. Where 16 describes the number of bits in the IP address that are used for comparison (here 192.168).
number_of_logins	R	This value is incremented for each successful login.
login_status[32].		This table displays data which are read from the inserted SFPs.
state	R	Indicates if this login record displays a currently active login or a history entry of a previous login which is logged off by now.
user_name	R	User name for which this record applies.

auth_name	R	Authorization name which maps to the local user names to define the actual access rights. For local authentication this value mirrors the user name. When RADIUS authentication is used, this reflects the name provided by the RADIUS server.
login_id	R	Unique value to reference this login operation
login_time_stamp	R	Indicated the time when this user has connected to this service.
login_epoch	R	Login time stamp in Linux time since the epoch format.
connect_time	R	Indicates since how long the connection is established. For logged off entries this indicates the last connect time of this entry.
service	R	Displays which service was used to perform the login.
remote_host	R	Displays from which remote host the login was performed. Details depend on the chosen interface.

3.4 Access Configuration Parameters

Group Path	General Parameters Management.Access	
authentication_mode	This parameter defines against which database incoming user and password are verified.	
	Values	<p><i>LOCAL</i> Verify against local database</p> <p><i>LOCAL_THEN_RADIUS</i> Verify against local database then try RADIUS server if user is not locally defined</p> <p><i>RADIUS</i> Verify against RADIUS server</p> <p><i>LOCAL_THEN_TACACS</i> Verify against local database then try TACACS+ server if user is not locally defined</p> <p><i>TACACS</i> Verify against TACACS+ server</p> <p><i>RADIUS_THEN_LOCAL</i> Verify against RADIUS server then try local database</p> <p><i>TACACS_THEN_LOCAL</i> Verify against TACACS+ server then try local database</p>
	OID	1.3.6.1.4.1.3181.10.6.3.76.1 (accessAuthenticationMode)
Group Path	Description	user , dynamical size Management.Access.user
name	Unique name used to login to the system regardless of the management interface used. At least 3 character are required.	<p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.2.1.2 (userName)</p>
associated_groups	A user must be part of a group and inherits the rights of the groups and their views.	<p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.2.1.3 (userAssociatedGroups)</p>

general_access_rights	<p>Limited access rights here overrule rights granted by the associated groups and their views. Use NO_ACCESS to temporarily suspend a user account.</p> <p>Values <i>NO_ACCESS</i> Neither read nor write of any parameter is permitted <i>READ_ONLY</i> This group may only read parameter <i>READ_WRITE</i> This group can read and write parameter</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.2.1.4 (userGeneralAccessRights)</p>
enable_telnet_access	<p>Permit CLI user access via insecure telnet session or via local serial port.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.2.1.5 (userEnableTelnetAccess)</p>
enable_ssh_access	<p>Permit CLI user access via secure shell.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.2.1.6 (userEnableSshAccess)</p>
enable_web_access	<p>Permit user access via the web interface.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.2.1.7 (userEnableWebAccess)</p>
enable_snmp_access	<p>Permit user access via SNMP of any version. Additionally use SNMP settings to restrict to only secure SNMP v3 if desired.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.2.1.8 (userEnableSnmpAccess)</p>
enable_nmp_access	<p>Permit user access via the nmp network management application.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.2.1.9 (userEnableNmpAccess)</p>
enable_ftp_access	<p>Permit ftp access for file transfers.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.2.1.10 (userEnableFtpAccess)</p>

enter_password	<p>Set a new authentication password which replaces the previous one. This password applies to all user access methods except SNMP. For SNMP v3 a separate set of passwords is used. Note: trailing spaces or multiple spaces in the password are automatically removed. Important when a software downgrade to a version prior 10.7.0 is intended, re-enter the admin password followed by the words: md5 before the downgrade. This stores the password compatible with older releases.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.2.1.11 (userEnterPassword)</p>						
encrypted_auth_password	<p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.2.1.12 (userEncryptedAuthPassword)</p>						
snmp_v3_security_level	<p>Defines if login authorization and/or privacy are used.</p> <p>Values</p> <table data-bbox="845 907 1420 1153"> <tr> <td><i>NO_AUTH_NO_PRIV</i></td><td>Open access. No authentication, no privacy.</td></tr> <tr> <td><i>AUTH_NO_PRIV</i></td><td>Use authentication to login but no encryption of the managed data.</td></tr> <tr> <td><i>AUTH_PRIV</i></td><td>Use authentication to login as well as encryption of the managed data.</td></tr> </table> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.2.1.13 (userSnmpV3SecurityLevel)</p>	<i>NO_AUTH_NO_PRIV</i>	Open access. No authentication, no privacy.	<i>AUTH_NO_PRIV</i>	Use authentication to login but no encryption of the managed data.	<i>AUTH_PRIV</i>	Use authentication to login as well as encryption of the managed data.
<i>NO_AUTH_NO_PRIV</i>	Open access. No authentication, no privacy.						
<i>AUTH_NO_PRIV</i>	Use authentication to login but no encryption of the managed data.						
<i>AUTH_PRIV</i>	Use authentication to login as well as encryption of the managed data.						
snmp_v3_auth_algorithm	<p>Defines with which algorithm the authorization key is created and decoded.</p> <p>Values</p> <table data-bbox="845 1332 1404 1444"> <tr> <td><i>NO_AUTHENTICATION</i></td><td>No authentication is used.</td></tr> <tr> <td><i>MD5</i></td><td>MD-5 algorithm is used.</td></tr> <tr> <td><i>SHA</i></td><td>SHA-1 algorithm is used.</td></tr> </table> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.2.1.14 (userSnmpV3AuthAlgorithm)</p>	<i>NO_AUTHENTICATION</i>	No authentication is used.	<i>MD5</i>	MD-5 algorithm is used.	<i>SHA</i>	SHA-1 algorithm is used.
<i>NO_AUTHENTICATION</i>	No authentication is used.						
<i>MD5</i>	MD-5 algorithm is used.						
<i>SHA</i>	SHA-1 algorithm is used.						

snmp_v3_privacy_algorithm	Defines which encryption method is used security level includes privacy.
Values	<div> <div><i>NO_PRIVACY</i></div> <div>No encryption for privacy is used.</div> </div> <div> <div><i>DES</i></div> <div>CBC_DES is used to encrypt the payload.</div> </div> <div> <div><i>AES</i></div> <div>AES-128 encryption is used to encrypt the payload</div> </div> <div> <div><i>AES_192</i></div> <div>AES-192 bit encryption is used to encrypt the payload</div> </div> <div> <div><i>AES_256</i></div> <div>AES-256 bit encryption is used to encrypt the payload</div> </div>
OID	1.3.6.1.4.1.3181.10.6.3.76.2.1.15 (userSnmpV3PrivacyAlgorithm)
enter_snmp_v3_auth_password	<p>Set a new SNMP v3 authentication password. This parameter only is required when SNMP v3 is used. This value correlates to the authorization key. No spaces are permitted and at least 8 character are required.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.2.1.16 (userEnterSnmpV3AuthPassword)</p>
encrypted_snmp_auth_password	<p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.2.1.17 (userEncryptedSnmpAuthPassword)</p>
enter_snmp_v3_privacy_password	<p>Set a new encryption password. This parameter only is required when SNMP v3 user based privacy is used. If left empty, the SNMP v3 authentication password is also used for SNMP v3 privacy. No spaces are permitted and at least 8 character are required. IMPORTANT: This password must be different to the authentication password !</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.2.1.18 (userEnterSnmpV3PrivacyPassword)</p>
encrypted_snmp_privacy_password	<p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.2.1.19 (userEncryptedSnmpPrivacyPassword)</p>

Group Path Description	group , dynamical size Management.Access.group
name	Enter a unique and descriptive name that identifies the group. At least 3 character are required. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.3.76.3.1.2 (groupName)
associated_views	A list which may point to one or several views that make up this group. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.3.76.3.1.3 (groupAssociatedViews)
Group Path Description	view , dynamical size Management.Access.view
name	Enter a unique and descriptive name that identifies the view. At least 3 character are required. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.3.76.4.1.2 (viewName)
associated_pattern	A list which may point to one or several pattern that make up this view. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.3.76.4.1.3 (viewAssociatedPattern)
Group Path Description	pattern , dynamical size Management.Access.pattern
name	Enter a unique and descriptive name that identifies the pattern. At least 3 character are required. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.3.76.5.1.2 (patternName)

dotstring	<p>A dotstring or partial dotstring can be defined here. Note that the first keyword (device, protocol, Management,App) must not be included. Example: port (for device.port) or port.config.alias</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.5.1.3 (patternDotstring)</p>
access_rights	<p>This defines in which way the dotstring is to be treated.</p> <p>Values</p> <p><i>NO_ACCESS</i> Do not permit any access. (Not even read)</p> <p><i>READ_ONLY</i> View of associated dotstring is enabled</p> <p><i>READ_WRITE</i> View of associated dotstring is disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.5.1.4 (patternAccessRights)</p>
Group	restrictions , dynamical size
Path	Management.Access.restrictions
Description	This table may be used to restrict access to the management system. Be careful not to lock your self out.
name	<p>Enter a unique and descriptive name that identifies the ip_address. At least 3 character are required.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.8.1.2 (restrictionsName)</p>
mode	<p>The associated IP address may be permitted or denied. Use UNUSED to temporarily suspend an entry.</p> <p>Values</p> <p><i>UNUSED</i> Entry is suspended</p> <p><i>PERMIT</i> Associated IP address is permitted</p> <p><i>DENY</i> Associated IP address is not accepted.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.8.1.3 (restrictionsMode)</p>
ip_address	<p>Enter an IP address or address range which is denied or permitted. For example, to describe a range of IP addresses from 192.168.0.1 to 192.168.255.255 you use: 192.168.0.0/16. Where 16 describes the number of bits in the IP address that are used for comparison (here 192.168).</p> <p>Value String, max. 64 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.76.8.1.4 (restrictionsIpAddress)</p>

Group	radius
Path	Management.Access.radius
Description	

primary_auth_server_name	Symbolic name of the RADIUS server used for authentication.
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.3.76.6.1.2 (radiusPrimaryAuthServerName)

fallback_auth_server_name	Symbolic name of the RADIUS server used for authentication if the primary server is down. Leave empty when no fallback is required.
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.3.76.6.1.3 (radiusFallbackAuthServerName)

Group	tacacs
Path	Management.Access.tacacs
Description	

primary_auth_server_name	Symbolic name of the TACACS+ server used for authentication.
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.3.76.7.1.2 (tacacsPrimaryAuthServerName)

fallback_auth_server_name	Symbolic name of the TACACS+ server used for authentication if the primary server is down. Leave empty when no fallback is required.
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.3.76.7.1.3 (tacacsFallbackAuthServerName)

privilege_level_0_user	This maps TACACS+ privilege levels to internal access model. Level 0 is lowest privilege level. Make sure the name entered here exists as local user name.
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.3.76.7.1.4 (tacacsPrivilegeLevel0User)

privilege_level_1_user	This maps TACACS+ privilege levels to internal access model. Level 1 is a basic privilege level. Make sure the name entered here exists as local user name.
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.3.76.7.1.5 (tacacsPrivilegeLevel1User)

privilege_level_15_user	This maps TACACS+ privilege levels to internal access model. Level 15 is highest privilege level and would usually be mapped to the admin user.
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.3.76.7.1.6 (tacacsPrivilegeLevel15User)

3.5 Access Status Parameters

Group Path	General Parameters Management.Access	
number_of_logins	This value is incremented for each successful login.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.3.76.100 (accessNumberOfLogins)

4 Access Control List (ACL)

4.1 Key Features

Access Control Lists (ACL)

ACL permit comprehensive wire-speed filtering of incoming data. This advanced feature may be used to block malicious or unwanted data from entering the network.

Properly defined ACLs greatly increase network security by blocking undesired traffic.

Dynamic ACL via RADIUS

Dynamic ACL ease deployment of ACL settings by centralizing their setup. The ACL settings are received during 802.1X port authentication and are automatically applied.

Simplifies ACL configuration in larger deployments.

4.2 Functional Description

Access Control Lists (ACL) are used to limit access to the network by filtering at frame layer. Rules are the heart of the logic. Rules may be defined to specify certain IP address ranges, a certain MAC, a certain VLAN or special protocol that is to be filtered out of the data stream to be treated specially.

Usually, a number of rules are needed to perform a certain function and thus several rules can be specified as a single list entry. A list in turn can contain many such entries. The `active_filter_port_config` table contains a pointer to name of acl list entries. The port filter are capable of filtering the data traffic entering a port in real time, with no additional latency being introduced. This works much like a firewall, albeit at frame level.

In addition to the port filter, there are other tables that reference the ACL list. The security feature ARP inspection, for example, points to ACL lists elements for manually declared IP/MAC relations. Note that this application only uses a subset of the options available for a rules definition. Another reference to ACL tables is made from the WIFI section, whereby the ACL list is used to define the firewall rules that protect from malicious data entering the wireless network.

The setup of rules, grouped in list entries and lists elements being referenced from yet other tables can become complex to setup. Therefore, it is highly recommended to make use of the various description fields to comment the use and function of each entry. Also note that rules are evaluated in the order of appearance in the configuration. Thus place more specific entries first, and less precise entries last. In all tables where ACLs are used there is also a default logic parameter that defines what happens if none of the ACL rules has matched.

In this way it is generally possible to provide a blocking list, where everything is permitted except the matched frames or an acceptance list, where everything is blocked except for specifically matched frames. Which behavior is more suitable depends on the desired result and the type of input data to match.

4.2.1 Important notes with regard to ACL use

Note 1

Be sure to thoroughly test ACLs in a test bed before going online. As soon as the first permit rule is applied, it implies that all other devices, not part of the permission, are blocked. This even includes the local switch itself. Also with a deny rule it easy to lock yourself out unintentionally.

Note 2

It is strongly recommended to add a permit-rule that covers ARP (address resolution protocol) in order to ensure address resolution can operate correctly. Failure to do so may result in the attached device to not even be able to send out ping.

Note 3

ACL are designed to operate with IPv4 addresses. (Ether type = 0x0800, e.g. TCP or UDP via IPv4). ARP is not supported automatically and need to be permitted separately. A possible solution is the following additional rule (the source MAC may be defined optionally):

```
Management.ACL.rules[permit_arp_pc1].name = permit_arp_pc1
Management.ACL.rules[permit_arp_pc1].description = Permit all ARP from PC1
Management.ACL.rules[permit_arp_pc1].mode = PERMIT
Management.ACL.rules[permit_arp_pc1].ether_type = 2054
Management.ACL.rules[permit_arp_pc1].protocol =
Management.ACL.rules[permit_arp_pc1].vlan_id =
Management.ACL.rules[permit_arp_pc1].source_mac = 00:11:22:33:44:55
Management.ACL.rules[permit_arp_pc1].source_ip =
Management.ACL.rules[permit_arp_pc1].source_mask =
Management.ACL.rules[permit_arp_pc1].source_port =
Management.ACL.rules[permit_arp_pc1].destination_mac =
Management.ACL.rules[permit_arp_pc1].destination_ip =
Management.ACL.rules[permit_arp_pc1].destination_mask =
Management.ACL.rules[permit_arp_pc1].destination_port =
```

4.3 ACL CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Management.						
	acl.					Access Control Lists
			enable_acl_filtering	R/W		General enable of access control list operation. Note that this function need only be enabled when port filtering is used. For WIFI, DHCP or ARP inspection function this enable parameter is meaningless..
		active_filter_port_config[PORT].				This table defines the parameter for access control of incoming data.
			enable_acl_filtering	R/W		Generally enables access control checking for this particular port. The details need to be configured in the list and rules tables. Tip: Be sure to include a permit-rule for ARP when creating the tables. Also include the switch itself in the rules.
			acl_list_name	R/W		Name of the ACL (access control list) which apply to this port. Several ACL lists may be specified with a comma separated list. Example acl1, otherlist
		list[DYNAMIC].				This table is used to combine and group individual rules for easier reference.
			name	R/W		Unique name to reference this entry and to remember whose MAC address is entered.
			description	R/W		Enter any information required to remember what this rule is intended to do.
			rules	R/W		Contains the names of rules that apply to this list separated by commas. Please beware of typing errors. Example: rule1,rule2,other_rule
		rules[DYNAMIC].				For filtering of incoming data this table defines the filter rules. The same table also applies to ARP inspection. In this use this table statically defines valid MAC/IP/VLAN relationships. Tip: Be sure to include a permit-rule for ARP when creating ACL tables. Also include the switch itself in these rules.
			name	R/W		Unique name to reference this entry and to remember whose MAC address is entered.

description	R/W	Enter any information required to remember what this rule is intended to do.
mode	R/W	Use UNUSED to temporarily suspend an entry. Use ACCEPT when the matched entry should be treated as valid. Use DENY when a matched entry should be treated as invalid match.
ether_type	R/W	Use 2048 to match IPv4 (0x800), 34525 to match IPv6 (0x86DD). A value of 0 ignores this field. The field is also ignored for ARP inspection rules.
protocol	R/W	Use 6 to specify TCP, 17 for UDP, etc. Use to ignore the protocol field. This field is also ignored for ARP inspection rules.
vlan_id	R/W	VLAN ID for which this entry is valid. A value of 0 ignores this field.
source_mac	R/W	MAC address entry.
source_ip	R/W	IP address associated with the given MAC.
source_mask	R/W	The mask may be used to create a valid address range.
source_port	R/W	May be used to specify a specific udp/tcp port. A value of 0 ignores this field. The field is also ignored for ARP inspection rules.
destination_mac	R/W	MAC address entry. This field is ignored for ARP inspection rules.
destination_ip	R/W	IP address associated with the given MAC. This field is ignored for ARP inspection rules.
destination_mask	R/W	The mask may be used to create a valid address range. This field is ignored for ARP inspection rules.
destination_port	R/W	May be used to specify a specific udp/tcp port. A value of 0 ignores this field. The field is also ignored for ARP inspection rules.

4.4 ACL Configuration Parameters

Group	General Parameters
Path	Management.ACL
enable_acl_filtering	<p>General enable of access control list operation. Note that this function need only be enabled when port filtering is used. For WIFI, DHCP or ARP inspection function this enable parameter is meaningless..</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.51.1 (aclEnableAclFiltering)</p>
Group	active_filter_port_config, for all ports[0..31]
Path	Management.ACL.active_filter_port_config[port]
Description	This table defines the parameter for access control of incoming data.
enable_acl_filtering	<p>Generally enables access control checking for this particular port. The details need to be configured in the list and rules tables. Tip: Be sure to include a permit-rule for ARP when creating the tables. Also include the switch itself in the rules.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.51.2.1.2 (activeFilterPortConfigEnableAclFiltering)</p>
acl_list_name	<p>Name of the ACL (access control list) which apply to this port. Several ACL lists may be specified with a comma separated list. Example acl1, otherlist</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.51.2.1.3 (activeFilterPortConfigAclListName)</p>
Group	list, dynamical size
Path	Management.ACL.list
Description	This table is used to combine and group individual rules for easier reference.
name	<p>Unique name to reference this entry and to remember whose MAC address is entered.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.51.3.1.2 (listName)</p>

description	<p>Enter any information required to remember what this rule is intended to do.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.51.3.1.3 (listDescription)</p>
rules	<p>Contains the names of rules that apply to this list separated by commas. Please beware of typing errors. Example: rule1,rule2,other_rule</p> <p>Value String, max. 512 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.51.3.1.4 (listRules)</p>
Group Path Description	<p>rules, dynamical size</p> <p>Management.ACL.rules</p> <p>For filtering of incoming data this table defines the filter rules. The same table also applies to ARP inspection. In this use this table statically defines valid MAC/IP/VLAN relationships. Tip: Be sure to include a permit-rule for ARP when creating ACL tables. Also include the switch itself in these rules.</p>
name	<p>Unique name to reference this entry and to remember whose MAC address is entered.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.51.4.1.2 (rulesName)</p>
description	<p>Enter any information required to remember what this rule is intended to do.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.51.4.1.3 (rulesDescription)</p>
mode	<p>Use UNUSED to temporarily suspend an entry. Use ACCEPT when the matched entry should be treated as valid. Use DENY when a matched entry should be treated as invalid match.</p> <p>Values</p> <ul style="list-style-type: none"> <i>UNUSED</i> Entry is suspended <i>PERMIT</i> Associated IP address is permitted <i>DENY</i> Associated IP address is not accepted. <p>OID 1.3.6.1.4.1.3181.10.6.3.51.4.1.4 (rulesMode)</p>
ether_type	<p>Use 2048 to match IPv4 (0x800), 34525 to match IPv6 (0x86DD). A value of 0 ignores this field. The field is also ignored for ARP inspection rules.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.51.4.1.5 (rulesEtherType)</p>
protocol	<p>Use 6 to specify TCP, 17 for UDP, etc. Use to ignore the protocol field. This field is also ignored for ARP inspection rules.</p> <p>Value Number in range 0-255</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.51.4.1.6 (rulesProtocol)</p>

vlan_id	VLAN ID for which this entry is valid. A value of 0 ignores this field.	
	Value	Number in range 0-4095
	OID	1.3.6.1.4.1.3181.10.6.3.51.4.1.7 (rulesVlanId)
source_mac	MAC address entry.	
	Format	MAC Address <i>hh-hh-hh-hh-hh-hh</i> (<i>hh</i> = hexadecimal number between 00 to ff)
	OID	1.3.6.1.4.1.3181.10.6.3.51.4.1.8 (rulesSourceMac)
source_ip	IP address associated with the given MAC.	
	Format	IPv4 Address <i>ddd.ddd.ddd.ddd</i> (<i>ddd</i> = decimal number between 000 to 255)
	OID	1.3.6.1.4.1.3181.10.6.3.51.4.1.9 (rulesSourceIp)
source_mask	The mask may be used to create a valid address range.	
	Format	IPv4 Address <i>ddd.ddd.ddd.ddd</i> (<i>ddd</i> = decimal number between 000 to 255)
	OID	1.3.6.1.4.1.3181.10.6.3.51.4.1.10 (rulesSourceMask)
source_port	May be used to specify a specific udp/tcp port. A value of 0 ignores this field. The field is also ignored for ARP inspection rules.	
	Value	Number in range 0-65535
	OID	1.3.6.1.4.1.3181.10.6.3.51.4.1.11 (rulesSourcePort)
destination_mac	MAC address entry. This field is ignored for ARP inspection rules.	
	Format	MAC Address <i>hh-hh-hh-hh-hh-hh</i> (<i>hh</i> = hexadecimal number between 00 to ff)
	OID	1.3.6.1.4.1.3181.10.6.3.51.4.1.12 (rulesDestinationMac)
destination_ip	IP address associated with the given MAC. This field is ignored for ARP inspection rules.	
	Format	IPv4 Address <i>ddd.ddd.ddd.ddd</i> (<i>ddd</i> = decimal number between 000 to 255)
	OID	1.3.6.1.4.1.3181.10.6.3.51.4.1.13 (rulesDestinationIp)
destination_mask	The mask may be used to create a valid address range. This field is ignored for ARP inspection rules.	
	Format	IPv4 Address <i>ddd.ddd.ddd.ddd</i> (<i>ddd</i> = decimal number between 000 to 255)
	OID	1.3.6.1.4.1.3181.10.6.3.51.4.1.14 (rulesDestinationMask)

destination_port	May be used to specify a specific udp/tcp port. A value of 0 ignores this field. The field is also ignored for ARP inspection rules.
Value	Number in range 0-65535
OID	1.3.6.1.4.1.3181.10.6.3.51.4.1.15 (rulesDestinationPort)

5 Web Manager

5.1 Key Features

Base Features

Integrated Web Manager with graphical user interface (GUI) for device configuration and administration using a standard web browser. The web interface may be used to configure all aspects of the device in a convenient manner.

Web Authentication

In order to access the web interface a login/password sequence as globally defined for the device in the access section is required.

Same access protection and credentials regardless if selected user interface type enforces uniform security.

RADIUS access verification

Users that wish to gain system access may be authenticated via a RADIUS server instead of the locally stored names. Fallback to local is possible.

Centralized access control.

HTTPS

HTTPS offers secure encrypted data transport. Alternative standard HTTP is also supported. When HTTPS is configured unsecure HTTP traffic is automatically blocked. Since 10.7.7 only TLS 1.2 is supported. For older TLS versions a new parameter setting (LESS_SECURE) was added.

Enforce secure web access with high security level. In HTTPS setting only TLS1.2 encryption is accepted.

Less Secure HTTPS

Since 10.7.7 the less secure standards TLS1.0 and TLS1.1 as well as SSLv2 and SSLv3 are no longer supported when HTTPS is selected. The less secure setting for HTTPS makes these older standards available if required.

Permit use with older equipment that does not support current TLS1.2 standard. In default setting this feature is disabled and thus use of more secure TLS1.2 is automatically enforced.

Custom SSL Certificates

Custom SSL certificate for secure web access can be uploaded and downloaded via file transfer. Also chain files are supported.

Enables operator to use private certificates that adhere to a given company policy.

Full Functional Support

All features of the device, including actions functions, are accessible from the web interface.

No need to open a parallel Telnet session for ping tests or similar special functions

Animated Device Graphics

When a device is selected all LED and connectors are shown as located on the device. Colored borders indicate the individual status. LEDs are showing identical to the real device.

Graphic help to locate the connectors. Visual display illustrates overall status at one glance.

Firmware Update

Since all functions of the device are available, also firmware update is easily possible.

All management can be done from the web interface.

Online Documentation

The product offers a detailed and automatically updated handbook. This handbook is readily available from the web interface.

Up-to-date documentation readily accessible.

SNMP MIB download

All MICROSENS specific SNMP MIB files can be downloaded from the web interface. The MIB files are required when G6 specific functions shall be accessible via SNMP interface.

Up-to-date online MIBs help operator to select and find the proper MIBs.

Event Display

the 20 latest events (traps) are visible in the web interface for immediate detection of special conditions. An individual log filter may be set.

Previously, event where only visible in the CLI or via NMP or SNMP.

REST API interface

All configuration, status and SmartOffice parameter can be accessed remotely using an REST interface. Versions with and without JSON are available. Multiple objects can be processed per message. All access protection schemes apply. SSH is used.

This permits secure machine-to-machine communication mostly intended for but not limited to IoT applications.

5.2 Functional Description

Switch status and configuration parameter values can be accessed via the integrated Web Manager using a standard web browser. For secure access, HTTPS protocol can be enabled (default setting).

ATTENTION: When using NMP for device management, HTTPS protocol is mandatory. When changing access protocol to HTTP, NMP cannot communicate with device.

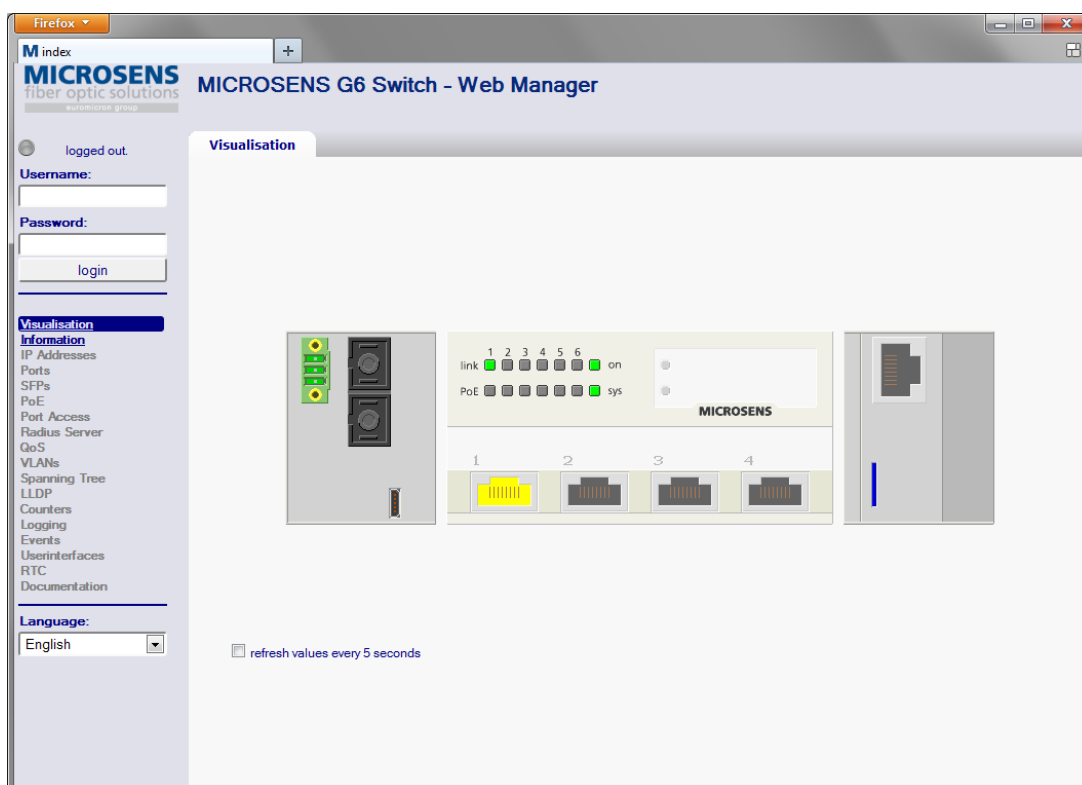
5.2.1 Browser Compatibility

The Web manager content was designed for maximum compatibility with standard web browsers like Microsoft® Internet Explorer® 8 and Mozilla® Firefox® 14. For correct function the Web Manager requires Java Script support to be enabled. For best view we recommend Firefox Version 14.

5.2.2 Start Page

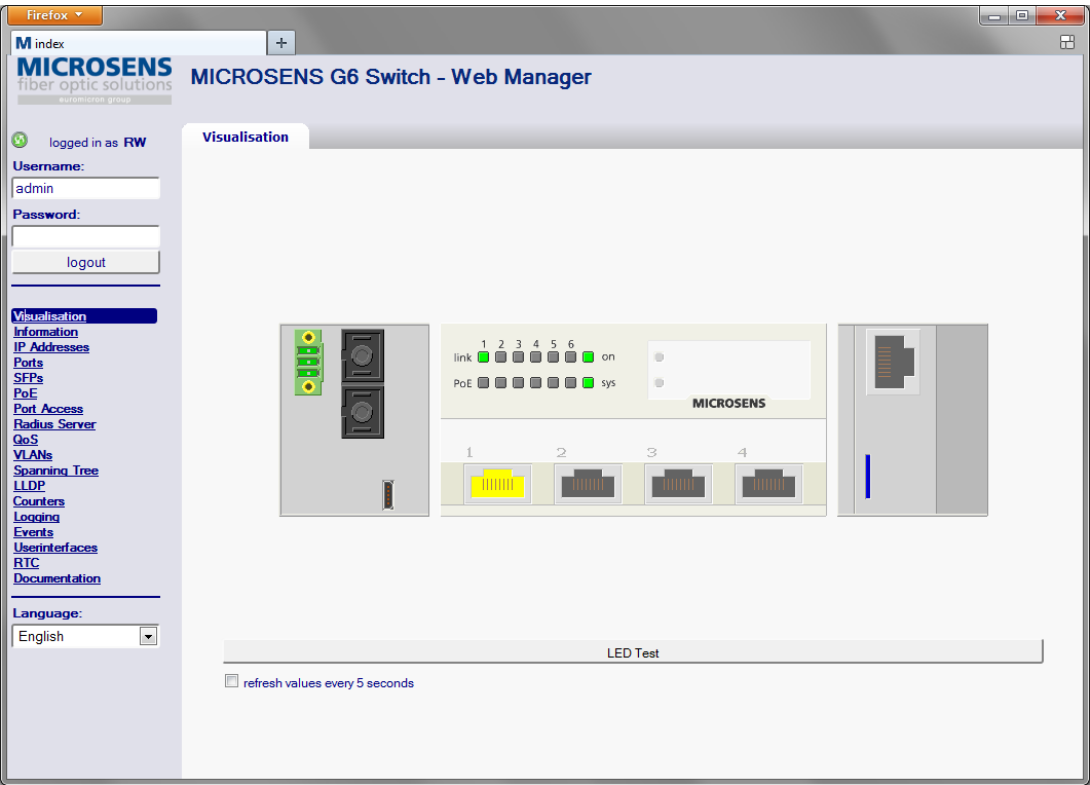
To access the Web Manager, open a web browser and insert the device IP address into the address field. The start page of the device should be displayed immediately. Without a valid login, only basic device status information is displayed. No changes to the device settings can be made, most of the menu items on the sidebar are deactivated.

INFO: For security reasons, the default protocol for Web Manager access is HTTPS. When typing the device IP address, use 'https://' prefix for protocol selection. It may be required to confirm a security exception before the page is displayed by the browser. This is no security risk. The protocol used can be changed in the Web Manager configuration section (CLI command: 'Management.WEB.protocol = DISABLED|HTTP|HTTPS').



5.2.3 Login

For full access to the Web Manager, a login with a valid user name/password is required. Enter the login credential into the fields on the sidebar and click the 'Login' button. The sidebar menu items become activated for full access to all functions.



5.3 WEB CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Management.						
	web.					Web interface settings and SmartOffice web gui definitions
			protocol		R/W	Define which web client access protocol is used. Changes only become active after restarting the web server or the whole device.
			web_timeout		R/W	Inactivity time out in seconds. When a web session is unused for the specified duration, the user is logged off.
			http_port_web		R/W	Port used for http protocol access. Standard port is 80. Can be changed when non-standard port shall be used for Web management traffic. Changes only become active after restarting the web server or the whole device.
			https_port_web		R/W	Port used for https protocol access. Standard port is 443. Can be changed when non-standard port shall be used for Web management traffic. Changes only become active after restarting the web server or the whole device.
			certificate_source		R/W	Determines if internal default certificate is used or a customer downloaded certificate is used. The custom certificate needs to be specified after selecting the CUSTOM option using the Management.files.certificate.activate_for_web command.
			enter_cert_passphrase		X	Set a new certificate passphrase. This parameter is only required when certificate_source is set to CUSTOM and the activated certificate requires a passphrase
			encrypted_cert_passphrase		R/W	
			login_message		R/W	This message is displayed during login to the management web server. Changes only become active after restarting the web server or the whole device.
			restart_web_server		X	This command will restart the web server. Currently open web sessions will be lost. The connection to nmp will briefly be interrupted. Syntax: restart_web_server = CONFIRM.
		gui_page[DYNAMIC].				Define the look and feel of the SmartOffice graphical user interface.
			name		R/W	Unique name under which the page is reference a in the web gui.

gui_mode	R/W	Permits limiting of gui functionality for example in public places.
color_scheme	R/W	Select desired look of the page. Different pages may use different color schemes even if the same elements are placed on them.
element_placement	R/W	Determines how the gui_elements are placed in the browser window.
limited_to_users	R/W	When left blank, every user has access to the gui page and its associated elements. When one or more comma separated user names are defined, then local or remote access to the page and its elements is limited to the listed users.
options	R/W	Optional additional parameter may be defined here is a comma separated list. Rendering options defined here, will be applied to all elements placed on the page, unless overridden with options defined at element level.
gui_element[DYNAMIC].		Defines a single element of the user interface gui. Defines position as well as content and function.
name	R/W	Unique name of the element.
type	R/W	Predefined type of element. Choose to suit the functionality needed.
page	R/W	Name of gui page(s) on which this element is placed on. Use comma to specify several pages.
visibility	R/W	Defines if an element is rendered on the gui.
auto_save	R/W	When enabled, this gui element saves the current setting as the default value to be used should the system restart.
remote_accessible	R/W	When enabled, this gui element may be accessed via the remote access interface. Use this parameter to restrict the remote interface to the required elements only.
sensor_attribute	R/W	Indicates which type of sensor this gui element simulates when being operated. If left blank the element will register with its type as default.
script_name	R/W	When this element is updated the script specified in this parameter is executed. If the parameter is left blank, the standard MS_SmartOfficeControl.ms script is executed. The specified script should not contain any time consuming functions. Syntax: app/file:sub par1 par2 Parameter are optional. When the app part is not supplied the file is expected in xml_cli_scripts folder.
watched_element	R/W	Here a valid CLI command may be entered to display any system parameter. Status or config values may be specified. Alternatively, the content of a persistent variable may be watched. Such variables can be maintained by microScript. Syntax: \$varname.
order	R/W	Elements are displayed in this order. Elements with same index appear in the order they are configured. There may be gaps in the order of elements.

height	R/W	Height of element in percent of container height.
width	R/W	Width of element in percent of container width.
top_margin	R/W	Defines the distance of element in percent of container height below the above element. Can be used to position element in relation to others.
left_margin	R/W	Defines the distance of element in percent of container width from the end of the previous element to the left. Can be used to position element in relation to others.
header	R/W	Title to be displayed above the element, doesn't preserve space if left empty.
text	R/W	Comma separated list of texts. Appearance depends on the type of element.
value	R/W	Comma separated list of values. Usage depends on the type of element.
start_value	R/W	Default or start value which is used when the element is first created. This value is automatically updated to reflect the last setting when the auto_save parameter is enabled. This value only applies to active elements.
image	R/W	Comma separated list of images to display on the element.
options	R/W	Optional element specific additional parameter may be placed here.

5.4 WEB Configuration Parameters

Group Path	General Parameters Management.WEB								
protocol	<p>Define which web client access protocol is used. Changes only become active after restarting the web server or the whole device.</p> <p>Values</p> <table> <tr> <td><i>DISABLED</i></td><td>Web interface is disabled</td></tr> <tr> <td><i>HTTP_UNSECURE</i></td><td>Standard client interface without encryption</td></tr> <tr> <td><i>HTTPS_LESS_SECURE</i></td><td>Secure client interface which still permits use of deprecated versions TLS1.0 and 1.1 as well as SSLv2 and SSLv3</td></tr> <tr> <td><i>HTTPS_SECURE</i></td><td>Secure client interface which requires at least TLS 1.2</td></tr> </table> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.1 (webProtocol)</p>	<i>DISABLED</i>	Web interface is disabled	<i>HTTP_UNSECURE</i>	Standard client interface without encryption	<i>HTTPS_LESS_SECURE</i>	Secure client interface which still permits use of deprecated versions TLS1.0 and 1.1 as well as SSLv2 and SSLv3	<i>HTTPS_SECURE</i>	Secure client interface which requires at least TLS 1.2
<i>DISABLED</i>	Web interface is disabled								
<i>HTTP_UNSECURE</i>	Standard client interface without encryption								
<i>HTTPS_LESS_SECURE</i>	Secure client interface which still permits use of deprecated versions TLS1.0 and 1.1 as well as SSLv2 and SSLv3								
<i>HTTPS_SECURE</i>	Secure client interface which requires at least TLS 1.2								
web_timeout	<p>Inactivity time out in seconds. When a web session is unused for the specified duration, the user is logged off.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.2 (webWebTimeout)</p>								
http_port_web	<p>Port used for http protocol access. Standard port is 80. Can be changed when non-standard port shall be used for Web management traffic. Changes only become active after restarting the web server or the whole device.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.3 (webHttpPortWeb)</p>								
https_port_web	<p>Port used for https protocol access. Standard port is 443. Can be changed when non-standard port shall be used for Web management traffic. Changes only become active after restarting the web server or the whole device.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.4 (webHttpsPortWeb)</p>								
certificate_source	<p>Determines if internal default certificate is used or a customer downloaded certificate is used. The custom certificate needs to be specified after selecting the CUSTOM option using the Management.files.certificate.activate_for_web command.</p> <p>Values</p> <table> <tr> <td><i>INTERN</i></td><td>Use internal default certificate</td></tr> <tr> <td><i>CUSTOM</i></td><td>Use custom certificate. Needs further activation via certificate.activate = certificate command.</td></tr> </table> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.5 (webCertificateSource)</p>	<i>INTERN</i>	Use internal default certificate	<i>CUSTOM</i>	Use custom certificate. Needs further activation via certificate.activate = certificate command.				
<i>INTERN</i>	Use internal default certificate								
<i>CUSTOM</i>	Use custom certificate. Needs further activation via certificate.activate = certificate command.								

enter_cert_passphrase	<p>Set a new certificate passphrase. This parameter is only required when certificate_source is set to CUSTOM and the activated certificate requires a passphrase</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.6 (webEnterCertPassphrase)</p>
encrypted_cert_passphrase	<p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.7 (webEncryptedCertPassphrase)</p>
login_message	<p>This message is displayed during login to the management web server. Changes only become active after restarting the web server or the whole device.</p> <p>Value String, max. 512 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.8 (webLoginMessage)</p>
restart_web_server	<p>This command will restart the web server. Currently open web sessions will be lost. The connection to nmp will briefly be interrupted. Syntax: restart_web_server = CONFIRM.</p> <p>Action Execute command with parameter string max. 16 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.9 (webRestartWebServer)</p>

Group	gui_page , dynamical size		
Path	Management.WEB.gui_page		
Description	Define the look and feel of the SmartOffice graphical user interface.		
<hr/>			
name	Unique name under which the page is reference a in the web gui.		
	Value	String, max. 32 characters.	
	OID	1.3.6.1.4.1.3181.10.6.3.63.10.1.2 (guiPageName)	
<hr/>			
gui_mode	Permits limiting of gui functionality for example in public places.		
	Values	<div><div><i>DISABLED</i></div><div>This gui page is turned off</div></div> <div><div><i>DISPLAY_ONLY</i></div><div>The gui can be used to display values but no actions may be performed. No set command is accepted via the remote access interface</div></div> <div><div><i>NORMAL</i></div><div>Normal gui operation with all available features. Also permits use of the remote access interface.</div></div> <div><div><i>REMOTE_ONLY</i></div><div>This gui page is not available to the browser, but its elements can be controlled with the remote_access interface</div></div>	
	OID	1.3.6.1.4.1.3181.10.6.3.63.10.1.3 (guiPageGuiMode)	

color_scheme	Select desired look of the page. Different pages may use different color schemes even if the same elements are placed on them.																						
Values	<table> <tr><td><i>GRAY</i></td><td>Gray color scheme</td></tr> <tr><td><i>BLUE</i></td><td>Default blueish color scheme</td></tr> <tr><td><i>RED</i></td><td>Red color scheme</td></tr> <tr><td><i>LIME</i></td><td>Lime color scheme</td></tr> <tr><td><i>YELLOW</i></td><td>Yellow color scheme</td></tr> <tr><td><i>PINK</i></td><td>Pink color scheme</td></tr> <tr><td><i>CYAN</i></td><td>Cyan color scheme</td></tr> <tr><td><i>GREEN</i></td><td>Green color scheme</td></tr> <tr><td><i>ORANGE</i></td><td>Orange color scheme</td></tr> <tr><td><i>PURPLE</i></td><td>Purple color scheme</td></tr> <tr><td><i>TEAL</i></td><td>Teal color scheme</td></tr> </table>	<i>GRAY</i>	Gray color scheme	<i>BLUE</i>	Default blueish color scheme	<i>RED</i>	Red color scheme	<i>LIME</i>	Lime color scheme	<i>YELLOW</i>	Yellow color scheme	<i>PINK</i>	Pink color scheme	<i>CYAN</i>	Cyan color scheme	<i>GREEN</i>	Green color scheme	<i>ORANGE</i>	Orange color scheme	<i>PURPLE</i>	Purple color scheme	<i>TEAL</i>	Teal color scheme
<i>GRAY</i>	Gray color scheme																						
<i>BLUE</i>	Default blueish color scheme																						
<i>RED</i>	Red color scheme																						
<i>LIME</i>	Lime color scheme																						
<i>YELLOW</i>	Yellow color scheme																						
<i>PINK</i>	Pink color scheme																						
<i>CYAN</i>	Cyan color scheme																						
<i>GREEN</i>	Green color scheme																						
<i>ORANGE</i>	Orange color scheme																						
<i>PURPLE</i>	Purple color scheme																						
<i>TEAL</i>	Teal color scheme																						
OID	1.3.6.1.4.1.3181.10.6.3.63.10.1.4 (guiPageColorScheme)																						
element_placement	Determines how the gui_elements are placed in the browser window.																						
Values	<table> <tr> <td><i>CHAINED</i></td> <td>Each gui_element is placed behind the each other. When line is full the next line below is selected. Default mode of operation.</td> </tr> <tr> <td><i>ABSOLUTE</i></td> <td>The position of a gui_element is determined by the margins relative to the container. Overlapping of elements may occur.</td> </tr> </table>	<i>CHAINED</i>	Each gui_element is placed behind the each other. When line is full the next line below is selected. Default mode of operation.	<i>ABSOLUTE</i>	The position of a gui_element is determined by the margins relative to the container. Overlapping of elements may occur.																		
<i>CHAINED</i>	Each gui_element is placed behind the each other. When line is full the next line below is selected. Default mode of operation.																						
<i>ABSOLUTE</i>	The position of a gui_element is determined by the margins relative to the container. Overlapping of elements may occur.																						
OID	1.3.6.1.4.1.3181.10.6.3.63.10.1.5 (guiPageElementPlacement)																						
limited_to_users	When left blank, every user has access to the gui page and its associated elements. When one or more comma separated user names are defined, then local or remote access to the page and its elements is limited to the listed users.																						
Value	String, max. 128 characters.																						
OID	1.3.6.1.4.1.3181.10.6.3.63.10.1.6 (guiPageLimitedToUsers)																						
options	Optional additional parameter may be defined here is a comma separated list. Rendering options defined here, will be applied to all elements placed on the page, unless overridden with options defined at element level.																						
Value	String, max. 512 characters.																						
OID	1.3.6.1.4.1.3181.10.6.3.63.10.1.7 (guiPageOptions)																						
Group Path Description	gui_element , dynamical size Management.WEB.gui_element Defines a single element of the user interface gui. Defines position as well as content and function.																						

name	Unique name of the element.		
	Value	String, max. 32 characters.	
	OID	1.3.6.1.4.1.3181.10.6.3.63.11.1.2 (guiElementName)	
type	Predefined type of element. Choose to suit the functionality needed.		
	Values	LABEL	Static (fixed) text to display
		IMAGE	Used to place graphics from file
		HYPER_LINK	Button to click on to switch to another web page
		SPACE	Positioning tool
		LINE	Graphical element to draw lines
		FRAME	Graphical element to visually group elements that belong together logically
		BUTTON	One or several buttons to click on
		SELECT_BOX	Select box with predefined values
		SLIDER	Slider with predefined range
		RADIO_BUTTON	Radiobuttons with predefined values
		TOGGLE	Toggle button
		INPUT	Text input box which pops up a keypad
		CHECKBOX	Single or multiple check boxes
		TEXT_BOX	Text field which can hold information
		BAR_GRAPH	Bargraph to display an integer value
		GAUGE	Scaled gauge with pointer and range
		SYMBOL	Dynamic graphical status element
		DIAGRAM	Diagram as bar chart
		TABLE	Table element
	OID	1.3.6.1.4.1.3181.10.6.3.63.11.1.3 (guiElementType)	
page	Name of gui page(s) on which this element is placed on. Use comma to specify several pages.		
	Value	String, max. 512 characters.	
	OID	1.3.6.1.4.1.3181.10.6.3.63.11.1.4 (guiElementPage)	
visibility	Defines if an element is rendered on the gui.		
	Values	NORMAL	The element is shown
		HIDDEN	The element takes up screen space but is not visible
		DISABLED	The element is not drawn and takes no screen space
	OID	1.3.6.1.4.1.3181.10.6.3.63.11.1.5 (guiElementVisibility)	
auto_save	When enabled, this gui element saves the current setting as the default value to be used should the system restart.		
	Values	enabled, disabled	
	OID	1.3.6.1.4.1.3181.10.6.3.63.11.1.6 (guiElementAutoSave)	

remote_accessible	<p>When enabled, this gui element may be accessed via the remote access interface. Use this parameter to restrict the remote interface to the required elements only.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.11.1.7 (guiElementRemoteAccessible)</p>
sensor_attribute	<p>Indicates which type of sensor this gui element simulates when being operated. If left blank the element will register with its type as default.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.11.1.8 (guiElementSensorAttribute)</p>
script_name	<p>When this element is updated the script specified in this parameter is executed. If the parameter is left blank, the standard MS_SmartOfficeControl.ms script is executed. The specified script should not contain any time consuming functions. Syntax: app/file:sub par1 par2 Parameter are optional. When the app part is not supplied the file is expected in xml_cli_scripts folder.</p> <p>Value String, max. 63 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.11.1.9 (guiElementScriptName)</p>
watched_element	<p>Here a valid CLI command may be entered to display any system parameter. Status or config values may be specified. Alternatively, the content of a persistent variable may be watched. Such variables can be maintained by microScript. Syntax: \$varname.</p> <p>Value String, max. 512 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.11.1.10 (guiElementWatchedElement)</p>
order	<p>Elements are displayed in this order. Elements with same index appear in the order they are configured. There may be gaps in the order of elements.</p> <p>Value Number in range 0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.11.1.11 (guiElementOrder)</p>
height	<p>Height of element in percent of container height.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.11.1.12 (guiElementHeight)</p>
width	<p>Width of element in percent of container width.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.11.1.13 (guiElementWidth)</p>
top_margin	<p>Defines the distance of element in percent of container height below the above element. Can be used to position element in relation to others.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.11.1.14 (guiElementTopMargin)</p>

left_margin	<p>Defines the distance of element in percent of container width from the end of the previous element to the left. Can be used to position element in relation to others.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.11.1.15 (guiElementLeftMargin)</p>
header	<p>Title to be displayed above the element, doesn't preserve space if left empty.</p> <p>Value String, max. 64 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.11.1.16 (guiElementHeader)</p>
text	<p>Comma separated list of texts. Appearance depends on the type of element.</p> <p>Value String, max. 512 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.11.1.17 (guiElementText)</p>
value	<p>Comma separated list of values. Usage depends on the type of element.</p> <p>Value String, max. 512 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.11.1.18 (guiElementValue)</p>
start_value	<p>Default or start value which is used when the element is first created. This value is automatically updated to reflect the last setting when the auto_save parameter is enabled. This value only applies to active elements.</p> <p>Value String, max. 64 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.11.1.19 (guiElementStartValue)</p>
image	<p>Comma separated list of images to display on the element.</p> <p>Value String, max. 512 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.11.1.20 (guiElementImage)</p>
options	<p>Optional element specific additional parameter may be placed here.</p> <p>Value String, max. 512 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.63.11.1.21 (guiElementOptions)</p>

6 Simple Network Management Protocol (SNMP)

6.1 Key Features

SNMP V1/V2c

Simple Network Management Protocol v1, v2c (SNMPv1, v2c) to access device information stored in Management Information Base (MIB). Security provided by community strings for Set/Get commands.

Provide universal access to all parameter using standards based interface.

SNMP V1/2c Security

SNMP v1/v2c does not provide any access protection other than an easily scanned community string. The device offers additional protection through the possibility to map SNMP requests to a certain user. Each request inherits the access rights of this user and these are applied prior to execution. Please refer to Access section. Additionally, it is possible to generally block all SET commands.

This unique feature combines the ease of SNMP V1/V2c with the view model protection of SNMP V3 without the burden SNMP V3 carries along.

SNMP V3

Simple Network Management Protocol v3 (SNMPv3) for secure access to device information stored in Management Information Base (MIB). SNMPv3 supports data encryption, User-based Security Model (USM) and View-based Access Control Model (VACM).

Full implementation of SNMP V3 allows secure and standards based interoperability with third party management systems.

SNMP TSM

Support of Transport Security Model TSM for SNMP v3. This includes agent and user certificates . SNMP traffic is tunnelled via SSH.

Highest security options for SNMP permit use of SNMP in mission critical networks.

Traps (SNMP V1/V2c/V3)

Traps, Notifications or Informs can be sent to an unlimited number of independently configurable receiver destinations. Sending of message is triggered by internal device status change events. Informs provide secured messaging by requiring response message. Event triggers can be configured individually per destination. Test function to trigger Trap/Notification for simplified configuration check

Highly configurable event and trap system adapts to any networking environment.

Private Traps

In addition or alternatively, private traps may be generated. Any internal event that causes a syslog may also be presented as SNMP trap. This includes configuration changes or user log-in for example. There are about 80 private event types.

Private traps offer more detail and insight into the device than the limited standard traps would allow.

Private and Public MIBs

The device supports private MIBs that cover every aspect of the device. Additionally numerous standard MIBs are supported. Please refer to separate documentation. Private MIB File can be downloaded from the integrated Web Manager.

Private MIBs allow access to any device parameter even if not usually included in standard MIBs. Standard MIB support ensures integration in tool chains that work across a number of different vendors.

ARP-Guard Compliance

Compliant with ARP-Guard (ISL GmbH) network control software which may be used for additional network security. Requires precise implementation of all BRIDGE-MIB features and other SNMP details.

Ensures seamless network integration.

MACMON Compliance

Compliant with MACMON (MIKADO AG) network control software which may be used for additional network security. Requires precise implementation of all BRIDGE-MIB features and other SNMP details.

Ensures seamless network integration.

Integrated SNMP Browser

SNMP commandline browser supports GET, GETNEXT, SET and WALK with all protocol levels v1/v2c/v3. Understands G6 private MIBs and some basic general purpose MIBs for easy textual retrieval.

Permits monitoring of foreign devices. The browser can be used inside microScripts to perform local actions depending on the state of another machine. May also be used to configure a foreign machine.

6.2 Functional Description

The Simple Network Management Protocol (SNMP) is an application-layer protocol for the exchange of management information between network devices. It is part of the TCP/IP protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

6.2.1 SNMP key components

SNMP consists of following key components:

- Managed device is a network node that contains SNMP agent. Managed devices collect and store management information and make this information available to NMS using SNMP. Managed device can be switches/Hub, etc.
- MIB (Management Information Base) define the complete manageable entries of the managed device. These MIB entries can be either read-only or read-write. For example, the 'System Version' is a read-only variable. The 'Port State Enable' or 'Disable' is a read-write variable and a network administrator can not only read but also set its value remotely.
- SNMP Agent is a management module resides in the managed device that responds to the SNMP Manager request. SNMP Manager/NMS executes applications that monitor and control managed devices. NMS provide the bulk of the processing and memory resources

required for the complete network management. SNMP Manager often composed by desktop computer/work station and software program such like HP OpenView.

6.2.2 SNMP Operations

Totally 4 types of operations are used between SNMP Agent and Manager to change the MIB information. These 4 operations all use the UDP/IP protocol to exchange packets.

- GET: This command is used by an SNMP Manager to monitor managed devices. The SNMP Manager examines different variables that are maintained by managed devices.
- GET Next: This command provides traversal operation and is used by the SNMP Manager to sequentially gather information in variable tables, such as a routing table.
- SET: This command is used by an SNMP Manager to control managed devices. The NMS changes the values of variables stored within managed devices.
- Trap: Trap is used by the managed device to report asynchronously a specified event to the SNMP Manager. When certain types of events occur, a managed device will send a trap to alert the SNMP Manager.

6.2.3 SNMP Versions

The Simple Network Management protocol can be implemented in 3 different versions, SNMPv1, v2c and SNMPv3.

SNMPv1 and v2c implement only rudimentary security mechanism and transmit information unencrypted, whereas SNMPv3 implements an user based access model and transmits all information encrypted.

For maximum security, SNMPv1 and SNMPv2c access can be disabled when SNMPv3 is used.

6.2.4 SNMP Notifications (Traps and Informs)

System events can trigger the sending of SNMP notifications to an external receiver. These notifications can be one-way only (Traps) or acknowledged (Informs). Please see section 'Event Messages' of this document for further reference.

6.2.5 SNMP MIB File

Before using the SNMP based network management system, normally the MIB file must be installed to be able to decode the device parameters. The MIB file (Management Information Base) defines all parameters (OIDs) that can be accessed via SNMP protocol.

Besides the standard MIBs defined in RFCs, all device specific functions can be accessed via an enterprise-specific private MIB.

The private MIB files can be downloaded from the integrated Web-Manager in the 'Documents' section. There is one separate MIB file for each feature section and one global MIB file. The file name extension is .mib, which SNMP based compiler can import.

Please refer to the appropriate documentation for the instructions of installing the system private MIB on your network management software.

6.2.6 SNMP System Information

To simplify the identification and administration of installed devices, individual information fields can be set by the user. This includes the standard information *description*, *location* and *contact* plus an additional field for device group information (for structuring networks into functional

groups) and an inventory string which can be used for entering an individual identification number used for automatic inventory retrieval.

6.3 SNMP CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Management.						
		snmp.				Simple Network Mangement Protocol (SNMP) server setup
		device_info.				SNMP version MIB-2 variables
			sys_description		R	Device description. This value is SNMP accessible as sysDescr.
			sys_name		R/W	Device name as assigned by customer. This value is SNMP accessible as sysName.
			sys_location		R/W	Location of this device as assigned by customer. This value is SNMP accessible as sysLocation.
			sys_group		R/W	Customer defined group definition. Note: This field does not have a MIB-2 counterpart.
			sys_contact		R/W	Contact person for this device as required by customer. This value is SNMP accessible as sysContact.
			sys_object_id		R	Response to SNMP sysObject request.
		v1v2_config.				SNMP version V1 / V2 variables
			enable_snmp_v1		R/W	Only when enabled will SNMP V1 requests be responded to. May be disabled when only secure SNMP V3 access is allowed.
			enable_snmp_v2c		R/W	Only when enabled will SNMP V2C requests be responded to. May be disabled when only secure SNMP V3 access is allowed.
			get_community		R/W	Community string to enable V1/ V2c get commands.
			set_community		R/W	Community string to enable V1/ V2c set commands.

snmp_v1v2_username	R/W	SNMP v1/v2 normally only provides light security by means of the community strings. Additional V3 like security can be applied by setting this field to any user.name defined in the access section. The access restrictions defined for the selected user also apply to the SNMP V1/v2 access when the user name is specified here. When no username or an invalid user name is configured, SNMP access is blocked.
permit_v1v2_set_commands	R/W	When disabled SNMP sets (writes) are declined and no modifications to the system via unsecure SNMP V1/V2 can occur.
v3_config.		SNMP version V3 variables
enable_snmp_v3	R/W	Only when enabled will SNMP V3 requests be responded to. To limit access to SNMP V3 only, disable SNMP V1 and V2 access in the configuration.
security_model	R/W	Selects if user based or view based security model is used.
snmp_engine_id	R/W	Administratively assigned part of the computed engine id. Here the used MAC address can be used to ensure a unique value.
trap_engine_id	R/W	This engine id is used for outgoing SNMP v3 traps. The value is treated as hexadecimal characters. The associated trap receiver must match this sequence or may be setup to ignore the engine id altogether. Default value defines 80000c6d which represents the our IANA value in hex followed by 03 indicating that a MAC is following. The remaining 12 character represent the MAC address of this device.
browser.		SNMP browser actions
get	X	Invokes SNMP GET command at other device. Easiest syntax: ..get hostname OID. Type = (nothing) for basic help and = ? for extensive help.
next	X	Invokes SNMP GETNEXT command at other device. It will display the next OID following the given one. Syntax: ..get -v 2c -c community hostname OID. Hostname can be symbolic or IP address.
set	X	Invokes SNMP SET command at other device. Easiest syntax: ..set hostname OID type value. Check examples shown with = (enter).

walk	X	Invokes SNMP MIBWALK command at other device. Basic syntax: = IP_address. To see MIB-II system group type = IP system. WARNING: an unlimited MIB walk may take a long time. Even when the output is cancelled, the walk will continue to the end. During this time other action commands may not operate!
engine_boots	R	Number of reboots of SNMP engine since system reboot.
engine_runtime	R	Runtime of SNMP engine in seconds.

6.4 SNMP Configuration Parameters

Group	device_info
Path	Management.SNMP.device_info
Description	SNMP version MIB-2 variables
sys_description	<p>Device description. This value is SNMP accessible as sysDescr.</p> <p>Value String, max. 255 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.65.1.1.2 (deviceInfoSysDescription) 1.3.6.1.2.1.1.1 (sysDescr) 1.0.8802.1.1.2.1.3.4 (lldpLocSysDesc)</p>
sys_name	<p>Device name as assigned by customer. This value is SNMP accessible as sysName.</p> <p>Value String, max. 255 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.65.1.1.3 (deviceInfoSysName) 1.3.6.1.2.1.1.5 (sysName) 1.0.8802.1.1.2.1.3.3 (lldpLocSysName)</p>
sys_location	<p>Location of this device as assigned by customer. This value is SNMP accessible as sysLocation.</p> <p>Value String, max. 255 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.65.1.1.4 (deviceInfoSysLocation) 1.3.6.1.2.1.1.6 (sysLocation)</p>
sys_group	<p>Customer defined group definition. Note: This field does not have a MIB-2 counterpart.</p> <p>Value String, max. 255 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.65.1.1.5 (deviceInfoSysGroup)</p>
sys_contact	<p>Contact person for this device as required by customer. This value is SNMP accessible as sysContact.</p> <p>Value String, max. 255 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.65.1.1.6 (deviceInfoSysContact) 1.3.6.1.2.1.1.4 (sysContact)</p>
sys_object_id	<p>Response to SNMP sysObject request.</p> <p>Value String, max. 24 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.65.1.1.7 (deviceInfoSysObjectId) 1.3.6.1.2.1.1.2 (sysObjectID)</p>

Group Path Description	v1v2_config Management.SNMP.v1v2_config SNMP version V1 / V2 variables
enable_snmp_v1	<p>Only when enabled will SNMP V1 requests be responded to. May be disabled when only secure SNMP V3 access is allowed.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.65.2.1.2 (v1v2ConfigEnableSnmpV1)</p>
enable_snmp_v2c	<p>Only when enabled will SNMP V2C requests be responded to. May be disabled when only secure SNMP V3 access is allowed.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.65.2.1.3 (v1v2ConfigEnableSnmpV2c)</p>
get_community	<p>Community string to enable V1/V2c get commands.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.65.2.1.4 (v1v2ConfigGetCommunity)</p>
set_community	<p>Community string to enable V1/V2c set commands.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.65.2.1.5 (v1v2ConfigSetCommunity)</p>
snmp_v1v2_username	<p>SNMP v1/v2 normally only provides light security by means of the community strings. Additional V3 like security can be applied by setting this field to any user.name defined in the access section. The access restrictions defined for the selected user also apply to the SNMP V1/v2 access when the user name is specified here. When no username or an invalid user name is configured, SNMP access is blocked.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.65.2.1.6 (v1v2ConfigSnmpV1v2Username)</p>
permit_v1v2_set_commands	<p>When disabled SNMP sets (writes) are declined and no modifications to the system via unsecure SNMP V1/V2 can occur.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.65.2.1.7 (v1v2ConfigPermitV1v2SetCommands)</p>
Group Path Description	v3_config Management.SNMP.v3_config SNMP version V3 variables

enable_snmp_v3	Only when enabled will SNMP V3 requests be responded to. To limit access to SNMP V3 only, disable SNMP V1 and V2 access in the configuration. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.3.65.3.1.2 (v3ConfigEnableSnmpV3)
security_model	Selects if user based or view based security model is used. Values <i>USM</i> User-based Security Model. <i>VACM</i> View-based Access Control Model. <i>TSM</i> Transport Security Model. OID 1.3.6.1.4.1.3181.10.6.3.65.3.1.3 (v3ConfigSecurityModel)
snmp_engine_id	Administratively assigned part of the computed engine id. Here the used MAC address can be used to ensure a unique value. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.3.65.3.1.4 (v3ConfigSnmpEngineId)
trap_engine_id	This engine id is used for outgoing SNMP v3 traps. The value is treated as hexadecimal characters. The associated trap receiver must match this sequence or may be setup to ignore the engine id altogether. Default value defines 80000c6d which represents the our IANA value in hex followed by 03 indicating that a MAC is following. The remaining 12 character represent the MAC address of this device. Value String, max. 66 characters. OID 1.3.6.1.4.1.3181.10.6.3.65.3.1.5 (v3ConfigTrapEngineId)

Group	browser
Path	Management.SNMP.browser
Description	SNMP browser actions
get	Invokes SNMP GET command at other device. Easiest syntax: ..get hostname OID. Type = (nothing) for basic help and = ? for extensive help. Action Execute command with parameter string max. 128 characters. OID 1.3.6.1.4.1.3181.10.6.3.65.4.1.2 (browserGet)
next	Invokes SNMP GETNEXT command at other device. It will display the next OID following the given one. Syntax: ..get -v 2c -c community hostname OID. Hostname can be symbolic or IP address. Action Execute command with parameter string max. 128 characters. OID 1.3.6.1.4.1.3181.10.6.3.65.4.1.3 (browserNext)

set	Invokes SNMP SET command at other device. Easiest syntax: ..set hostname OID type value. Check examples shown with = (enter).
Action	Execute command with parameter string max. 128 characters.
OID	1.3.6.1.4.1.3181.10.6.3.65.4.1.4 (browserSet)

walk	Invokes SNMP MIBWALK command at other device. Basic syntax: = IP_address. To see MIB-II system group type = IP system. WARNING: an unlimited MIB walk may take a long time. Even when the output is cancelled, the walk will continue to the end. During this time other action commands may not operate!
Action	Execute command with parameter string max. 128 characters.
OID	1.3.6.1.4.1.3181.10.6.3.65.4.1.5 (browserWalk)

6.5 SNMP Status Parameters

Group Path	General Parameters Management.SNMP
engine_boots	<div>Number of reboots of SNMP engine since system reboot.</div> <div>Value Number in range 0-0xFFFFFFFF</div> <div>OID 1.3.6.1.4.1.3181.10.6.3.65.100 (snmpEngineBoots)</div>
engine_runtime	<div>Runtime of SNMP engine in seconds.</div> <div>Value Number in range 0-0xFFFFFFFF</div> <div>OID 1.3.6.1.4.1.3181.10.6.3.65.101 (snmpEngineRuntime)</div>

7 RADIUS Servers

7.1 Key Features

Access

RADIUS client via UDP/IP ports 1812 (access) for Remote Authentication Dial In User Service (RADIUS) server for authorizing user access.

Use of RADIUS permits access to network wide login policies which eases user management in large companies.

Accounting

RADIUS client via UDP/IP port 1813 (accounting) for Remote Authentication Dial In User Service (RADIUS) server for logging of user accounting information.

Centralized RADIUS server can log user access information.

Redundancy

In case of a response timeout, a secondary RADIUS server can be requested. Up to 8 RADIUS server for use in different applications may be specified.

Multiple RADIUS server may be specified to ensure continued service.

Tunnel Attributes

When port-based network access control and VLANs are enabled additional RADIUS attributes can be added to the RADIUS ACCESS-REQUEST frames.

This allows for a port to be placed into a particular VLAN, based on the result of the authentication.

7.2 Functional Description

When Port-based Access Control is enabled, user login is controlled by a central RADIUS server (Remote Authentication Dial-In User Service). Multiple RADIUS servers can be defined for redundancy. If a server fails to respond to a request, the next active server is requested.

ATTENTION: *If you have a single RADIUS Server for both authentication and accounting, make sure that is present twice in the device's database with the correct port number for each type of service and that you assign the proper server to the port access control parameters referencing it.*

7.2.1 RADIUS Authentication

The user or machine connected to a switch port is requested to send its access credentials, typically in the form of username and password or security certificate. This information is sent by the switch to a central RADIUS server.

The RADIUS server verifies that the information is correct against a user database and then returns a response:

Access Reject

The user is denied access to the network. Reasons may be failure of identification or an unknown or inactive user account.

Access Accept

The user is granted access to the network.

Attributes in the Access-Accept RADIUS packet

The switch supports several attributes in the Access-Accept RADIUS packet.

To set a VLAN for a specific user authorized on a certain switch port via PACC, the following attributes are required:

Tunnel-Type = VLAN(13),

Tunnel-Medium-Type = 802(6)

Tunnel-Private-Group-Id = (VLAN ID #) OR (name of locally configured VLAN)

INFO: The Tunnel-Type attribute indicates the tunneling protocol(s) to be used and must always be VLAN(13).

INFO: The Tunnel-Medium-Type attribute indicates which transport medium to use and must always be 802(6).

INFO: The Tunnel-Private-Group-Id attribute indicates the VLAN ID for this authorization response.

To assign privileges to a RADIUS authorized user on any management interface, the RADIUS Server must provide the Filter-ID attribute defined in RFC2865 with a locally known user as parameter. Example:

Filter-Id(11) = admin

The default users of "admin" and "user" allow for full access and read-only access.

7.3 RADIUS CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Management.						
	radius.					RADIUS server definitions
			server[DYNAMIC].			This dynamic table is used to specify access parameter to authentication servers using RADIUS or TACACS+.
			name	R/W		Unique name used to identify the server. Used for reference in Port-based Access Control configuration.
			server_type	R/W		Flags if RADIUS or TACACS+ is specified in this entry.
			host_address	R/W		IP address or symbolic name of the authentication server. IPv4 or IPv6 with lower case letter is acceptable
			udp_port	R/W		UDP port for RADIUS authentication service. Standard port is 1812. For TACACS+ this specifies the TCP port which defaults to 49.
			shared_secret	R/W		Shared Secret as common password between authenticator and server. THIS FIELD IS DEPRACATED. Provided for backward compatibility. Use the secure enter_shared_secret command instead.
			enter_shared_secret	X		Set a shared secret as common password between authenticator and server. The input is encrypted and saved as encrypted_shared_secret. No spaces are permitted.
			encrypted_shared_secret	R/W		This holds the encrypted shared secret. When empty the legacy unencrypted shared secret is used instead.
			interim_interval	R/W		If an accountant server is used, this value defines the interval between accounting updates. Set to 0 to disable this function.

7.4 RADIUS Configuration Parameters

Group	server , dynamical size
Path	Management.RADIUS.server
Description	This dynamic table is used to specify access parameter to authentication servers using RADIUS or TACACS+.
name	<p>Unique name used to identify the server. Used for reference in Port-based Access Control configuration.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.69.1.1.2 (serverName) 1.3.6.1.2.1.67.1.1.1.1.1.0 (radiusAuthServIdent)</p>
server_type	<p>Flags if RADIUS or TACACS+ is specified in this entry.</p> <p>Values <i>RADIUS</i> This is a RADIUS server entry <i>TACACS</i> This is a TACACS+ server entry</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.69.1.1.3 (serverServerType)</p>
host_address	<p>IP address or symbolic name of the authentication server. IPv4 or IPv6 with lower case letter is acceptable</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.69.1.1.4 (serverHostAddress) 1.3.6.1.2.1.67.1.2.1.1.3.1.2 (radiusAuthServerAddress)</p>
udp_port	<p>UDP port for RADIUS authentication service. Standard port is 1812. For TACACS+ this specifies the TCP port which defaults to 49.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.69.1.1.5 (serverUdpPort) 1.3.6.1.2.1.67.1.2.1.1.3.1.3 (radiusAuthClientServerPortNumber)</p>
shared_secret	<p>Shared Secret as common password between authenticator and server. THIS FIELD IS DEPRACATED. Provided for backward compatibility. Use the secure enter_shared_secret command instead.</p> <p>Value String, max. 256 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.69.1.1.6 (serverSharedSecret) 1.3.6.1.2.1.67.2.1.1.1.14.1 (radiusAccClientEntry)</p>
enter_shared_secret	<p>Set a shared secret as common password between authenticator and server. The input is encrypted and saved as encrypted_shared_secret. No spaces are permitted.</p> <p>Action Excecute command with parameter string max. 256 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.69.1.1.7 (serverEnterSharedSecret)</p>

encrypted_shared_secret	This holds the encrypted shared secret. When empty the legacy unencrypted shared secret is used instead.
Value	String, max. 256 characters.
OID	1.3.6.1.4.1.3181.10.6.3.69.1.1.8 (serverEncryptedSharedSecret)

interim_interval	If an accountant server is used, this value defines the interval between accounting updates. Set to 0 to disable this function.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.3.69.1.1.9 (serverInterimInterval)

8 Network Time Protocol (NTP)

8.1 Key Features

NTP Client

Network time is automatically retrieved from NTP server. Two NTP server may be specified. The clock may also manually be set if NTP access is not desired.

Time handling is automatic provided network access is granted.

8.2 Functional Description

Internal Real Time Clock

The management agent includes a precision real time clock that can be automatically synchronized with external time servers.

If no time server is available, the real time clock can also be manually set via System group parameters.

External Time Server Synchronization

The device internal real time clock can be synchronized with external time servers using NTP (Network Time Protocol). When enabled, the system requests at boot time the configured NTP time server and sets the internal real time clock parameters for time and date accordingly.

If the configured main NTP server does not answer, after a timeout period an alternative backup NTP server is requested.

If this also fails, the internal real time clock remains unchanged and should be adjusted manually.

For a permanent resynchronization, a time interval can be defined in which the NTP server is requested.

Localisation

As an external time server does not know where the requesting device is located, it always provides the UTC time (Universal Time Coordinated). For the correct local time value, the local time zone must be configured. Daylight saving is automatically derived from the time zone and date information and applied to the local time.

8.3 NTP CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Management.						
	ntp.					Network Time Protocol (NTP)
			enable_ntp		R/W	When enabled the local clock will be synchronized with the time provided by a time server.
			sync_now		X	Action command to read time server now and setup the internal clock.
			dhcp_provides_ntp_server		R/W	Enable DHCP to automatically retrieve NTP server address(es). When disabled, the locally defined addresses are used instead.
			main_ntp_server		R/W	This is the preferred NTP server address. IP address or symbolic name may be used. IPv4 or IPv6 (with lower case letters) is acceptable.
			backup_ntp_server		R/W	This defines an optional alternate NTP server address. IP address or symbolic name may be used. IPv4 or IPv6 (with lower case letters) is acceptable.
			trusted_server		R/W	Some NTP server (Windows) indicate a too large deviation or indicate they are unreliable when they are not externally synchronized. To be able to still use such a server set this option to true.
			sync_interval		R/W	Resynchronization interval (minutes), default once per day.
			show_time_date		X	Show system time and date.
			list_time_zones		X	Displays a long list of available time zones. Pick the time zone that matches your location and use this name for the time_zone parameter.
			time_zone		R/W	Enter a string exactly as obtained via list_time_zones command. Note that a change of the time zone if only effective after a system reboot.

time_format	R/W	This parameter permits definition of the time format displayed under <code>ntp.local_time</code> . When left blank the default format <code>hrs:min:sec</code> is used. The parameter follows the Linux date command syntax. Please refer to external documentation for details. Use <code>%k:%M</code> for time without seconds. Use <code>%P</code> to add AM/PM where is applies. There are more options.
date_format	R/W	This parameter permits definition of the data format displayed under <code>ntp.local_date</code> . When left blank the default format <code>year-month-date</code> is used. The parameter follows the Linux date command syntax. Please refer to external documentation for details. It is also possible to add weekday <code>%A</code> or month <code>%B</code> or week of year <code>%V</code> , etc.
status	R	Indicates by which means the clock was last set.
local_time	R	Displays the current local date according to selected time zone in the format defined user <code>ntp.time_format</code> .
local_date	R	Displays the current local date according to selected time zone in the format defined user <code>ntp.date_format</code> .
used_ntp_server	R	Actually used NTP server IP address or name
dynamic_ntp_server_1	R	Main dynamically assigned NTP server IP address.
dynamic_ntp_server_2	R	Alternate dynamically assigned NTP server IP address.
dynamic_ntp_server_3	R	Alternate dynamically assigned NTP server IP address.
dynamic_ntp_server_4	R	Alternate dynamically assigned NTP server IP address.

8.4 NTP Configuration Parameters

Group Path	General Parameters Management.NTP
enable_ntp	<p>When enabled the local clock will be synchronized with the time provided by a time server.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.73.1 (ntpEnableNtp)</p>
sync_now	<p>Action command to read time server now and setup the internal clock.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.73.2 (ntpSyncNow)</p>
dhcp_provides_ntp_server	<p>Enable DHCP to automatically retrieve NTP server address(es). When disabled, the locally defined addresses are used instead.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.73.3 (ntpDhcpProvidesNtpServer)</p>
main_ntp_server	<p>This is the preferred NTP server address. IP address or symbolic name may be used. IPv4 or IPv6 (with lower case letters) is acceptable.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.73.4 (ntpMainNtpServer)</p>
backup_ntp_server	<p>This defines an optional alternate NTP server address. IP address or symbolic name may be used. IPv4 or IPv6 (with lower case letters) is acceptable.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.73.5 (ntpBackupNtpServer)</p>
trusted_server	<p>Some NTP server (Windows) indicate a too large deviation or indicate they are unreliable when they are not externally synchronized. To be able to still use such a server set this option to true.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.73.6 (ntpTrustedServer)</p>
sync_interval	<p>Resynchronization interval (minutes), default once per day.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.73.7 (ntpSyncInterval)</p>
show_time_date	<p>Show system time and date.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.73.8 (ntpShowTimeDate)</p>

list_time_zones	<p>Displays a long list of available time zones. Pick the time zone that matches your location and use this name for the time_zone parameter.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.73.9 (ntpListTimeZones)</p>
time_zone	<p>Enter a string exactly as obtained via list_time_zones command. Note that a change of the time zone is only effective after a system reboot.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.73.10 (ntpTimeZone)</p>
time_format	<p>This parameter permits definition of the time format displayed under ntp.local_time. When left blank the default format hrs:min:sec is used. The parameter follows the Linux date command syntax. Please refer to external documentation for details. Use %k:%M for time without seconds. Use %P to add AM/PM where it applies. There are more options.</p> <p>Value String, max. 64 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.73.11 (ntpTimeFormat)</p>
date_format	<p>This parameter permits definition of the data format displayed under ntp.local_date. When left blank the default format year-month-date is used. The parameter follows the Linux date command syntax. Please refer to external documentation for details. It is also possible to add weekday %A or month %B or week of year %V, etc.</p> <p>Value String, max. 64 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.73.12 (ntpDateFormat)</p>

8.5 NTP Status Parameters

Group Path	General Parameters Management.NTP										
status	<p>Indicates by which means the clock was last set.</p> <p>Values</p> <table> <tr> <td><i>UNSET</i></td><td>The real time clock is not set</td></tr> <tr> <td><i>MANUALLY_SET</i></td><td>The clock was set via set_time command</td></tr> <tr> <td><i>SYNCHRONIZED</i></td><td>The clock is synchronized with an NTP server</td></tr> <tr> <td><i>SYNC_FAILED</i></td><td>Synchronization with the NTP server has failed</td></tr> <tr> <td><i>DAY_LIGHT_SAVING_TIME</i></td><td>Daylight saving time is active</td></tr> </table> <p>OID 1.3.6.1.4.1.3181.10.6.3.73.100 (ntpStatus)</p>	<i>UNSET</i>	The real time clock is not set	<i>MANUALLY_SET</i>	The clock was set via set_time command	<i>SYNCHRONIZED</i>	The clock is synchronized with an NTP server	<i>SYNC_FAILED</i>	Synchronization with the NTP server has failed	<i>DAY_LIGHT_SAVING_TIME</i>	Daylight saving time is active
<i>UNSET</i>	The real time clock is not set										
<i>MANUALLY_SET</i>	The clock was set via set_time command										
<i>SYNCHRONIZED</i>	The clock is synchronized with an NTP server										
<i>SYNC_FAILED</i>	Synchronization with the NTP server has failed										
<i>DAY_LIGHT_SAVING_TIME</i>	Daylight saving time is active										
local_time	<p>Displays the current local date according to selected time zone in the format defined user ntp.time_format.</p> <p>Value String, max. 64 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.73.101 (ntpLocalTime)</p>										
local_date	<p>Displays the current local date according to selected time zone in the format defined user ntp.date_format.</p> <p>Value String, max. 64 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.73.102 (ntpLocalDate)</p>										
used_ntp_server	<p>Actually used NTP server IP address or name</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.73.103 (ntpUsedNtpServer)</p>										
dynamic_ntp_server_1	<p>Main dynamically assigned NTP server IP address.</p> <p>Format IPv4 Address ddd.ddd.ddd.ddd (ddd = decimal number between 000 to 255)</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.73.104 (ntpDynamicNtpServer1)</p>										
dynamic_ntp_server_2	<p>Alternate dynamically assigned NTP server IP address.</p> <p>Format IPv4 Address ddd.ddd.ddd.ddd (ddd = decimal number between 000 to 255)</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.73.105 (ntpDynamicNtpServer2)</p>										

dynamic_ntp_server_3 Alternate dynamically assigned NTP server IP address.

Format IPv4 Address
ddd.ddd.ddd.ddd
(*ddd* = decimal number between 000 to 255)

OID 1.3.6.1.4.1.3181.10.6.3.73.106 (ntpDynamicNtpServer3)

dynamic_ntp_server_4 Alternate dynamically assigned NTP server IP address.

Format IPv4 Address
ddd.ddd.ddd.ddd
(*ddd* = decimal number between 000 to 255)

OID 1.3.6.1.4.1.3181.10.6.3.73.107 (ntpDynamicNtpServer4)

9 File Operations

9.1 Key Features

File Transfer Protocols

File transfers may be used to upgrade the software or to load configuration or script files. The unit supports TFTP, FTP, SFTP, HTTP, HTTPS transfer protocols. Additionally files may be loaded via DHCP directives. The device can act as server or client for FTP, SFTP, FTPS and TFTP.

Numerous file transfer protocols are available. Choose secure versions for privacy, disable unsecure versions.

Firmware Download

Software download can be complete or incremental. The download is independent of its activation. Several firmware versions may reside on the SD card in parallel.

Firmware update is very flexible and independent of actual activation.

Secure Firmware Update

Secure firmware update with encrypted and digitally signed upgrade files. A flexible update mechanism permits customized upgrade files if required. Configuration remains intact after firmware upgrade

By accepting only signed upgrades malware cannot be loaded into the system.

Firmware and Configuration Export and Import

(Industrial Switch only)

Firmware update files and configuration files may be exported and re-imported by another unit via DOS formatted USB memory stick.

This can simplify device duplication when network access is not available.

Script Files

CLI script files may be up and downloaded in the same way as other files. This way for example a network wide special configuration can be distributed.

Scripting may be used to customize the configuration or operation.

Configuration Files

All device configurations are stored in XML files. These may be edited offline (CLI - offline mode) and then be distributed to other devices. Configuration files may be backed up to keep a save copy. A custom factory default configuration may be configured.

State-of-the-Art configuration scheme permits highest flexibility for distribution and storage.

Compare Config and create Transformation Scripts

Device configurations may be compared to view differences. Scripts file are generated that permit automated transformation of one config to another.

State-of-the-Art configuration scheme permits automated bulk configuration updates without losing device specific settings.

Temporary Configuration

Usually, the device configuration should be saved permanently. For some applications like public kiosk systems it is desirable to only temporarily activate a configuration and start afresh with the next user.

Permits reliable use in public network designs.

9.2 Functional Description

The switch has an internal filing system to store CLI scripts, configurations and firmware images and updates. These files can be accessed via standard file transfer protocols (TFTP, FTP, SFTP). To access to the files, the switch can act as client or server.

File access using remote server

When acting as client, the switch can download or upload the files to a remote TFTP/FTP/SFTP server. Before using this method, the corresponding client service must be enabled via 'client.enable_pppp', where 'pppp' stands for the protocol to be used (TFTP/FTP/SFTP). Remote servers can then be accessed using the 'download_from_server' or 'upload_to_server' commands.

File access using remote client

When acting as server, the switch files can be downloaded or uploaded via a remote TFTP/FTP/SFTP client. Before using this method, the corresponding server service must be enabled via 'server.enable_pppp', where 'pppp' stands for the protocol to be used (TFTP/FTP/SFTP). Use a standard file transfer client software (e.g. 'FileZilla') to access the switch internal files.

CLI script files

Sequences of CLI commands to be executed can be stored in script files. When these scripts are executed, the result is identical to manually entering these commands at the CLI prompt. See Section 'Command Line Interface' for a detailed description how these scripts can be generated from CLI output.

Configuration files

The configuration of all switch parameters is stored in XML files, one for each feature-group (e.g. port-specific functions or Spanning Tree Protocol). There can be multiple folders to store different configurations on the device.

Using the 'backup_to_folder', the running configuration can be saved to a folder. The 'restore_from_folder' command retrieves a stored configuration from a folder to the running configuration.

Firmware images and update files

Firmware images or updates are stored in single files. These files can be downloaded from remote servers. Before installing an update, the release information can be displayed. With the 'install_software_update' command, a downloaded update file can be installed to the system.

While installing a firmware update to system the 'on' LED is static green and 'sys' LED is flashing orange. Port 1 to 5 'link' LEDs are blinking blue and changing to static blue one after the other to indicate progress as follows:

LED 'link'	State	Description
------------	-------	-------------

P1	blinking	Preparing update and stopping services
P2	blinking	Create backup of existing config
P3	blinking	Extract and copy new files
P4	blinking	Restoring configuration
P5	blinking	Cleanup
P1 to 5	static	Done.

Depending on update type the switch may perform a hardware reboot before returning to normal function.

9.3 Files CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Management.						
		files.				File transfer is used to store and load configuration, script and log files and for software upgrades.
		apps.				This section defines commands to view, load and install apps. The files are also accessible via ftp in the apps directory.
			list_installed_apps		X	Lists which apps are actually installed and ready for use.
			show_notes		X	Displays information about an app . The app does not need to be installed for this operation. Syntax: show_notes = appname
			display_files		X	Displays a list of all available app installation files.
			delete_file		X	Deletes a previously downloaded app installation file. This does not affect unit operation.
			download		X	Apps can be downloaded using various protocols. The downloaded app will not be activated until requested using the install command. Example: download = ftp://name:passwd@machine.domain:port/full/path/to/appfile.app Type = without parameter for additional online help.
			list_media_files		X	Display a list of all app files available on the external media in the apps folder.
			export_to_media		X	The function depends on the type of device. On devices with USB port this action copies to an inserted memory stick. On a micro switch running from internal memory this action copies to an optional DOS formatted SD card. On all other switch versions this action will do nothing. When applicable this action copies the specified app file onto the removable media. If the file already exists it is overwritten. Syntax: export_to_media = appname

import_from_media	X	The function depends on the type of device. On devices with USB port this action imports the specified config from an inserted memory stick. On a micro switch running from internal memory this imports the specified config from a DOS formatted SD card. On all other switch versions this action will do nothing. When applicable this action imports the specified app installation file. If the app file name already exists the file is overwritten. Any already running version of the app is not affected. To actually install the imported app use the install command. Syntax: import_from_media = app_file
install	X	Installs the app as contained in the .app installation file. Syntax: install = myapp.msapp. The .msapp suffix may be omitted. Just typing the app file name (with correct capitalization) will automatically select the latest version available on the device. To update an app simply install the new version without deinstallation first. This will keep the app configuration intact (as far as the app parameter are identical between versions).
patch	X	Patches an installed app with the data contained in the supplied .app installation file. Syntax: patch = myapp.msapp. The .app suffix may be omitted. Just typing the app name (with correct capitalization) will automatically select the latest version available on the device. IMPORTANT: Only use patch (instead of install) when it is clear that not changes to the parameter structure have been made between the current and the new version. The patch command only copies scripts, image and sound data, but does not make configuration backups etc. It is intended for quick upgrade of script code or to add new images etc. Note: The same .app file is used for install or patch command.
deinstall	X	Deinstalls the specified app. The app will no longer be active and all configuration and status entries will be removed. The .app file itself is retained for possible future re-installation. Syntax: deinstall = appname. Note there is no need to deinstall prior to installing an update.
scripts.		This section defines commands to manipulate scripts. Sub-folders are permitted. The files are also accessible via ftp in the xml_cli_scripts directory.
list_files	X	Displays a list of all available script files, their size and date of last change.
show_file	X	Displays the content of a script file. In order to edit a file please use the EditScriptFile command.

execute	X	Executes the script file supplied. Example: files.scripts.execute = myscript or ..execute = myfolder/myscript. It also possible to execute a specific subroutine and even to supply parameter to it. Syntax: script:subroutine par1 par2. Parameter with spaces can be enclosed with curly brackets.
download_from_server	X	A script can be downloaded from a server. Example: download_from_server = ftp://name:passwd@machine.domain:port/full/path/to/scriptfile. A local file with same name is overwritten. Type = without parameter for additional online help.
upload_to_server	X	A script file can be uploaded to a foreign server. Syntax: upload_to_server = scriptfile ftp://user:passwd@ftp.upload.com/target_folder/. Append verbose to the command to start a verbose transfer for trouble shooting. Type = without parameter for additional online help.
copy_file	X	Copies an existing script file to another file. Example: copy_file = MyScript NewScript. Do not use whitespace in the new file name.
delete_file	X	Deletes a script file. Careful, there is no undelete.
terminate	X	This action command can be used to terminate (stop) a background script. This may also be used to terminate a script with an endless loop or a too long wait timer. Syntax: files.scripts.terminate = scriptname or files.scripts.terminate = app/scriptname.
scriptdata.		This section defines commands to manipulate data files created by or to be used by script programs or certain apps. For example script generated log data. The files are also accessible via ftp in the script_data directory.
list_files	X	Displays a list of all available data files.
show_file	X	Displays the content of a data file. A text format is assumed. The files cannot not be edited via CLI or the embedded editor within the CLI.
download_from_server	X	A data file can be downloaded. Various protocols may be used. Example: download_from_server = ftp://name:passwd@machine.domain:port/full/path/to/scriptfile. A possible existing local file with same name is overwritten. Type = without parameter for additional online help.
upload_to_server	X	A script data file can be uploaded. Various protocols may be used. Example: upload_to_server = scriptfile ftp://user:passwd@ftp.upload.com/ Type = without parameter for additional online help.
copy_file	X	Copies an existing data file to another file. Example: copy_file = MyData NewData. Do not use whitespace in the new file name.

delete_file	X	Deletes a data file. It does not delete a script file. There is no undelete!
list_media_files	X	Display a list of all files available on the external media in the script_data folder.
export_to_media	X	The function depends on the type of device. On devices with USB port this action copies to an inserted memory stick. On a micro switch running from internal memory this action copies to an optional DOS formatted SD card. On all other switch versions this action will do nothing. When applicable this action copies the specified script_data file(s) onto the removable media. If the file(s) already exists it is overwritten. Syntax: export_to_media = filename Wildcard * is supported to copy many files at once.
import_from_media	X	The function depends on the type of device. On devices with USB port this action imports the specified config from an inserted memory stick. On a micro switch running from internal memory this imports the specified config from a DOS formatted SD card. On all other switch versions this action will do nothing. When applicable this action imports the specified files to the script_data folder. If the file(s) already exists they are overwritten. Syntax: import_from_media = filename.
configuration.		This section defines commands to load and store the system configuration. The configuration files are also accessible via ftp under the config directory.
list_folders	X	Displays a list of all available configuration folders.
backup_to_folder	X	Copies running configuration to a new or existing folder. If the folder name already exists the previous configuration is overwritten. Syntax: backup_to_folder = my_new_config
restore_from_folder	X	Restores and activates the specified user configuration. Each resulting config change will be logged as usual. Specify source folder. Syntax: restore_from_folder = folder_name. Important: This command does not restore the IP and factory configuration files.
commit_config	X	Commits the config to SD card now. Data are otherwise autosaved using a timer. Use this command to speed up the process. Syntax: commit_config = folder_name. Special case: 'commit_config =' will be automatically extended to 'running' to immediately save the currently running configuration. Use this command to permanently store the configuration while system.config_save_mode = TEMPORARILY is selected.

compare_configuration	X	Compares two configurations and creates CLI script file that can transform the configurations to each other. Syntax: compare_configuration = (with no argument behind =) compares running config against factory config (as defined by factory_default_folder). compare_configuration = somename compares config somename against factory_default_folder. compare_configuration = somename someothername compares the two named configurations. Special names are factory (factory defaults) and running (currently active configuration).
copy_folder	X	Copies one user config to another. The config will not be activated. Do not use whitespace for the new configuration name.
delete_folder	X	Deletes the specified user config. There is no undelete !
download_from_server	X	A configuration packed as tar or gztar file can be downloaded to a custom folder. Example: download_from_server = local_config_name ftp://name:passwd@machine.domain/full/path/to/config_file The downloaded config is not automatically activated. Type = without parameter for additional online help.
upload_to_server	X	The content of the specified configuration folder is compressed into a single file (in tar.gz format) and then uploaded to a server. Various protocols may be used. Example: upload_to_server = folder ftp://user:passwd@ftp.upload.com/dir/ Note the trailing / is mandatory for ftp. Instead of a hostname an IP address may be specified. Instead of ftp other transport formats like tftp or http can be specified. The saved file will be prefixed by the local IP address of the sending device. Type = without parameter for additional online help.
list_media_folders	X	Display a list of all configuration folders available on the external media.
export_to_media	X	The function depends on the type of device. On devices with USB port this action copies to an inserted memory stick. On a micro switch running from internal memory this action copies to an optional DOS formatted SD card. On all other switch versions this action will do nothing. When applicable this action copies the specified configuration folder to a new or existing folder on the removable media. If the folder name already exists the previous configuration is overwritten. Syntax: export_media = running (This example copies the actively running config to folder config/running)

import_from_media	X	The function depends on the type of device. On devices with USB port this action imports the specified config from an inserted memory stick. On a micro switch running from internal memory this imports the specified config from a DOS formatted SD card. On all other switch versions this action will do nothing. When applicable this action imports the specified configuration to a new or existing user folder. If the folder name already exists the previous configuration is overwritten. The config folder must be located under config/name to be detected. Note that when a reserved name like running is imported, the folder is imported as running_imported. To actually activate the imported config use the restore_from_folder action. Syntax: import_from_media = my_new_config
factory_default_folder	R/W	This parameter permits the definition of a customer specific alternative factory configuration. Care must be taken to create the desired folder beforehand via download or the backup_to_folder command.
force_factory_default	X	This forcibly overwrites the current configuration with the factory files bypassing regular processing. This is intended for service personnel only and requires special permission. For normal return to factory settings please use restore_from_folder = factory command.
firmware.		This section defines commands to view, load and update the system firmware.
list_installed_versions	X	Lists detailed version information of individual system programs.
display_files	X	Displays a list of all available software files.
delete_file	X	Deletes a previously downloaded firmware file. This does not affect unit operation.
download	X	Complete updates or patches can be downloaded using various protocols. The downloaded files will not be activated until requested using the install_software_update command. Example: download = ftp://name:passwd@machine.domain:port/full/path/to/firmwarefile. Type = without parameter for additional online help.
verify_update_file	X	Verifies the software contained in the update file specified as parameter. Syntax: verify_update_file = newcode.msu The file will not be installed, just verified.
show_release_notes	X	Use to read information about a particular software archive file. Syntax: show_release_notes = filename
install_software_update	X	Installs the software as contained in the update file specified as parameter. Syntax: install_software_update = newcode.msu NOTE: the unit may automatically reboot after the installation.
list_media_files	X	Display a list of all firmware files available on the external media in the updates folder.

export_to_media	X	The function depends on the type of device. On devices with USB port this action copies to an inserted memory stick. On a micro switch running from internal memory this action copies to an optional DOS formatted SD card. On all other switch versions this action will do nothing. When applicable this action copies the specified firmware update file (msu) onto the removable media. If the file already exists it is overwritten. Syntax: export_media = u_10_3_3.msu
import_from_media	X	The function depends on the type of device. On devices with USB port this action imports the specified config from an inserted memory stick. On a micro switch running from internal memory this imports the specified config from a DOS formatted SD card. On all other switch versions this action will do nothing. When applicable this action imports all firmware update files (msu files) located in the root directory of the media. No parameter are required. Syntax: import_from_media
mirror_sd_card	X	The function mirrors the whole content of the SD card into the internal flash memory of a micro switch with internal memory. This command only executes when the device is currently running on the SD card to be copied. On switch versions without internal memory nothing will happen. There are two options. OVERWRITE: All data previously stored in the internal memory, including config and passwords, is overwritten. Possibly existing custom configurations or scripts are retained. REPLACE: The internal memory is first erased before the copy commences. Any existing data are removed. This assures are clean copy of the SD card without possible extra data being retained. Note: The mirror command will not operate when system.boot_preference is set to INTERN_ONLY to safeguard the device against an illegally inserted SD card. Syntax: mirror_sd_card = OVERWRITE (or REPLACE) (uppercase).
certificate.		This section defines commands use private SSL certificate for secure web access.
list_files	X	Displays a list of all custom certificates available.
download_from_server	X	Custom certificate files can be downloaded. Various protocols may be used. Example: download_from_server = ftp://name:passwd@machine.domain:port/full/path/to/certificatefile. A possible local file with same name is overwritten. Type = without parameter for additional online help.
upload_to_server	X	Custom certificate files can be uploaded. Various protocols may be used. Example: upload_to_server = certificate_file ftp://user:passwd@ftp.upload.com/ Type = without parameter for additional online help.

delete_file	X	Deletes an individual certificate file. The full name must be specified.
activate_for_web	X	Activates the specified certificate to become active immediately for https. Syntax: activate_for_web = target certificate_name. Use target: CRT or KEY. Expects 'certificate_name.crt' and 'certificate_name.key' in certificate directory and optionally 'certificate_name.chain.crt' to be used as chain certificate file.
deactivate_for_web	X	Deactivates the specified target certificate for the web interface. Syntax: deactivate_for_web = target. Use target: CRT or KEY. No certificate name is required. The certificate is not deleted, it is just not used anymore.
activate_for_supplciant	X	Activates the specified certificate to become active immediately for the supplciant. Syntax: activate_for_supplciant = target certificate_name. Use target: CA, LOCAL or KEY. Expects existing certificate file name.
deactivate_for_supplciant	X	Deactivates the specified target certificate for the supplciant. Syntax: deactivate_for_supplciant = target. Use target: CA, LOCAL or KEY. No certificate name is required. The certificate is not deleted, it is just not used anymore.
activate_for_snmp	X	Activates the specified certificate to become active for snmp v3 in TSM mode. Syntax: activate_for_snmp = AGENT certificate_name or activate_for_snmp = MANAGER certificate_name user_name. The user name must exist as a local user (See management.acess.user). Several user can be assigned to the same certificate. Expects an existing certificate file name and key file with same name. Enable TSM module in SNMP.v3_config.security_model.
deactivate_for_snmp	X	Deactivates the specified target certificate for snmp v3. Syntax: deactivate_for_snmp = AGENT or deactivate_for_snmp = MANAGER certificate_name username. The username is optional. When omitted, then all user assigned to the specified MANAGER certificate are deactivated. The certificate is not deleted, it is just not used anymore.
activate_for_mqtt	X	Activates the specified certificate to become active immediately for MQTT. Syntax: activate_for_mqtt = target certificate_name. Use target: CRT or KEY. Expects 'certificate_name.crt' and 'certificate_name.key' in certificate directory and optionally 'certificate_name.chain.crt' to be used as chain certificate file.
deactivate_for_mqtt	X	Deactivates the specified target certificate for MQTT. Syntax: deactivate_for_mqtt = target. Use target: CRT or KEY. No certificate name is required. The certificate is not deleted, it is just not used anymore.

view_active_certificates	X	Displays the content of all currently active certificates.
license.		This section defines commands install, active and check software licensing files.
list_files	X	Displays a list of all licenses installed.
show_file	X	Displays the content of a selected license file. License files are human readable. Be aware that any manual change to then will invalidate the signature.
download_from_server	X	License files can be downloaded. Various protocols may be used. Example: download_from_server = ftp://name:passwd@machine.domain:port/ full/path/to/certificatefile. A possible local file with same name is overwritten. Type = without parameter for additional online help.
delete_file	X	Deletes an individual license file. The full name must be specified.
activate	X	Activates all available licenses to become active immediately. No parameter are required. Licenses are also activated upon system start.
view_active_licenses	X	Displays a summary of all licenses and their expiration dates.
history.		This section defines commands to access the history files created of history logging is enabled. The files are also accessible via ftp in the history directory.
list_files	X	Displays a list of all available history files.
show_file	X	Displays the content of a history file. The files cannot not be edited via CLI or the embedded editor within the CLI.
upload_to_server	X	A script data file can be uploaded. Various protocols may be used. Example: upload_to_server = file ftp://user:passwd@ftp.upload.com/ Type = without parameter for additional online help.
copy_file	X	Copies an existing history data file to another file. Example: copy_file = history_file backup_name. Do not use whitespace in the new file name.
delete_file	X	Deletes a history file. When a file is deleted, which is still updated by the history process, then a new file started as soon as the next history update cycle starts.
list_media_files	X	Display a list of all history files available on the external media in the history folder.

export_to_media	X	The function depends on the type of device. On devices with USB port this action copies to an inserted memory stick. On a micro switch running from internal memory this action copies to an optional DOS formatted SD card. On all other switch versions this action will do nothing. When applicable this action copies the specified history files onto the removable media. If a file already exists it is overwritten. Syntax: export_media = filename. Wildcard * may be used to select several files at once. Example: temperature_day_2017_11* to get all files of November.
logfiles.		This section permits read access to various system log files. The files are also accessible via ftp in the logs directory.
list_files	X	Displays a list of all available log files.
show_file	X	Displays the content of a log file. The files cannot not be edited via CLI or the embedded editor within the CLI.
show_last_update_log	X	Displays the last firmware update logfile.
upload_last_snapshot	X	A system snapshot contains all data required for comprehensive offsite troubleshooting. A snapshot can be created under Device.system.create_snapshot. Use the upload command to send the result to a remote system. Example: upload_last_snapshot = ftp://user:passwd@ftp.upload.com/ Type = without parameter for additional online help.
export_to_media	X	The function depends on the type of device. On devices with USB port this action copies to an inserted memory stick. On a micro switch running from internal memory this action copies to an optional DOS formatted SD card. On all other switch versions this action will do nothing. When applicable this action copies all log files onto the removable media.
server.		The different file transfer protocols may individually be enabled or disabled for protection.
enable_tftp	R/W	Enable TFTP server for file up-/download.
enable_ftp	R/W	Enable FTP server for file up-/download.
enable_sftp	R/W	Enable SFTP server for file up-/download. Note SFTP also requires SSH to be enabled (see CLI settings). TCP/IP Port 8022 is used.
enable_api	R/W	Enable API server for dotstring management via https.
enable_rest	R/W	Enable REST api server for dotstring management via https.
enable_json_rpc	R/W	Enable JSON/RPC interface for M2M management via https.

9.4 Files Configuration Parameters

Group	apps
Path	Management.Files.apps
Description	This section defines commands to view, load and install apps. The files are also accessible via ftp in the apps directory.
list_installed_apps	<p>Lists which apps are actually installed and ready for use.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.1.1.2 (appsListInstalledApps)</p>
show_notes	<p>Displays information about an app . The app does not need to be installed for this operation. Syntax: show_notes = appname</p> <p>Action Execute command with parameter string max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.1.1.3 (appsShowNotes)</p>
display_files	<p>Displays a list of all available app installation files.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.1.1.4 (appsDisplayFiles)</p>
delete_file	<p>Deletes a previously downloaded app installation file. This does not affect unit operation.</p> <p>Action Execute command with parameter string max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.1.1.5 (appsDeleteFile)</p>
download	<p>Apps can be downloaded using various protocols. The downloaded app will not be activated until requested using the install command. Example: download = ftp://name:passwd@machine.domain:port/full/path/to/appfile.app Type = without parameter for additional online help.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.1.1.6 (appsDownload)</p>
list_media_files	<p>Display a list of all app files available on the external media in the apps folder.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.1.1.7 (appsListMediaFiles)</p>
export_to_media	<p>The function depends on the type of device. On devices with USB port this action copies to an inserted memory stick. On a micro switch running from internal memory this action copies to an optional DOS formatted SD card. On all other switch versions this action will do nothing. When applicable this action copies the specified app file onto the removable media. If the file already exists it is overwritten. Syntax: export_to_media = appname</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.1.1.8 (appsExportToMedia)</p>

import_from_media The function depends on the type of device. On devices with USB port this action imports the specified config from an inserted memory stick. On a micro switch running from internal memory this imports the specified config from a DOS formatted SD card. On all other switch versions this action will do nothing. When applicable this action imports the specified app installation file. If the app file name already exists the file is overwritten. Any already running version of the app is not affected. To actually install the imported app use the install command. Syntax: `import_from_media = app_file`

Action Execute command with parameter string max. 128 characters.

OID 1.3.6.1.4.1.3181.10.6.3.72.1.1.9 (appsImportFromMedia)

install Installs the app as contained in the .app installation file. Syntax: `install = myapp.msapp`. The .msapp suffix may be omitted. Just typing the app file name (with correct capitalization) will automatically select the latest version available on the device. To update an app simply install the new version without deinstallation first. This will keep the app configuration intact (as far as the app parameter are identical between versions).

Action Execute command with parameter string max. 32 characters.

OID 1.3.6.1.4.1.3181.10.6.3.72.1.1.10 (appsInstall)

patch Patches an installed app with the data contained in the supplied .app installation file. Syntax: `patch = myapp.msapp`. The .app suffix may be omitted. Just typing the app name (with correct capitalization) will automatically select the latest version available on the device. **IMPORTANT:** Only use patch (instead of install) when it is clear that not changes to the parameter structure have been made between the current and the new version. The patch command only copies scripts, image and sound data, but does not make configuration backups etc. It is intended for quick upgrade of script code or to add new images etc. Note: The same .app file is used for install or patch command.

Action Execute command with parameter string max. 32 characters.

OID 1.3.6.1.4.1.3181.10.6.3.72.1.1.11 (appsPatch)

deinstall Deinstalls the specified app. The app will no longer be active and all configuration and status entries will be removed. The .app file itself is retained for possible future re-installation. Syntax: `deinstall = appname`. Note there is no need to deinstall prior to installing an update.

Action Execute command with parameter string max. 32 characters.

OID 1.3.6.1.4.1.3181.10.6.3.72.1.1.12 (appsDeinstall)

Group	scripts
Path	Management.Files.scripts
Description	This section defines commands to manipulate scripts. Sub-folders are permitted. The files are also accessible via ftp in the xml_cli_scripts directory.

list_files	<p>Displays a list of all available script files, their size and date of last change.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.2.1.2 (scriptsListFiles)</p>
show_file	<p>Displays the content of a script file. In order to edit a file please use the EditScriptFile command.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.2.1.3 (scriptsShowFile)</p>
execute	<p>Executes the script file supplied. Example: files.scripts.execute = myscript or ..execute = myfolder/myscript. It also possible to execute a specific subroutine and even to supply parameter to it. Syntax: script:subroutine par1 par2. Parameter with spaces can be enclosed with curly brackets.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.2.1.4 (scriptsExecute)</p>
download_from_server	<p>A script can be downloaded from a server. Example: download_from_server = ftp://name:passwd@machine.domain:port/full/path/to/scriptfile. A local file with same name is overwritten. Type = without parameter for additional online help.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.2.1.5 (scriptsDownloadFromServer)</p>
upload_to_server	<p>A script file can be uploaded to a foreign server. Syntax: upload_to_server = scriptfile ftp://user:passwd@ftp.upload.com/target_folder/. Append verbose to the command to start a verbose transfer for trouble shooting. Type = without parameter for additional online help.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.2.1.6 (scriptsUploadToServer)</p>
copy_file	<p>Copies an existing script file to another file. Example: copy_file = MyScript NewScript. Do not use whitespace in the new file name.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.2.1.7 (scriptsCopyFile)</p>
delete_file	<p>Deletes a script file. Careful, there is no undelete.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.2.1.8 (scriptsDeleteFile)</p>
terminate	<p>This action command can be used to terminate (stop) a background script. This may also be used to terminate a script with an endless loop or a too long wait timer. Syntax: files.scripts.terminate = scriptname or files.scripts.terminate = app/scriptname.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.2.1.9 (scriptsTerminate)</p>

Group	scriptdata
Path	Management.Files.scriptdata
Description	This section defines commands to manipulate data files created by or to be used by script programs or certain apps. For example script generated log data. The files are also accessible via ftp in the script_data directory.
list_files	<p>Displays a list of all available data files.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.3.1.2 (scriptdataListFiles)</p>
show_file	<p>Displays the content of a data file. A text format is assumed. The files cannot not be edited via CLI or the embedded editor within the CLI.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.3.1.3 (scriptdataShowFile)</p>
download_from_server	<p>A data file can be downloaded. Various protocols may be used. Example: download_from_server = ftp://name:passwd@machine.domain:port/full/path/to/scriptfile. A possible existing local file with same name is overwritten. Type = without parameter for additional online help.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.3.1.4 (scriptdataDownloadFromServer)</p>
upload_to_server	<p>A script data file can be uploaded. Various protocols may be used. Example: upload_to_server = scriptfile ftp://user:passwd@ftp.upload.com/ Type = without parameter for additional online help.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.3.1.5 (scriptdataUploadToServer)</p>
copy_file	<p>Copies an existing data file to another file. Example: copy_file = MyData NewData. Do not use whitespace in the new file name.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.3.1.6 (scriptdataCopyFile)</p>
delete_file	<p>Deletes a data file. It does not delete a script file. There is no undelete!</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.3.1.7 (scriptdataDeleteFile)</p>
list_media_files	<p>Display a list of all files available on the external media in the script_data folder.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.3.1.8 (scriptdataListMediaFiles)</p>

export_to_media	<p>The function depends on the type of device. On devices with USB port this action copies to an inserted memory stick. On a micro switch running from internal memory this action copies to an optional DOS formatted SD card. On all other switch versions this action will do nothing. When applicable this action copies the specified script_data file(s) onto the removable media. If the file(s) already exists it is overwritten. Syntax: export_to_media = filename Wildcard * is supported to copy many files at once.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.3.1.9 (scriptdataExportToMedia)</p>
import_from_media	<p>The function depends on the type of device. On devices with USB port this action imports the specified config from an inserted memory stick. On a micro switch running from internal memory this imports the specified config from a DOS formatted SD card. On all other switch versions this action will do nothing. When applicable this action imports the specified files to the script_data folder. If the file(s) already exists they are overwritten. Syntax: import_from_media = filename.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.3.1.10 (scriptdataImportFromMedia)</p>
Group Path Description	<p>configuration</p> <p>Management.Files.configuration</p> <p>This section defines commands to load and store the system configuration. The configuration files are also accessible via ftp under the config directory.</p>
list_folders	<p>Displays a list of all available configuration folders.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.4.1.2 (configurationListFolders)</p>
backup_to_folder	<p>Copies running configuration to a new or existing folder. If the folder name already exists the previous configuration is overwritten. Syntax: backup_to_folder = my_new_config</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.4.1.3 (configurationBackupToFolder)</p>
restore_from_folder	<p>Restores and activates the specified user configuration. Each resulting config change will be logged as usual. Specify source folder. Syntax: restore_from_folder = folder_name. Important: This command does not restore the IP and factory configuration files.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.4.1.4 (configurationRestoreFromFolder)</p>

commit_config	<p>Commits the config to SD card now. Data are otherwise autosaved using a timer. Use this command to speed up the process. Syntax: commit_config = folder_name. Special case: 'commit_config =' will be automatically extended to 'running' to immediately save the currently running configuration. Use this command to permanently store the configuration while system.config_save_mode = TEMPORARILY is selected.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.4.1.5 (configurationCommitConfig)</p>
compare_configuration	<p>Compares two configurations and creates CLI script file that can transform the configurations to each other. Syntax: compare_configuration = (with no argument behind =) compares running config against factory config (as defined by factory_default_folder). compare_configuration = somename compares config somename against factory_default_folder. compare_configuration = somename someothername compares the two named configurations. Special names are factory (factory defaults) and running (currently active configuration).</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.4.1.6 (configurationCompareConfiguration)</p>
copy_folder	<p>Copies one user config to another. The config will not be activated. Do not use whitespace for the new configuration name.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.4.1.7 (configurationCopyFolder)</p>
delete_folder	<p>Deletes the specified user config. There is no undelete !</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.4.1.8 (configurationDeleteFolder)</p>
download_from_server	<p>A configuration packed as tar or gztar file can be downloaded to a custom folder. Example: download_from_server = local_config_name ftp://name:passwd@machine.domain/full/path/to/config_file The downloaded config is not automatically activated. Type = without parameter for additional online help.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.4.1.9 (configurationDownloadFromServer)</p>
upload_to_server	<p>The content of the specified configuration folder is compressed into a single file (in tar.gz format) and then uploaded to a server. Various protocols may be used. Example: upload_to_server = folder ftp://user:passwd@ftp.upload.com/dir/ Note the trailing / is mandatory for ftp. Instead of a hostname an IP address may be specified. Instead of ftp other transport formats like tftp or http can be specified. The saved file will be prefixed by the local IP address of the sending device. Type = without parameter for additional online help.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.4.1.10 (configurationUploadToServer)</p>

list_media_folders	Display a list of all configuration folders available on the external media.
Action	Execute command.
OID	1.3.6.1.4.1.3181.10.6.3.72.4.1.11 (configurationListMediaFolders)
export_to_media	<p>The function depends on the type of device. On devices with USB port this action copies to an inserted memory stick. On a micro switch running from internal memory this action copies to an optional DOS formatted SD card. On all other switch versions this action will do nothing. When applicable this action copies the specified configuration folder to a new or existing folder on the removable media. If the folder name already exists the previous configuration is overwritten. Syntax: export_media = running (This example copies the actively running config to folder config/running)</p>
Action	Execute command with parameter string max. 128 characters.
OID	1.3.6.1.4.1.3181.10.6.3.72.4.1.12 (configurationExportToMedia)
import_from_media	<p>The function depends on the type of device. On devices with USB port this action imports the specified config from an inserted memory stick. On a micro switch running from internal memory this imports the specified config from a DOS formatted SD card. On all other switch versions this action will do nothing. When applicable this action imports the specified configuration to a new or existing user folder. If the folder name already exists the previous configuration is overwritten. The config folder must be located under config/ name to be detected. Note that when a reserved name like running is imported, the folder is imported as running_imported. To actually activate the imported config use the restore_from_folder action. Syntax: import_from_media = my_new_config</p>
Action	Execute command with parameter string max. 128 characters.
OID	1.3.6.1.4.1.3181.10.6.3.72.4.1.13 (configurationImportFromMedia)
factory_default_folder	<p>This parameter permits the definition of a customer specific alternative factory configuration. Care must be taken to create the desired folder beforehand via download or the backup_to_folder command.</p>
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.3.72.4.1.14 (configurationFactoryDefaultFolder)
force_factory_default	<p>This forcibly overwrites the current configuration with the factory files bypassing regular processing. This is intended for service personnel only and requires special permission. For normal return to factory settings please use restore_from_folder = factory command.</p>
Action	Execute command with parameter string max. 16 characters.
OID	1.3.6.1.4.1.3181.10.6.3.72.4.1.15 (configurationForceFactoryDefault)

Group	firmware
Path	Management.Files.firmware
Description	This section defines commands to view, load and update the system firmware.
list_installed_versions	<p>Lists detailed version information of individual system programs.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.5.1.2 (firmwareListInstalledVersions)</p>
display_files	<p>Displays a list of all available software files.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.5.1.3 (firmwareDisplayFiles)</p>
delete_file	<p>Deletes a previously downloaded firmware file. This does not affect unit operation.</p> <p>Action Execute command with parameter string max. 48 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.5.1.4 (firmwareDeleteFile)</p>
download	<p>Complete updates or patches can be downloaded using various protocols. The downloaded files will not be activated until requested using the install_software_update command. Example: download = ftp://name:passwd@machine.domain:port/full/path/to/firmwarefile. Type = without parameter for additional online help.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.5.1.5 (firmwareDownload)</p>
verify_update_file	<p>Verifies the software contained in the update file specified as parameter. Syntax: verify_update_file = newcode.msu The file will not be installed, just verified.</p> <p>Action Execute command with parameter string max. 48 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.5.1.6 (firmwareVerifyUpdateFile)</p>
show_release_notes	<p>Use to read information about a particular software archive file. Syntax: show_release_notes = filename</p> <p>Action Execute command with parameter string max. 48 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.5.1.7 (firmwareShowReleaseNotes)</p>
install_software_update	<p>Installs the software as contained in the update file specified as parameter. Syntax: install_software_update = newcode.msu NOTE: the unit may automatically reboot after the installation.</p> <p>Action Execute command with parameter string max. 48 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.5.1.8 (firmwareInstallSoftwareUpdate)</p>

list_media_files	<p>Display a list of all firmware files available on the external media in the updates folder.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.5.1.9 (firmwareListMediaFiles)</p>
export_to_media	<p>The function depends on the type of device. On devices with USB port this action copies to an inserted memory stick. On a micro switch running from internal memory this action copies to an optional DOS formatted SD card. On all other switch versions this action will do nothing. When applicable this action copies the specified firmware update file (msu) onto the removable media. If the file already exists it is overwritten. Syntax: export_media = u_10_3_3.msu</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.5.1.10 (firmwareExportToMedia)</p>
import_from_media	<p>The function depends on the type of device. On devices with USB port this action imports the specified config from an inserted memory stick. On a micro switch running from internal memory this imports the specified config from a DOS formatted SD card. On all other switch versions this action will do nothing. When applicable this action imports all firmware update files (msu files) located in the root directory of the media. No parameter are required. Syntax: import_from_media</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.5.1.11 (firmwareImportFromMedia)</p>
mirror_sd_card	<p>The function mirrors the whole content of the SD card into the internal flash memory of a micro switch with internal memory. This command only executes when the device is currently running on the SD card to be copied. On switch versions without internal memory nothing will happen. There are two options. OVERWRITE: All data previously stored in the internal memory, including config and passwords, is overwritten. Possibly existing custom configurations or scripts are retained. REPLACE: The internal memory is first erased before the copy commences. Any existing data are removed. This assures a clean copy of the SD card without possible extra data being retained. Note: The mirror command will not operate when system.boot_preference is set to INTERN_ONLY to safeguard the device against an illegally inserted SD card. Syntax: mirror_sd_card = OVERWRITE (or REPLACE) (uppercase).</p> <p>Action Execute command with parameter string max. 16 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.5.1.12 (firmwareMirrorSdCard)</p>

Group	certificate
Path	Management.Files.certificate
Description	This section defines commands use private SSL certificate for secure web access.

list_files	<p>Displays a list of all custom certificates available.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.6.1.2 (certificateListFiles)</p>
download_from_server	<p>Custom certificate files can be downloaded. Various protocols may be used. Example: download_from_server = ftp://name:passwd@machine.domain:port/full/path/to/certificatefile. A possible local file with same name is overwritten. Type = without parameter for additional online help.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.6.1.3 (certificateDownloadFromServer)</p>
upload_to_server	<p>Custom certificate files can be uploaded. Various protocols may be used. Example: upload_to_server = certificate_file ftp://user:passwd@ftp.upload.com/ Type = without parameter for additional online help.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.6.1.4 (certificateUploadToServer)</p>
delete_file	<p>Deletes an individual certificate file. The full name must be specified.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.6.1.5 (certificateDeleteFile)</p>
activate_for_web	<p>Activates the specified certificate to become active immediately for https. Syntax: activate_for_web = target certificate_name. Use target: CRT or KEY. Expects 'certificate_name.crt' and 'certificate_name.key' in certificate directory and optionally 'certificate_name.chain.crt' to be used as chain certificate file.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.6.1.6 (certificateActivateForWeb)</p>
deactivate_for_web	<p>Deactivates the specified target certificate for the web interface. Syntax: deactivate_for_supplciant = target. Use target: CRT or KEY. No certificate name is required. The certificate is not deleted, it is just not used anymore.</p> <p>Action Execute command with parameter string max. 16 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.6.1.7 (certificateDeactivateForWeb)</p>
activate_for_supplciant	<p>Activates the specified certificate to become active immediately for the supplicant. Syntax: activate_for_supplciant = target certificate_name. Use target: CA, LOCAL or KEY. Expects existing certificate file name.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.6.1.8 (certificateActivateForSupplciant)</p>

deactivate_for_suppl	<p>Deactivates the specified target certificate for the supplicant. Syntax: deactivate_for_suppl = target. Use target: CA, LOCAL or KEY. No certificate name is required. The certificate is not deleted, it is just not used anymore.</p> <p>Action Execute command with parameter string max. 16 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.6.1.9 (certificateDeactivateForSuppl)</p>
----------------------	--

activate_for_snmp	<p>Activates the specified certificate to become active for snmp v3 in TSM mode. Syntax: activate_for_snmp = AGENT certificate_name or activate_for_snmp = MANAGER certificate_name user_name. The user name must exist as a local user (See management.access.user). Several user can be assigned to the same certificate. Expects an existing certificate file name and key file with same name. Enable TSM module in SNMP.v3_config.security_model.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.6.1.10 (certificateActivateForSnmp)</p>
-------------------	---

deactivate_for_snmp	<p>Deactivates the specified target certificate for snmp v3. Syntax: deactivate_for_suppl = AGENT or deactivate_for_suppl = MANAGER certificate_name username. The username is optional. When omitted, then all user assigned to the specified MANAGER certificate are deactivated. The certificate is not deleted, it is just not used anymore.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.6.1.11 (certificateDeactivateForSnmp)</p>
---------------------	---

activate_for_mqtt	<p>Activates the specified certificate to become active immediately for MQTT. Syntax: activate_for_mqtt = target certificate_name. Use target: CRT or KEY. Expects 'certificate_name.crt' and 'certificate_name.key' in certificate directory and optionally 'certificate_name.chain.crt' to be used as chain certificate file.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.6.1.12 (certificateActivateForMqtt)</p>
-------------------	--

deactivate_for_mqtt	<p>Deactivates the specified target certificate for MQTT. Syntax: deactivate_for_mqtt = target. Use target: CRT or KEY. No certificate name is required. The certificate is not deleted, it is just not used anymore.</p> <p>Action Execute command with parameter string max. 16 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.6.1.13 (certificateDeactivateForMqtt)</p>
---------------------	---

view_active_certificates	<p>Displays the content of all currently active certificates.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.6.1.14 (certificateViewActiveCertificates)</p>
--------------------------	---

Group Path Description	license Management.Files.license This section defines commands install, active and check software licensing files.
list_files	<p>Displays a list of all licenses installed.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.7.1.2 (licenseListFiles)</p>
show_file	<p>Displays the content of a selected license file. License files are human readable. Be aware that any manual change to then will invalidate the signature.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.7.1.3 (licenseShowFile)</p>
download_from_server	<p>License files can be downloaded. Various protocols may be used. Example: download_from_server = ftp://name:passwd@machine.domain:port/full/path/to/certificatefile. A possible local file with same name is overwritten. Type = without parameter for additional online help.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.7.1.4 (licenseDownloadFromServer)</p>
delete_file	<p>Deletes an individual license file. The full name must be specified.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.7.1.5 (licenseDeleteFile)</p>
activate	<p>Activates all available licenses to become active immediately. No parameter are required. Licenses are also activated upon system start.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.7.1.6 (licenseActivate)</p>
view_active_licenses	<p>Displays a summary of all licenses and their expiration dates.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.7.1.7 (licenseViewActiveLicenses)</p>
Group Path Description	history Management.Files.history This section defines commands to access the history files created of history logging is enabled. The files are also accessible via ftp in the history directory.

list_files	Displays a list of all available history files.
Action	Execute command.
OID	1.3.6.1.4.1.3181.10.6.3.72.8.1.2 (historyListFiles)
show_file	Displays the content of a history file. The files cannot not be edited via CLI or the embedded editor within the CLI.
Action	Execute command with parameter string max. 128 characters.
OID	1.3.6.1.4.1.3181.10.6.3.72.8.1.3 (historyShowFile)
upload_to_server	A script data file can be uploaded. Various protocols may be used. Example: upload_to_server = file ftp://user:passwd@ftp.upload.com/ Type = without parameter for additional online help.
Action	Execute command with parameter string max. 128 characters.
OID	1.3.6.1.4.1.3181.10.6.3.72.8.1.4 (historyUploadToServer)
copy_file	Copies an existing history data file to another file. Example: copy_file = history_file backup_name. Do not use whitespace in the new file name.
Action	Execute command with parameter string max. 128 characters.
OID	1.3.6.1.4.1.3181.10.6.3.72.8.1.5 (historyCopyFile)
delete_file	Deletes a history file. When a file is deleted, which is still updated by the history process, then a new file started as soon as the next history update cycle starts.
Action	Execute command with parameter string max. 128 characters.
OID	1.3.6.1.4.1.3181.10.6.3.72.8.1.6 (historyDeleteFile)
list_media_files	Display a list of all history files available on the external media in the history folder.
Action	Execute command.
OID	1.3.6.1.4.1.3181.10.6.3.72.8.1.7 (historyListMediaFiles)
export_to_media	The function depends on the type of device. On devices with USB port this action copies to an inserted memory stick. On a micro switch running from internal memory this action copies to an optional DOS formatted SD card. On all other switch versions this action will do nothing. When applicable this action copies the specified history files onto the removable media. If a file already exists it is overwritten. Syntax: export_media = filename. Wildcard * may be used to select several files at once. Example: temperature_day_2017_11* to get all files of November.
Action	Execute command with parameter string max. 128 characters.
OID	1.3.6.1.4.1.3181.10.6.3.72.8.1.8 (historyExportToMedia)

Group	logfiles
Path	Management.Files.logfiles
Description	This section permits read access to various system log files. The files are also accessible via ftp in the logs directory.
list_files	<p>Displays a list of all available log files.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.9.1.2 (logfilesListFiles)</p>
show_file	<p>Displays the content of a log file. The files cannot not be edited via CLI or the embedded editor within the CLI.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.9.1.3 (logfilesShowFile)</p>
show_last_update_log	<p>Displays the last firmware update logfile.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.9.1.4 (logfilesShowLastUpdateLog)</p>
upload_last_snapshot	<p>A system snapshot contains all data required for comprehensive offsite troubleshooting. A snapshot can be created under Device.system.create_snapshot. Use the upload command to send the result to a remote system. Example: upload_last_snapshot = ftp://user:passwd@ftp.upload.com/ Type = without parameter for additional online help.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.9.1.5 (logfilesUploadLastSnapshot)</p>
export_to_media	<p>The function depends on the type of device. On devices with USB port this action copies to an inserted memory stick. On a micro switch running from internal memory this action copies to an optional DOS formatted SD card. On all other switch versions this action will do nothing. When applicable this action copies all log files onto the removable media.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.9.1.6 (logfilesExportToMedia)</p>
Group	server
Path	Management.Files.server
Description	The different file transfer protocols may individually be enabled or disabled for protection.
enable_tftp	<p>Enable TFTP server for file up-/download.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.72.10.1.2 (serverEnableTftp)</p>

enable_ftp	Enable FTP server for file up-/download. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.3.72.10.1.3 (serverEnableFtp)
<hr/>	
enable_sftp	Enable SFTP server for file up-/download. Note SFTP also requires SSH to be enabled (see CLI settings). TCP/IP Port 8022 is used. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.3.72.10.1.4 (serverEnableSftp)
<hr/>	
enable_api	Enable API server for dotstring management via https. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.3.72.10.1.5 (serverEnableApi)
<hr/>	
enable_rest	Enable REST api server for dotstring management via https. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.3.72.10.1.6 (serverEnableRest)
<hr/>	
enable_json_rpc	Enable JSON/RPC interface for M2M management via https. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.3.72.10.1.7 (serverEnableJsonRpc)

10 Event Messages (Syslog, SNMP Notifications)

10.1 Key Features

Function

Syslog protocol for UDP/IPv4 and UDP/IPv6. Syslog messages are triggered by system events and can be sent to any number of Syslog servers.

Integrates with any support structure.

Syslog to CLI

The default syslog target is the CLI. A logged-in user receives Syslogs depending on the preset severeness. The filter mechanism can be tailored.

Even without a syslog receiver Syslogs can be viewed on the CLI.

Local Logfile

All events, forwarded or not, are saved to a local logfile. This permits searching to past events to aid trouble shooting. Two logfiles are used in rotation to limit the used storage. The logfile may be uploaded via file transfer.

Access to the log files permit "post mortem" dump of sequence of events.

Log Filters

What is logged or forwarded as SNMP trap can be filtered independently for each log target destination. Please check Events section for details.

A special syslog target can be defined that logs for example only configuration changes.

Recent Logs

The recent logs table hold the last 15 events in reverse order. The lastets event at the top. This can be used in combination or instead of the instant event display in the CLI.

This is a convenience feature and also permits easy access to the latest events from within a script program.

Log to MQTT topic

Event messages can be forwarded as MQTT topics. Different format options apply. A fixed or a dynamic topic can be selected.

This can be used by other MQTT enabled devices to act on changes in the system. Suitable to IoT applications.

Long Term History

Up to 15 arbitrary status parameter can be defined which will internally be sampled every second. The values are then accumulated the last minute, hour and day. In addition logfiles are written which permit backtracking the data monthly. The created csv files can be forwarded to a collection server for further processing in Excel or similar tools.

Long term historic data can for example be used to track PoE power consumption or bit errors over time.

10.2 Functional Description

10.2.1 Introduction

The logging section contains functions to forward events to other management entities by using various formats. An event is an information about a certain change which may be more or less important to know about. The logging may take place using Syslog or SNMP Notifications.

For each receiver the type of message and the minimum severity level of the event that triggers the message can be defined.

10.2.2 Events

Logging is tightly integrated with the Event scheme embedded in the product. Many functions inside the product are controlled using internal events. Many of those events may be exposed to the outside if so desired. Events are grouped and classified by severity and other criteria. The Logging functions include filters that determine, if an internal event meets the criteria to be forwarded to the outside.

See the section 'System Event Manager' of this document for more details on the configuration and handling of system events.

10.2.3 Targets

A single internal event may be forwarded to multiple target destinations. For each target individual forwarding criteria apply and also the output format can individually be set.

10.2.4 Syslog

A Syslog is essentially a readable text message that can be logged on an external server. The Syslog protocol is standardized and Syslog receivers, which can list, sort and store the event information are readily available for many platforms.

For each event type an individual Syslog message is predefined. See 'System Event Manager' section of this manual for further reference. The device supports two Syslog output formats, whereby the 'VERBOSE' output contains the alias names of the ports and the hostname for unit related events.

10.2.5 Traps

Most events may be forwarded as SNMP notification messages, called Traps or Informs. While Traps are one-way messages, Informs are acknowledged. The information is encapsulated in SNMP compliant IP frames destined for collection in a SNMP management station. In contrast to Syslog, SNMP is more structured and better suited for automatic evaluation by software.

The device supports several SNMP versions, SNMPv1, SNMPv2c or SNMPv3. Standard traps are defined in the public MIBs. Additional traps are defined in the private MIB.

SNMP output and Syslog can run in parallel. Also an unlimited number of trap destinations (targets) may be assigned. To verify which event may be forwarded as trap, please check the 'trap_map' parameter.

Example:

```
>>Management.Event.event_list[*].trap_map
[RESERVED].trap_map:
[REGISTER_EVENT_QUEUE].trap_map:
[TIMER].trap_map:
[DEBUG].trap_map:
[ALIVE_TEST].trap_map:
[FIRMWARE_UPDATE_OK].trap_map:
[FIRMWARE_UPDATE_FAIL].trap_map:
[LICENSE_VIOLATION].trap_map:
[COLDSTART].trap_map: 1
[WARMSTART].trap_map: 2
[FACTORY_RESET_LOADED].trap_map: 8
[FACTORY_RESET_DENIED].trap_map:
[CHANGE_CONFIG].trap_map: 0
[CHANGE_OFFLINE_CONFIG].trap_map:
[ACTION_RESPONSE].trap_map:
[POWER_SUPPLY_OK].trap_map: 14
[POWER_SUPPLY_FAIL].trap_map: 14
[LOGIN].trap_map: 0
[LOGOUT].trap_map: 0
[LOGIN_ATTEMPT].trap_map: 16
[LINK_UP].trap_map: 4,7
[LINK_DOWN].trap_map: 3,7
Hit q to quit or any key to continue..
```

When trap_map value is either blank (empty) or 0, then NO trap is possible.

10.2.6 Configuration Overview

All logging parameter can be found under the following tree sections:

```
Management.Logging.target[*].
Management.Logging.statistics.
```

Use the wildcard operator '*' to select multiple targets at once.

Example:

```
>>Management.Logging.target[*].
Parameter : [StdError] [local]
alias : StdError local
host_address : 192.168.214.1:514 local
log_type : SNMP_TRAP_V2C SYSLOG
minimum_severity : ERROR DEBUG
required_relevance : ANY ANY
required_source : ANY ANY
log_config_changes : Enabled Enabled
log_debug_events_only : Disabled Disabled
>>
```

INFO: The default entry for logging writes to the local syslog log file. The keyword 'local' as host_address enabled this function.

10.2.7 Adding a target

The target list is a dynamic table. To add a new target do the following:

- Type the dotstring and use any existing alias (or '*') .alias
- Then type '=' to edit.
- The CLI will write 'Add:'
- Continue with a unique name that identifies your log target.

```
Management.Logging.target[StdError].alias = Add: my log
```

10.2.8 Delete a target

To rename a target or to delete it (including its associated parameter) use the [Cursor Up/Down] keys.

```
Management.Logging.target[StdError].alias = Delete: StdError ?
```

Press [Return] to delete. There is no undo.

10.3 Logging CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Management.						
			logging.			Logging is used to write event notifications to a server for collection. SYSLOG, SNMP traps or the CLI may be specified as destinations. Additionally, local logfiles are written to the SD card. In addition status data can be specified to create long term history data.
			send_test_event	X		Creates an ALIVE_TEST event. This may be used to check out log functionality. Hint: The severeness of the ALIVE_TEST event may be changed to try out alarm thresholds.
			auto_discovery_beacon	R/W		When enabled, the system will send out ALIVE_TEST events at the specified interval. These may be used by a management system for auto discovery.
			log_file_storage	R/W		Select the storage type of the logfile. Writing to SD card protects the file against reboot but significantly increases SD card write cycles.
			target[DYNAMIC].			An unlimited number of syslog receivers may be specified.
			alias	R/W		Name of this syslog entry for reference.
			host_address	R/W		IP address or hostname to the syslog server or snmp manager. Leave empty for local targets such as CLI or recent logs buffer.
			log_type	R/W		Specifies the type of event forwarding to match the desired manager.
			detail_level	R/W		Permits setting the detail level of the logged information. For SMNP v1 the setting EXTENDED changes the trap OID to indicate the private trap OID. For Syslog the setting EXTENDED prepends a rfc3164 compliant header.
			message_format	R/W		Determines if custom message text is used. It may be desirable to use custom on the console but to use standard text in log files.
			trap_type	R/W		Decides whether public or private traps are used. This parameter only applies then a SNMP log_type is selected.

trap_community	R/W	For SNMP v1/v2c this parameter may be used to help receiving manager filtering out unwanted traps. For logtype=SYSLOG a decimal number may be defined for a custom facility number. When empty or a string is defined, the default facility 1 (user) is used.
snmp_v3_username	R/W	When SNMP v3 is used this name is associated with a user under Management.access.user.name of the same name. The SNMP security level and passwords are taken from this user. For non SNMP logs this parameter has no effect.
minimum_severity	R/W	Only events with the defined severeness or worse are forwarded.
required_relevance	R/W	Forward any event or only negative ones.
required_source	R/W	Forward any event or only port or unit related events.
log_config_changes	R/W	When enabled configuration changes are logged regardless of relevance or source. When disabled no config changes are logged.
log_debug_events_only	R/W	When enabled debugging events with a minimum severity are logged. Other events are suppressed! When disabled no debugging events are logged.
history_config[DYNAMIC].		Up to 15 distinct values may be polled and saved to create a value history.
name	R/W	Name of this chart
record_mode	R/W	Defines in which way the history data are recorded.
history_file_mode	R/W	When set, the recorded data points will be saved to flash memory. The files can be accessed in the ftp history folder or using commands under Management.files.history.
dotstring	R/W	CLI compliant dotstring (command line) that will be executed in order to obtain the data to record. Alternatively, a persistent variable may be monitored. Syntax: \$varname
precision	R/W	Determines the precision with which the data are stored. Use NORMAL when the data should be unchanged. Note that only integer values are stored.
restart	X	Clear all historic data (in RAM) and start from now on again. Only this selected dotstring is affected. History files are NOT affected.
statistics.		These statistics indicate about the operation of the logging process.
number_of_targets	R	Indicates who many recipients exist for an event. This includes local log file when selected.
logfile_counter	R	All logs written in the internal logfile system are counted here.

syslog_counter	R	All logs to any target are counted here.
syslog_error_counter	R	All logs to any target that failed are counted here.
last_syslog_response	R	This contains a copy of the last syslog response for trouble shooting.
trap_counter	R	All traps to any target are counted here.
trap_error_counter	R	All traps to any target that failed are counted here.
active_logfile_index	R	Indicates which of the alternating logfiles is currently selected and contains the recent logs.
logfile_1_size	R	Indicates the size of the internal local log file 1 in bytes.
logfile_2_size	R	Indicates the size of the internal local log file 2 in bytes.
recent_logs[20].		This table displays the last 15 log events ordered from latest to oldest.
time_stamp	R	Updated whenever the entry is updated.
severity	R	Indicates the severeness of the event.
source	R	Indicates unit or port id of originating event source.
message	R	This contains a copy of the last syslog message
history_records[15].		Displays historic values accumulated over time. These data may be used to plot graphs or to detect trends.
name	R	Reflects the name of the related history_config entry.
state	R	Indicates if this record displays a currently running script or a history entry of a previously running script which has ended by now.
used_precision	R	Indicates the precision with which the data were stored.
last_value	R	This value is updated every second with the latest polled value.
average_last_minute	R	This value is updated every second but averages over the last minute.
average_last_hour	R	This value is updated every minute but averages over the last hour.
last_minute	R	Comma separated list with one value per every second starting at second 00. 60 values are recorded. Successive commas with no content in between indicate time positions for which no data are available.
last_hour	R	Comma separated list with one value per minute, starting at minute 00. 60 values are recorded. Successive commas with no content in between indicate time positions for which no data are yet available. Every hour the daily file gets one line appended. Every day a new file is created.

last_day	R	Comma separated list with one value per every 15 minutes, starting at hour 00. 96 values are recorded. Successive commas with no content in between indicate time positions for which no data are yet available. Every day at midnight the file gets one line appended with the current day. Every month a new file is started.
last_update	R	Indicates the time when this record was last updated.

10.4 Logging Configuration Parameters

Group Path	General Parameters												
	Management.Logging												
send_test_event	<p>Creates an ALIVE_TEST event. This may be used to check out log functionality. Hint: The severeness of the ALIVE_TEST event may be changed to try out alarm thresholds.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.71.1 (loggingSendTestEvent)</p>												
auto_discovery_beacon	<p>When enabled, the system will send out ALIVE_TEST events at the specified interval. These may be used by a management system for auto discovery.</p> <p>Values</p> <table> <tr> <td><i>DISABLED</i></td><td>No ALIVE events will be generated automatically</td></tr> <tr> <td><i>EVERY_10S</i></td><td>ALIVE events are send every 10s for test purposes</td></tr> <tr> <td><i>EVERY_MINUTE</i></td><td>ALIVE events are send every 60s</td></tr> <tr> <td><i>EVERY_5_MINUTES</i></td><td>ALIVE events are send every 300s</td></tr> <tr> <td><i>EVERY_15_MINUTES</i></td><td>ALIVE events are send every 15 minutes</td></tr> <tr> <td><i>EVERY_HOUR</i></td><td>ALIVE events are send every 60 minutes</td></tr> </table> <p>OID 1.3.6.1.4.1.3181.10.6.3.71.2 (loggingAutoDiscoveryBeacon)</p>	<i>DISABLED</i>	No ALIVE events will be generated automatically	<i>EVERY_10S</i>	ALIVE events are send every 10s for test purposes	<i>EVERY_MINUTE</i>	ALIVE events are send every 60s	<i>EVERY_5_MINUTES</i>	ALIVE events are send every 300s	<i>EVERY_15_MINUTES</i>	ALIVE events are send every 15 minutes	<i>EVERY_HOUR</i>	ALIVE events are send every 60 minutes
<i>DISABLED</i>	No ALIVE events will be generated automatically												
<i>EVERY_10S</i>	ALIVE events are send every 10s for test purposes												
<i>EVERY_MINUTE</i>	ALIVE events are send every 60s												
<i>EVERY_5_MINUTES</i>	ALIVE events are send every 300s												
<i>EVERY_15_MINUTES</i>	ALIVE events are send every 15 minutes												
<i>EVERY_HOUR</i>	ALIVE events are send every 60 minutes												
log_file_storage	<p>Select the storage type of the logfile. Writing to SD card protects the file against reboot but significantly increases SD card write cycles.</p> <p>Values</p> <table> <tr> <td><i>RAM_DISK</i></td><td>Log is written on RAM disk. Log is lost on reboot</td></tr> <tr> <td><i>SD_CARD</i></td><td>Logfile is written to SD card. Data survive a reboot</td></tr> </table> <p>OID 1.3.6.1.4.1.3181.10.6.3.71.3 (loggingLogFileStorage)</p>	<i>RAM_DISK</i>	Log is written on RAM disk. Log is lost on reboot	<i>SD_CARD</i>	Logfile is written to SD card. Data survive a reboot								
<i>RAM_DISK</i>	Log is written on RAM disk. Log is lost on reboot												
<i>SD_CARD</i>	Logfile is written to SD card. Data survive a reboot												

Group Path Description	target, dynamical size
	Management.Logging.target
	An unlimited number of syslog receivers may be specified.
alias	<p>Name of this syslog entry for reference.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.71.4.1.2 (targetAlias)</p>

host_address	<p>IP address or hostname to the syslog server or snmp manager. Leave empty for local targets such as CLI or recent logs buffer.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.71.4.1.3 (targetHostAddress)</p>																						
log_type	<p>Specifies the type of event forwarding to match the desired manager.</p> <p>Values</p> <table> <tr> <td><i>DISABLED</i></td><td>This logging entry is disabled</td></tr> <tr> <td><i>SYSLOG</i></td><td>The event will be forwarded as Syslog</td></tr> <tr> <td><i>SNMP_TRAP_V1</i></td><td>The event will be forwarded as SNMP trap using SNMP V1 format</td></tr> <tr> <td><i>SNMP_TRAP_V2C</i></td><td>The event will be forwarded as SNMP trap using SNMP V2c format</td></tr> <tr> <td><i>SNMP_TRAP_V3</i></td><td>The event will be forwarded as SNMP trap using SNMP V3 format</td></tr> <tr> <td><i>SNMP_INFORM_V2C</i></td><td>The event will be forwarded as SNMP trap using SNMP V2c acknowledged Inform format</td></tr> <tr> <td><i>SNMP_INFORM_V3</i></td><td>The event will be forwarded as SNMP trap using SNMP V3 acknowledged Inform format</td></tr> <tr> <td><i>DISPLAY_IN_CLI</i></td><td>The event will be shown to all currently open terminal sessions</td></tr> <tr> <td><i>RECENT_LOGS</i></td><td>The event will be stored in the recent_logs status ram</td></tr> <tr> <td><i>MQTT_FIXED_TOPIC</i></td><td>The event will be published as MQTT message with topic [topic_prefix]/event/log. MQTT must be properly configured to support this mode. The detail_level parameter can be used to affect the data payload.</td></tr> <tr> <td><i>MQTT_DYN_TOPIC</i></td><td>The event will be published as MQTT message with topic [topic_prefix]/event/[event_group]/[event_name]/([slot])/[port]). MQTT must be properly configured to support this mode. The data will contain textual string like in CLI. Detail_level parameter apply.</td></tr> </table> <p>OID 1.3.6.1.4.1.3181.10.6.3.71.4.1.4 (targetLogType)</p>	<i>DISABLED</i>	This logging entry is disabled	<i>SYSLOG</i>	The event will be forwarded as Syslog	<i>SNMP_TRAP_V1</i>	The event will be forwarded as SNMP trap using SNMP V1 format	<i>SNMP_TRAP_V2C</i>	The event will be forwarded as SNMP trap using SNMP V2c format	<i>SNMP_TRAP_V3</i>	The event will be forwarded as SNMP trap using SNMP V3 format	<i>SNMP_INFORM_V2C</i>	The event will be forwarded as SNMP trap using SNMP V2c acknowledged Inform format	<i>SNMP_INFORM_V3</i>	The event will be forwarded as SNMP trap using SNMP V3 acknowledged Inform format	<i>DISPLAY_IN_CLI</i>	The event will be shown to all currently open terminal sessions	<i>RECENT_LOGS</i>	The event will be stored in the recent_logs status ram	<i>MQTT_FIXED_TOPIC</i>	The event will be published as MQTT message with topic [topic_prefix]/event/log. MQTT must be properly configured to support this mode. The detail_level parameter can be used to affect the data payload.	<i>MQTT_DYN_TOPIC</i>	The event will be published as MQTT message with topic [topic_prefix]/event/[event_group]/[event_name]/([slot])/[port]). MQTT must be properly configured to support this mode. The data will contain textual string like in CLI. Detail_level parameter apply.
<i>DISABLED</i>	This logging entry is disabled																						
<i>SYSLOG</i>	The event will be forwarded as Syslog																						
<i>SNMP_TRAP_V1</i>	The event will be forwarded as SNMP trap using SNMP V1 format																						
<i>SNMP_TRAP_V2C</i>	The event will be forwarded as SNMP trap using SNMP V2c format																						
<i>SNMP_TRAP_V3</i>	The event will be forwarded as SNMP trap using SNMP V3 format																						
<i>SNMP_INFORM_V2C</i>	The event will be forwarded as SNMP trap using SNMP V2c acknowledged Inform format																						
<i>SNMP_INFORM_V3</i>	The event will be forwarded as SNMP trap using SNMP V3 acknowledged Inform format																						
<i>DISPLAY_IN_CLI</i>	The event will be shown to all currently open terminal sessions																						
<i>RECENT_LOGS</i>	The event will be stored in the recent_logs status ram																						
<i>MQTT_FIXED_TOPIC</i>	The event will be published as MQTT message with topic [topic_prefix]/event/log. MQTT must be properly configured to support this mode. The detail_level parameter can be used to affect the data payload.																						
<i>MQTT_DYN_TOPIC</i>	The event will be published as MQTT message with topic [topic_prefix]/event/[event_group]/[event_name]/([slot])/[port]). MQTT must be properly configured to support this mode. The data will contain textual string like in CLI. Detail_level parameter apply.																						
detail_level	<p>Permits setting the detail level of the logged information. For SMNP v1 the setting EXTENDED changes the trap OID to indicate the private trap OID. For Syslog the setting EXTENDED prepends a rfc3164 compliant header.</p> <p>Values</p> <table> <tr> <td><i>CONCISE</i></td><td>CLI, Syslog and Trap only present the required fields. No alias names included.</td></tr> <tr> <td><i>VERBOSE</i></td><td>CLI, syslog and Traps also contain alias names for ports and the SysName for unit related messages.</td></tr> <tr> <td><i>EXTENDED</i></td><td>Like VERBOSE plus SNMP traps contain additional supporting OIDs, SYSLOG contains RFC 3264 header and CLI prepends a time stamp</td></tr> </table> <p>OID 1.3.6.1.4.1.3181.10.6.3.71.4.1.5 (targetDetailLevel)</p>	<i>CONCISE</i>	CLI, Syslog and Trap only present the required fields. No alias names included.	<i>VERBOSE</i>	CLI, syslog and Traps also contain alias names for ports and the SysName for unit related messages.	<i>EXTENDED</i>	Like VERBOSE plus SNMP traps contain additional supporting OIDs, SYSLOG contains RFC 3264 header and CLI prepends a time stamp																
<i>CONCISE</i>	CLI, Syslog and Trap only present the required fields. No alias names included.																						
<i>VERBOSE</i>	CLI, syslog and Traps also contain alias names for ports and the SysName for unit related messages.																						
<i>EXTENDED</i>	Like VERBOSE plus SNMP traps contain additional supporting OIDs, SYSLOG contains RFC 3264 header and CLI prepends a time stamp																						
message_format	<p>Determines if custom message text is used. It may be desirable to use custom on the console but to use standard text in log files.</p> <p>Values</p> <table> <tr> <td><i>STANDARD</i></td><td>The event uses the standard syslog_message text</td></tr> <tr> <td><i>PREFER_CUSTOM</i></td><td>When a custom message is defined it will be used. Otherwise the standard text is used.</td></tr> <tr> <td><i>CUSTOM_ONLY</i></td><td>Event will use the custom message text. When no text is defined, no event is send at all! Thus this acts as filter as well.</td></tr> </table> <p>OID 1.3.6.1.4.1.3181.10.6.3.71.4.1.6 (targetMessageFormat)</p>	<i>STANDARD</i>	The event uses the standard syslog_message text	<i>PREFER_CUSTOM</i>	When a custom message is defined it will be used. Otherwise the standard text is used.	<i>CUSTOM_ONLY</i>	Event will use the custom message text. When no text is defined, no event is send at all! Thus this acts as filter as well.																
<i>STANDARD</i>	The event uses the standard syslog_message text																						
<i>PREFER_CUSTOM</i>	When a custom message is defined it will be used. Otherwise the standard text is used.																						
<i>CUSTOM_ONLY</i>	Event will use the custom message text. When no text is defined, no event is send at all! Thus this acts as filter as well.																						

trap_type	Decides whether public or private traps are used. This parameter only applies then a SNMP log_type is selected.
Values	<div>PUBLIC Only sent public traps. Event for which no public trap exists are not generated</div> <div>PREFER_PUBLIC Send public traps if defined. Otherwise send a private trap</div> <div>PRIVATE Only sent private traps</div> <div>BOTH Send a private trap and a public trap, if defined, as well</div>
OID	1.3.6.1.4.1.3181.10.6.3.71.4.1.7 (targetTrapType)
trap_community	For SNMP v1/v2c this parameter may be used to help receiving manager filtering out unwanted traps. For logtype=SYSLOG a decimal number may be defined for a custom facility number. When empty or a string is defined, the default facility 1 (user) is used.
Value	String, max. 128 characters.
OID	1.3.6.1.4.1.3181.10.6.3.71.4.1.8 (targetTrapCommunity)
snmp_v3_username	When SNMP v3 is used this name is associated with a user under Management.access.user.name with the same name. The SNMP security level and passwords are taken from this user. For non SNMP logs this parameter has no effect.
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.3.71.4.1.9 (targetSnmpV3Username)
minimum_severity	Only events with the defined severeness or worse are forwarded.
Values	<div>DISABLED Syslog output to this target is disabled</div> <div>DEBUG Internal system debugging information</div> <div>INFO Information with no important consequences</div> <div>NOTICE Notification about normal occurrence</div> <div>WARNING Warning about a normal problem</div> <div>ERROR Unexpected error has occurred</div> <div>CRITICAL Critical error which compromises data traffic or stability</div> <div>ALERT Very important error condition</div> <div>EMERGENCY Highest possible error condition (no set by this product)</div>
OID	1.3.6.1.4.1.3181.10.6.3.71.4.1.10 (targetMinimumSeverity)
required_relevance	Forward any event or only negative ones.
Values	<div>ANY Log events with any relevance</div> <div>NEG_ONLY Log only negative events</div>
OID	1.3.6.1.4.1.3181.10.6.3.71.4.1.11 (targetRequiredRelevance)
required_source	Forward any event or only port or unit related events.
Values	<div>ANY Log events regardless of source</div> <div>PORT_ONLY Logs only port related events</div> <div>UNIT_ONLY Logs only unit related events</div>
OID	1.3.6.1.4.1.3181.10.6.3.71.4.1.12 (targetRequiredSource)

log_config_changes	When enabled configuration changes are logged regardless of relevance or source. When disabled no config changes are logged. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.3.71.4.1.13 (targetLogConfigChanges)
log_debug_events_only	When enabled debugging events with a minimum severity are logged. Other events are suppressed! When disabled no debugging events are logged. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.3.71.4.1.14 (targetLogDebugEventsOnly)
Group Path Description	history_config , dynamical size Management.Logging.history_config Up to 15 distinct values may be polled and saved to create a value history.
name	Name of this chart Value String, max. 31 characters. OID 1.3.6.1.4.1.3181.10.6.3.71.5.1.2 (historyConfigName)
record_mode	Defines in which way the history data are recorded. Values <i>DISABLED</i> When disabled, no data are evaluated and stored <i>ENABLED</i> Data are inserted into result string in a fixed position. Position 1 is 00:00, Position 2 is 00:01, etc. OID 1.3.6.1.4.1.3181.10.6.3.71.5.1.3 (historyConfigRecordMode)
history_file_mode	When set, the recorded data points will be saved to flash memory. The files can be accessed in the ftp history folder or using commands under Management.files.history. Values <i>DISABLED</i> When disabled, no files are created for this record <i>HOURLY</i> The last_hour table, with its minutely granularity, is appended to the file of the day. Every day a new file is created and updated hourly. <i>DAILY</i> The last_day table, with its 15 minutes granularity, is appended to the file of the month. Every month a new file is created and updated daily. OID 1.3.6.1.4.1.3181.10.6.3.71.5.1.4 (historyConfigHistoryFileMode)
dotstring	CLI compliant dotstring (command line) that will be executed in order to obtain the data to record. Alternatively, a persistent variable may be monitored. Syntax: \$varname Value String, max. 128 characters. OID 1.3.6.1.4.1.3181.10.6.3.71.5.1.5 (historyConfigDotstring)

precision	Determines the precision with which the data are stored. Use NORMAL when the data should be unchanged. Note that only integer values are stored.	
Values	<i>NORMAL</i>	Observed value remains unchanged, result is logged as integer
	<i>TENFOLD</i>	Observed value is multiplied with 10, result is logged as integer
	<i>HUNDREDFOLD</i>	Observed value is multiplied with 100, result is logged as integer
	<i>THOUSANDFOLD</i>	Observed value is multiplied with 1000, result is logged as integer
	<i>TENTH</i>	Observed value is divided with 10, result is logged as integer
	<i>HUNDREDTH</i>	Observed value is divided with 100, result is logged as integer
	<i>THOUSANDTH</i>	Observed value is divided with 1000, result is logged as integer
OID	1.3.6.1.4.1.3181.10.6.3.71.5.1.6 (historyConfigPrecision)	

restart	Clear all historic data (in RAM) and start from now on again. Only this selected dotstring is affected. History files are NOT affected.	
Action	Execute command.	
OID	1.3.6.1.4.1.3181.10.6.3.71.5.1.7 (historyConfigRestart)	

10.5 Logging Status Parameters

Group	statistics
Path	Management.Logging.statistics
Description	These statistics indicate about the operation of the logging process.
number_of_targets	Indicates how many recipients exist for an event. This includes local log file when selected.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.3.71.100.1.2 (statisticsNumberOfTargets)
logfile_counter	All logs written in the internal logfile system are counted here.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.3.71.100.1.3 (statisticsLogfileCounter)
syslog_counter	All logs to any target are counted here.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.3.71.100.1.4 (statisticsSyslogCounter)
syslog_error_counter	All logs to any target that failed are counted here.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.3.71.100.1.5 (statisticsSyslogErrorCounter)
last_syslog_response	This contains a copy of the last syslog response for trouble shooting.
Value	String, max. 256 characters.
OID	1.3.6.1.4.1.3181.10.6.3.71.100.1.6 (statisticsLastSyslogResponse)
trap_counter	All traps to any target are counted here.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.3.71.100.1.7 (statisticsTrapCounter)
trap_error_counter	All traps to any target that failed are counted here.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.3.71.100.1.8 (statisticsTrapErrorCounter)

active_logfile_index	Indicates which of the alternating logfiles is currently selected and contains the recent logs.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.3.71.100.1.9 (statisticsActiveLogfileIndex)

logfile_1_size	Indicates the size of the internal local log file 1 in bytes.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.3.71.100.1.10 (statisticsLogfile1Size)

logfile_2_size	Indicates the size of the internal local log file 2 in bytes.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.3.71.100.1.11 (statisticsLogfile2Size)

11 System Event Manager

11.1 Key Features

Event Scheme

The device internally makes extensive use of interprocess messaging. Many of these message events can be made public as Syslogs or private traps to provide insight into the internal proceedings.

Customizable events

Event severeness and alert level is freely configurable for each event. Event text strings may be customized via user interface.

Events could be translated to local language for example.

Configuration Changes

Each time any parameter is changed via any of the user interfaces, each individual change is recorded with time stamp, operator name, user interface, old and new value. These changes may trigger Syslogs or even traps.

It possible to clearly back track configuration changes if needed.

Debug Information

It is possible to turn internal debug messages into events which can be forwarded like any other event. Thus it is possible to enable remote debugging. Note: developer/support only. These functions are protected by customers access scheme and do not pose a security breach.

Advanced debug support may help trouble shooting difficult applications problems remotely.

Run Scripts on Event

Individual automated and programmed scripts can be attached to each event. This permits custom processes run on occurrence of event.

Permits creation of event based custom functions. This enables powerful extensions to standard functionality.

11.2 Functional Description

11.2.1 System Event Control

Status changes on the device result in event messages, that can be used to control internal handling and processing of the event.

11.3 Event CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Management.						
		event.				Event definitions for traps, syslogs, logfiles, etc.
		event_list[DYNAMIC].				
			name	R		Name of the event
			group	R		Associated group of this event
			relevance	R		Positive, negative or informational event
			internal	R		If enabled this event cannot be used for syslog or traps
			severity	R/W		Severity level of this event. Can be modified if required
			source	R		Unit or port related event
			trap	R/W		When enabled a trap may be generated for this event
			syslog_message	R		Fixed event text describing the cause of the event.
			custom_message	R/W		Here a custom or translated version of the event text may be inserted.
			integer_elements	R		Lists which integer value informations are available for the syslog message
			string_elements	R		Lists which string type informations are available for the syslog message
			cli_script	R/W		When a script name is present the script will be executed whenever this event occurs. Note: Internal events do not trigger scripts even though a script name may be entered. Several scripts may be assigned to a single event. Syntax: app/scriptfile:subroutine para1 para2, next script... All fields besides the scriptfile are optional.

11.4 Event Configuration Parameters

Group	event_list, dynamical size		
Path	Management.Event.event_list		
Description			
name	Name of the event		
	Value	String, max. 32 characters.	
	OID	1.3.6.1.4.1.3181.10.6.3.70.1.1.2 (eventListName)	
group	Associated group of this event		
	Values	INTERNAL	Internal events not for customer use
		DEBUG	Internal debugging related event
	TEST	Test group	
	RESET	Reset related events	
	FIRMWARE	Firmware load related events	
	SYSTEM	System error events	
	CONFIG	Configuration change events	
	LOGIN	Login related events	
	AUTH	Authentication related events	
	POWER	Power supply related events	
	TEMPERATURE	Operating temperature related events	
	LINK	Data link related events	
	SFP	SFP related events	
	POE	PoE related events	
	RING	Ring protocol related events	
	NTP	NTP related events	
	SIGNALS	IO signal pins	
	SCRIPT	CLI scripting events	
	FILTER	Packet filter related events	
	LACP	Link Aggregation Control Protocol	
	APP	APP installation	
	CABLE	Virtual Cable Tester	
	SECURITY	Network security related events	
	MSP1000	MSP1000 system related events	
	BACKUP	Backup data path events	
	FAN	Cooling fan related events	
	MESSAGING	From extern received alarm messages	
	TERMINAL_SERVER	Terminal server events	
	SMART_OFFICE	SmartOffice internal events	
	OID	1.3.6.1.4.1.3181.10.6.3.70.1.1.3 (eventListGroup)	

relevance	Positive, negative or informational event	
	Values	<i>POS</i> Identifies a positive event <i>NEG</i> Identifies a negative event <i>INFO</i> Identifies an informational event
	OID	1.3.6.1.4.1.3181.10.6.3.70.1.1.4 (eventListRelevance)
internal	If enabled this event cannot be used for syslog or traps	
	Values	enabled, disabled
	OID	1.3.6.1.4.1.3181.10.6.3.70.1.1.5 (eventListInternal)
severity	Severity level of this event. Can be modified if required	
	Values	<i>DISABLED</i> No Output
		<i>DEBUG</i> Internal system debugging information
		<i>INFO</i> Information with no important consequences
		<i>NOTICE</i> Notification about normal occurrence
		<i>WARNING</i> Warning about a normal problem
		<i>ERROR</i> Unexpected error has occurred
		<i>CRITICAL</i> Critical error which compromises data traffic or stability
		<i>ALERT</i> Very important error condition
		<i>EMERGENCY</i> Highest possible error condition (no set by this product)
	OID	1.3.6.1.4.1.3181.10.6.3.70.1.1.6 (eventListSeverity)
source	Unit or port related event	
	Values	<i>UNIT</i> Unit related event
		<i>PORT</i> Port related event
	OID	1.3.6.1.4.1.3181.10.6.3.70.1.1.7 (eventListSource)
trap	When enabled a trap may be generated for this event	
	Values	enabled, disabled
	OID	1.3.6.1.4.1.3181.10.6.3.70.1.1.8 (eventListTrap)
syslog_message	Fixed event text describing the cause of the event.	
	Value	String, max. 512 characters.
	OID	1.3.6.1.4.1.3181.10.6.3.70.1.1.9 (eventListSyslogMessage)
custom_message	Here a custom or translated version of the event text may be inserted.	
	Value	String, max. 512 characters.
	OID	1.3.6.1.4.1.3181.10.6.3.70.1.1.10 (eventListCustomMessage)

integer_elements	Lists which integer value informations are available for the syslog message
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.3.70.1.1.11 (eventListIntegerElements)

string_elements	Lists which string type informations are available for the syslog message
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.3.70.1.1.12 (eventListStringElements)

cli_script	When a script name is present the script will be executed whenever this event occurs. Note: Internal events do not trigger scripts even though a script name may be entered. Several scripts may be assigned to a single event. Syntax: app/scriptfile:subroutine para1 para2, next script... All fields besides the scriptfile are optional.
Value	String, max. 512 characters.
OID	1.3.6.1.4.1.3181.10.6.3.70.1.1.13 (eventListCliScript)

12 Miscellaneous

12.1 Key Features

Terminal Server

The serial port can be used to connect a foreign device. This device can then be reached via Telnet or SSH session. Also serial to serial connections via an IP network are supported. The serial port can also be reached via a PC-COM port emulation.

This saves customer a separate converter when a legacy device is to be controlled.

Loudspeaker support

Audio files (wav, mp3) and network audio streams can be streamed to external IP loudspeaker. Play function can be scripted and associated to selected events.

Alarm conditions can be made audible or network music streams can be played in an SmartOffice application.

12.2 Functional Description

Miscellaneous

Miscellaneous network management related parameter.

12.3 Misc CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Management.						
	misc.					Miscellaneous network management related parameter
		terminal_server_config.				This section defines setting for the terminal server feature.
			device_name	R/W		Descriptive name for customer reference. This name is echoed upon login.
			mode	R/W		Defines the operational mode of the terminal server.
			remote_ip	R/W		IP address of the associated remote partner. Only applies in CLIENT and COM_PORT mode.
			tcp_port	R/W		Defines the TCP port number under which the terminal server is reachable.
			inactivity_timeout	R/W		An unattended terminal server logs off automatically after specified seconds. Use 0 to disable timeout.
			data_rate	R/W		Data rate in bits per second.
			databits	R/W		Number of data bits per character.
			parity	R/W		Defines if the parity bit is used.
			stop_bits	R/W		Number of stop bits per character.
			flow_control	R/W		Determines if flow control is used.
			forwarding_timer	R/W		Defined in 100ms steps. After no more data are received for this time, the serial data are forwarded to the Ethernet side. (VTIME)
			character_count	R/W		At least this many character must be received before data are forwarded. Set to zero to ignore count. (VMIN)
			forwarding_character	R/W		When the specified character is received o the serial port, the TCP packet is forwarded.
		speaker_config.				This section defines settings for an optional network addressed loudspeaker. Wav or mps3 files may be played out. Local sound files or network music files can be accessed. Not that WAV files must be provided in the format as required by the selected source. With mp3 on-the-fly transcoding is available.

play	X	Play a sound file or stream. A local should file must reside in the sound folder accessible via ftp. Syntax: .play = mysound.mp3 Alternatively a remote file or stream may be played in the format: .play = http://webradiostream.mp3
stop	X	Cancels all sound output.
volume	X	Volume control if possible for this device.
device_name	R/W	Descriptive name for customer reference.
device_type	R/W	Select type or protocol of desired speaker.
output_rate	R/W	Output (re)sample rate only applies to MP3 files or streams. Default value 44100.
output_format	R/W	Mono Stereo conversion only applies to mp3 files or streams.
host_address	R/W	IP address or symbolic name of the speaker
udp_port	R/W	UDP port for

12.4 Misc Configuration Parameters

Group	terminal_server_config		
Path	Management.Misc.terminal_server_config		
Description	This section defines setting for the terminal server feature.		
device_name	Descriptive name for customer reference. This name is echoed upon login.		
	Value	String, max. 128 characters.	
	OID	1.3.6.1.4.1.3181.10.6.3.78.1.1.2 (terminalServerConfigDeviceName)	
mode	Defines the operational mode of the terminal server.		
	Values	SERVER	Use this mode when putty is used to connect to local serial port
		CLIENT	Use this mode for serial port to serial port forwarding. One side must be client
		COM_PORT	Use when PC with COM port emulation is used
	OID	1.3.6.1.4.1.3181.10.6.3.78.1.1.3 (terminalServerConfigMode)	
remote_ip	IP address of the associated remote partner. Only applies in CLIENT and COM_PORT mode.		
	Format	IPv4 Address ddd.ddd.ddd.ddd (ddd = decimal number between 000 to 255)	
	OID	1.3.6.1.4.1.3181.10.6.3.78.1.1.4 (terminalServerConfigRemoteIp)	
tcp_port	Defines the TCP port number under which the terminal server is reachable.		
	Value	Number in range 1000-65535	
	OID	1.3.6.1.4.1.3181.10.6.3.78.1.1.5 (terminalServerConfigTcpPort)	
inactivity_timeout	An unattended terminal server logs off automatically after specified seconds. Use 0 to disable timeout.		
	Value	Number in range 0-10000	
	OID	1.3.6.1.4.1.3181.10.6.3.78.1.1.6 (terminalServerConfigInactivityTimeout)	

data_rate	Data rate in bits per second.	
Values	<i>300</i>	300 bit/s
	<i>600</i>	600 bit/s
	<i>1200</i>	1200 bit/s
	<i>2400</i>	2400 bit/s
	<i>4800</i>	4800 bit/s
	<i>9600</i>	9600 bit/s
	<i>19200</i>	19200 bit/s
	<i>38400</i>	38400 bit/s
	<i>57600</i>	57600 bit/s
	<i>115200</i>	115200 bit/s
	<i>230400</i>	230400 bit/s
OID	1.3.6.1.4.1.3181.10.6.3.78.1.1.7 (terminalServerConfigDataRate)	
databits	Number of data bits per character.	
Values	<i>7_BIT</i>	7 bits per character
	<i>8_BIT</i>	8 bits per character
OID	1.3.6.1.4.1.3181.10.6.3.78.1.1.8 (terminalServerConfigDatabits)	
parity	Defines if the parity bit is used.	
Values	<i>NONE</i>	No parity bit
	<i>ODD</i>	Odd parity
	<i>EVEN</i>	Even parity
	<i>MARK</i>	Parity bit is always high
	<i>SPACE</i>	Parity bit is always low
OID	1.3.6.1.4.1.3181.10.6.3.78.1.1.9 (terminalServerConfigParity)	
stop_bits	Number of stop bits per character.	
Values	<i>1_BIT</i>	1 stop bit
	<i>2_BITS</i>	2 stop bits
OID	1.3.6.1.4.1.3181.10.6.3.78.1.1.10 (terminalServerConfigStopBits)	
flow_control	Determines if flow control is used.	
Values	<i>NONE</i>	No flow control at all
	<i>LOCAL_XON_XOFF</i>	Xon/Xoff is locally processed and buffering takes place within the switch
	<i>PASS_XON_XOFF</i>	Xon/Xoff is passed through to serial device and must be processed there
OID	1.3.6.1.4.1.3181.10.6.3.78.1.1.11 (terminalServerConfigFlowControl)	

forwarding_timer	<p>Defined in 100ms steps. After no more data are received for this time, the serial data are forwarded to the Ethernet side. (VTIME)</p> <p>Value Number in range 0-600</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.78.1.1.12 (terminalServerConfigForwardingTimer)</p>
character_count	<p>At least this many character must be received before data are forwarded. Set to zero to ignore count. (VMIN)</p> <p>Value Number in range 0-10000</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.78.1.1.13 (terminalServerConfigCharacterCount)</p>
forwarding_character	<p>When the specified character is received o the serial port, the TCP packet is forwarded.</p> <p>Values <i>NONE</i> No special character handling for data forwarding</p> <p> <i>CR</i> When a carriage return is received serially, the TCP packet is forwarded</p> <p> <i>LF</i> When a line feed is received serially, the TCP packet is forwarded</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.78.1.1.14 (terminalServerConfigForwardingCharacter)</p>
Group Path Description	<p>speaker_config</p> <p>Management.Misc.speaker_config</p> <p>This section defines settings for an optional network addressed loudspeaker. Wav or mps3 files may be played out. Local sound files or network music files can be accessed. Not that WAV files must be provided in the format as required by the selected source. With mp3 on-the-fly transcoding is available.</p>
play	<p>Play a sound file or stream. A local should file must reside in the sound folder accessible via ftp. Syntax: .play = mysound.mp3 Alternatively a remote file or stream may be played in the format: .play = http://webradiostream.mp3</p> <p>Action Excecute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.78.2.1.2 (speakerConfigPlay)</p>
stop	<p>Cancels all sound output.</p> <p>Action Excecute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.78.2.1.3 (speakerConfigStop)</p>
volume	<p>Volume control if possible for this device.</p> <p>Action Excecute command with parameter string max. 8 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.3.78.2.1.4 (speakerConfigVolume)</p>

device_name	Descriptive name for customer reference.	
	Value	String, max. 128 characters.
	OID	1.3.6.1.4.1.3181.10.6.3.78.2.1.5 (speakerConfigDeviceName)
device_type	Select type or protocol of desired speaker.	
	Values	<i>GENERIC_RTP</i> Generic RTP compatible speaker <i>SMARTAUDIO_CONTROLLER</i> SmartAudio Controller
	OID	1.3.6.1.4.1.3181.10.6.3.78.2.1.6 (speakerConfigDeviceType)
output_rate	Output (re)sample rate only applies to MP3 files or streams. Default value 44100.	
	Value	Number in range 8000-400000
	OID	1.3.6.1.4.1.3181.10.6.3.78.2.1.7 (speakerConfigOutputRate)
output_format	Mono Stereo conversion only applies to mp3 files or streams.	
	Values	<i>MONO</i> Stereo source data will be converted to mono <i>STEREO</i> Stereo output with a stereo source
	OID	1.3.6.1.4.1.3181.10.6.3.78.2.1.8 (speakerConfigOutputFormat)
host_address	IP address or symbolic name of the speaker	
	Value	String, max. 128 characters.
	OID	1.3.6.1.4.1.3181.10.6.3.78.2.1.9 (speakerConfigHostAddress)
udp_port	UDP port for	
	Value	Number in range 0-65535
	OID	1.3.6.1.4.1.3181.10.6.3.78.2.1.10 (speakerConfigUdpPort)

13 Factory Information

13.1 Key Features

Inventory and Factory information

Each device carries permanent information about its identity. This includes serial number, production codes, MAC address and a feature summary. These data are not located on the removable SD card.

This ensures that unit identity is locked to the physical hardware and not to the SD card.

Custom Device Info

Permanent hardware coupled custom information string which may be used for inventory or location info. This information persists even when the SD card is exchanged. Custom data may be entered by the customer or devices can be ordered individually preset from factory according to customer request.

This custom data may be preset in the factory according to customer request or can later be written by customer.

13.2 Functional Description

This section contains information about Inventory and Factory information stored permanently within the device.

13.3 Factory CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Device.	factory.					Factory settings which are not changeable by user
			article_number	R		This device article number.
			serial_number	R		This device serial number.
			device_mac	R		This device MAC address.
			number_of_macs	R		Number of MAC addresses this device supports.
			hardware_version	R		This device hardware revision number.
			board_id	R		This identifies the basic hardware type for internal operation.
			project_number	R		Development project number.
			mechanical_features	R		Bit mask which identifies mechanical features of this device.
			hardware_features	R		Bit mask which identifies installed hardware features of this device.
			company_name	R		Complete name and address of the manufacturing company.
			company_short	R		Shorthand name of the manufacturing company.
			web_link	R		Link to company homepage.
			web_description	R		Product feature summary.
			custom_info	R/W		This field can be used to permanently store custom inventory or location data. The data are stored within the device in irremovable storage and thus will persist even when the SD card or the entire configuration is changed.

13.4 Factory Configuration Parameters

Group Path	General Parameters
	Device.Factory
article_number	<p>This device article number.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.32.1 (factoryArticleNumber) 1.3.6.1.2.1.47.1.1.1.1.13 (entPhysicalModelName) 1.0.8802.1.1.2.1.5.4795.1.2.7.0 (lldpXMedLocModelName)</p>
serial_number	<p>This device serial number.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.32.2 (factorySerialNumber) 1.3.6.1.2.1.47.1.1.1.1.11 (entPhysicalSerialNum) 1.0.8802.1.1.2.1.5.4795.1.2.5.0 (lldpXMedLocSerialNum)</p>
device_mac	<p>This device MAC address.</p> <p>Format MAC Address <i>hh-hh-hh-hh-hh-hh</i> (<i>hh</i> = hexadecimal number between 00 to ff)</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.32.3 (factoryDeviceMac)</p>
number_of_macs	<p>Number of MAC addresses this device supports.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.32.4 (factoryNumberOfMacs)</p>
hardware_version	<p>This device hardware revision number.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.32.5 (factoryHardwareVersion) 1.3.6.1.2.1.47.1.1.1.1.8 (entPhysicalHardwareRev) 1.0.8802.1.1.2.1.5.4795.1.2.2.0 (lldpXMedLocHardwareRev)</p>
board_id	<p>This identifies the basic hardware type for internal operation.</p> <p>Value Number in range 0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.32.6 (factoryBoardId)</p>
project_number	<p>Development project number.</p> <p>Value String, max. 8 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.32.7 (factoryProjectNumber)</p>

mechanical_features	Bit mask which identifies mechanical features of this device.	
Values		
	<i>DESKTOP</i>	Desktop unit
	<i>RAIL</i>	Industry enclosure for hat rail mounting
	<i>DUCT_VERTICAL</i>	Cable duct mounting, Vertical version
	<i>DUCT_HORIZONTAL</i>	Cable duct mounting, Horizontal version
	<i>RACK</i>	Rack based system
	<i>STACKABLE</i>	Extensible unit
	<i>DC</i>	Direct DC power input
	<i>AC</i>	Direct AC power input
	<i>DUAL_PWR</i>	Redundant power input
	<i>EXT_TEMP</i>	Extended operating temperature range (DC)
	<i>EXT_SUPPLY</i>	Extended power supply range
	<i>EX_SECURE</i>	Explosive environment supported
	<i>MICRO_SD</i>	Firmware on removable Micro SD card
	<i>SDCARD</i>	Firmware on removable standard SD card
	<i>INTERNAL_MEMORY</i>	
	<i>IP30</i>	Schutzklasse IP30
	<i>IP42</i>	Schutzklasse IP42
	<i>IP44</i>	Schutzklasse IP44
	<i>IP55</i>	Schutzklasse IP55
	<i>IP67</i>	Schutzklasse IP67
OID	1.3.6.1.4.1.3181.10.6.1.32.8 (factoryMechanicalFeatures)	

hardware_features	Bit mask which identifies installed hardware features of this device.		
	Values	POE_PLUS	Power over Ethernet plus (30W ports) supported
		POE_PSE	Power over Ethernet plus (15W ports) supported
		POE_PD	Unit may be powered from POE source
		RAILWAY	Railway certified
		SUBSTATION	Power Substation certified
		EEE	Energy Efficient Ethernet
		SYNCE	Synchronous Ethernet supported
		1588	1588 protocol support
		USB	USB port supported
		RELAYS	Alarm relay connections
		RTC	Local real time clock
		MAX_100M	Hardware is limited to Fast Ethernet
		CSFP	Compact double SFP
		SFP	Pluggable optical port
		LC	Optical LC connector
		SC	Optical SC connector
		ST	Optical ST connector
		E2000	Optical E-2000 connector
		SLC	Smart Light Controller ports
	OID	1.3.6.1.4.1.3181.10.6.1.32.9 (factoryHardwareFeatures)	

company_name	Complete name and address of the manufacturing company.		
	Value	String, max. 64 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.32.10 (factoryCompanyName)	
		1.3.6.1.2.1.47.1.1.1.1.12 (entPhysicalMfgName)	
		1.0.8802.1.1.2.1.5.4795.1.2.6.0 (lldpXMedLocMfgName)	

company_short	Shorthand name of the manufacturing company.		
	Value	String, max. 16 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.32.11 (factoryCompanyShort)	

web_link	Link to company homepage.		
	Value	String, max. 128 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.32.12 (factoryWebLink)	

web_description	Product feature summary.
Value	String, max. 128 characters.
OID	1.3.6.1.4.1.3181.10.6.1.32.13 (factoryWebDescription) 1.3.6.1.2.1.47.1.1.1.1.7 (entPhysicalName) 1.3.6.1.2.1.47.1.1.1.1.2 (entPhysicalDescr)

custom_info	This field can be used to permanently store custom inventory or location data. The data are stored within the device in irremovable storage and thus will persist even when the SD card or the entire configuration is changed.
Value	String, max. 512 characters.
OID	1.3.6.1.4.1.3181.10.6.1.32.14 (factoryCustomInfo)

14 System Information

14.1 Key Features

Custom MAC address

While the MAC address is assigned at production time is possible to overwrite this MAC for special cases.

Should a unit need to be replaced and the MAC address of the original unit must be retained for some reason, the MAC can be reassigned.

Custom Inventory Data

The user can supply various private strings to customize the device. This includes port alias names (64 byte), system name, location and group strings (each 255 byte) plus a private inventory string of 512 byte length.

Customized inventory data permit integration in corporate inventory scheme.

Temperature Control

Temperature inside the device is monitored and actions are taken if required. There are warning events (Syslog, Trap) in several steps. Under severe condition the unit may reduce speed or power down some port to reduce heat dissipation.

The devices are designed to operate without a fan. They may be placed in hard to reach locations and thus early warning of possible heat issues can improve network reliability.

14.2 Functional Description

This section contains information about basic system hardware and software status.

14.3 System CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Device.						
	system.					General system information and control functions
			show_time_date	X		Show system time and date.
			set_time	X		Sets the system clock (time only). Syntax: 12:30:00
			set_date	X		Sets the system clock (date only). Syntax: 2012-12-24
			show_utilization	X		Show CPU status information
			reboot_device	X		This command will restart the device. All communication will be disrupted! Syntax: reboot_device = CONFIRM.
			create_snapshot	X		Creates a snapshot of all relevant configuration and status information packaged as a single tar archive. This file can be found in service/snapshot.
			send_wake_on_lan_packet	X		This command will send a magic packet to wake up a selected sleeping device. The device is identified by its MAC address. Syntax: send_wake_on_lan_packet = 00:11:22:44:55:66.
			alternative_mac_address	R/W		This field is usually empty. This field may be used to override the MAC address fixed in the factory setting. NOTE: This value is only activated after a reset!
			boot_preference	R/W		This feature only applies to devices that feature internal memory plus plugged-in SD cards. It defines which software is used after reboot.
			inventory	R/W		Inventory string free for customer use. Up to 512 character are accepted. Note this config is linked to the SD card and may change when config or SD card is exchanged. For an inventory information that is fixed to the hardware use Device.Factory.custom_info command.
			autorun_cli_script	R/W		Optional cli scripts executed after power sequence is completed. Several scripts may be assigned, with comma or blank separation.

serial_port	R/W	When set to DISABLED the local serial console port is disabled. Local access via serial cable is blocked. While this enhances local protection it also closes the emergency access should the device become inaccessible over the network due to misconfiguration. Other setting permit use of the serial port as TERMINAL_SERVER to attach a foreign device for management or to SMART_SENSOR to attach a local hardware extension for use with smart office solutions.
permit_debug_access	R/W	When enabled it is possible to log into the system for debug purposes. This includes telnet/ssh, as well as web and file transfer protocols. To protect the system from unauthorized access it is advised to disable this feature unless instructed by authorized service personnel. NOTE: To ensure that any possibly pending debug access is terminated reboot the device after setting this parameter to disabled.
permit_incoming_alerts	R/W	When enabled it is possible receive alerts via from external devices via SNMP or HTTP(S). This feature may be used in combination with custom scripting to react to external events. To protect the system from unauthorized spam it is advised to disable this feature unless there is an application for it.
character_set	R/W	This parameter can be set to support languages with characters not found the normal Western European character set. Be sure to set your CLI terminal to the matching setting.
configuration_save_mode	R/W	In most cases the configuration of the device should be permanently saved and automatically be applied after a power up. In some cases, however, where public access to the device is granted it can be desirable to only save changes temporarily. In this mode all configuration changes that occurred after setting this mode will be saved in RAM only and will be forgotten on the next system reboot. Important: When this parameter changed to PERMANENTLY all outstanding changes are committed to SD card immediately. When this parameter is changed to temporarily, this already is not saved permanently. Use Management.Files.configuration.commit_config to save this setting before proceeding.
compatibility.		This section contains parameter that may be required to select certain compatibility functions that cannot be auto-detected by the system.
link_detection	R/W	Usually the default setting POLL_AND_INTERRUPT should be selected. To attain fastest possible link change detection, as required by the RING protocols, select INT_ONLY. However, some older devices do not offer the faster interrupt only mode and cannot be used in this mode.

script_schedule[DYNAMIC].		This dynamic table permits the setup of automated script execution based on precise time scheduling definition. Any number of scripts may be executed at any desired interval or at selected dates. Please ensure the time and date are properly set (via NTP) when using this feature.
name	R/W	Unique name to reference this entry and to remember whose MAC address is entered.
mode	R/W	When set to disabled this entry is ignored. It is recommended to first set the mode to disabled before the associated time values are modified. When all values are properly set re-enable the entry.
cli_script	R/W	Enter the name of the cli script that should be executed when the defined time occurs. Ensure that the script name selects a valid file. Several scripts may be assigned, with comma or blank separation.
minutes	R/W	Format: 3,14 select exact minutes hour:03 and hour:14. * is every minute. */5 defines every five minutes.
hours	R/W	Format: 0-23. Range and comma separation is permitted. * is every hour.
days	R/W	Format: 1-31. Range and comma separation is permitted. * is every day.
months	R/W	Format: 1-12 or Jan-Dec. Range and comma separation is permitted. * is every month.
weekdays	R/W	Format: 0-6 or Sun-Sat. Range and comma separation is permitted. * is every day.
last_boot_time	R	The time and date when this device has booted.
uptime	R	Uptime since last reboot in seconds.
used_mac_address	R	Contains the mac address used by this unit. Usually follows to MAC defined in the factory setting, but may be overwritten by the alternative_mac_address.
used_boot_media	R	
temperature	R	Temperature value in centigrade.
climate_level	R	Annotated temperature level.
firmware.		This section provides details about the running firmware.
running_version	R	Running firmware version.
build_date	R	Build date of the running firmware. Format: 2012-01-18 12:00:22.
build_number	R	Build number of the running firmware retrieved from the repository.
patch_version	R	If extra patches are installed, their version(s) are indicated here.
save_info.		This section provided status information about the internal parameter saving process.
last_saved_parameter	R	Records the last written parameter.
save_mode	R	Reflects Device.system.configuration_save_mode setting.

write_status	R	Indicates if last parameter was written to SD card or temporary RAM.
time_stamp	R	Records the time the write status was last changed.

14.4 System Configuration Parameters

Group Path	General Parameters Device.System
show_time_date	<p>Show system time and date.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.30.1 (systemShowTimeDate)</p>
set_time	<p>Sets the system clock (time only). Syntax: 12:30:00</p> <p>Action Execute command with parameter string max. 8 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.30.2 (systemSetTime)</p>
set_date	<p>Sets the system clock (date only). Syntax: 2012-12-24</p> <p>Action Execute command with parameter string max. 10 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.30.3 (systemSetDate)</p>
show_utilization	<p>Show CPU status information</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.30.4 (systemShowUtilization)</p>
reboot_device	<p>This command will restart the device. All communication will be disrupted! Syntax: reboot_device = CONFIRM.</p> <p>Action Execute command with parameter string max. 16 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.30.5 (systemRebootDevice)</p>
create_snapshot	<p>Creates a snapshot of all relevant configuration and status information packaged as a single tar archive. This file can be found in service/snapshot.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.30.6 (systemCreateSnapshot)</p>
send_wake_on_lan_packet	<p>This command will send a magic packet to wake up a selected sleeping device. The device is identified by its MAC address. Syntax: send_wake_on_lan_packet = 00:11:22:44:55:66.</p> <p>Action Execute command with parameter string max. 20 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.30.7 (systemSendWakeOnLanPacket)</p>

alternative_mac_address	<p>This field is usually empty. This field may be used to override the MAC address fixed in the factory setting. NOTE: This value is only activated after a reset!</p> <p>Format MAC Address <i>hh-hh-hh-hh-hh-hh</i> (<i>hh</i> = hexadecimal number between 00 to ff)</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.30.8 (systemAlternativeMacAddress)</p>								
boot_preference	<p>This feature only applies to devices that feature internal memory plus plugged-in SD cards. It defines which software is used after reboot.</p> <p>Values</p> <table data-bbox="667 600 1342 1106"> <tr> <td><i>SD_CARD_FIRST</i></td><td>The SD card is tried first. When SD card is not present the internal memory is used to boot from if available.</td></tr> <tr> <td><i>INTERNAL_FIRST</i></td><td>The internal memory is tried first. When memory is not responding a possible SD card is used to boot from if available.</td></tr> <tr> <td><i>SD_CARD_ONLY</i></td><td>The SD card is used to boot. When SD card is not present the boot process will stop even if internal memory is available.</td></tr> <tr> <td><i>INTERNAL_ONLY</i></td><td>The internal memory is used to boot. Even when an optional SD card is inserted, it is not used to boot from. Should the internal memory fail will the boot process stop. Note: such a failed system cannot be recovered in the field and will need to be send in for repair. Use this setting to safeguard against a potentially illegally inserted SD card.</td></tr> </table> <p>OID 1.3.6.1.4.1.3181.10.6.1.30.9 (systemBootPreference)</p>	<i>SD_CARD_FIRST</i>	The SD card is tried first. When SD card is not present the internal memory is used to boot from if available.	<i>INTERNAL_FIRST</i>	The internal memory is tried first. When memory is not responding a possible SD card is used to boot from if available.	<i>SD_CARD_ONLY</i>	The SD card is used to boot. When SD card is not present the boot process will stop even if internal memory is available.	<i>INTERNAL_ONLY</i>	The internal memory is used to boot. Even when an optional SD card is inserted, it is not used to boot from. Should the internal memory fail will the boot process stop. Note: such a failed system cannot be recovered in the field and will need to be send in for repair. Use this setting to safeguard against a potentially illegally inserted SD card.
<i>SD_CARD_FIRST</i>	The SD card is tried first. When SD card is not present the internal memory is used to boot from if available.								
<i>INTERNAL_FIRST</i>	The internal memory is tried first. When memory is not responding a possible SD card is used to boot from if available.								
<i>SD_CARD_ONLY</i>	The SD card is used to boot. When SD card is not present the boot process will stop even if internal memory is available.								
<i>INTERNAL_ONLY</i>	The internal memory is used to boot. Even when an optional SD card is inserted, it is not used to boot from. Should the internal memory fail will the boot process stop. Note: such a failed system cannot be recovered in the field and will need to be send in for repair. Use this setting to safeguard against a potentially illegally inserted SD card.								
inventory	<p>Inventory string free for customer use. Up to 512 character are accepted. Note this config is linked to the SD card and may change when config or SD card is exchanged. For an inventory information that is fixed to the hardware use Device.Factory.custom_info command.</p> <p>Value String, max. 512 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.30.10 (systemInventory) 1.3.6.1.2.1.47.1.1.1.15 (entPhysicalAssetID)</p>								
autorun_cli_script	<p>Optional cli scripts executed after power sequence is completed. Several scripts may be assigned, with comma or blank separation.</p> <p>Value String, max. 512 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.30.11 (systemAutorunCliScript)</p>								

serial_port

When set to DISABLED the local serial console port is disabled. Local access via serial cable is blocked. While this enhances local protection it also closes the emergency access should the device become inaccessible over the network due to misconfiguration. Other setting permit use of the serial port as TERMINAL_SERVER to attach a foreign device for management or to SMART_SENSOR to attach a local hardware extension for use with smart office solutions.

Values	<i>DISABLED</i>	The serial port can no longer be used for local login.
	<i>CONSOLE</i>	Normal setting which permits use of the local serial port as emergency login console.
	<i>APP_CONTROLLED</i>	The port may be used for arbitrary serial I/O controlled via a microScript or App.
	<i>TERMINAL_SERVER</i>	The serial port is internally connected to the terminal server feature which permits to relay data between a telnet or SSH connection and the serial port. This can be used to access a (legacy) foreign device via Ethernet.
	<i>SMART_SENSOR</i>	The serial port expects an external extension module which relays infrastructure automation data.

OID 1.3.6.1.4.1.3181.10.6.1.30.12 (systemSerialPort)

permit_debug_access

When enabled it is possible to log into the system for debug purposes. This includes telnet/ssh, as well as web and file transfer protocols. To protect the system from unauthorized access it is advised to disable this feature unless instructed by authorized service personnel. NOTE: To ensure that any possibly pending debug access is terminated reboot the device after setting this parameter to disabled.

Values enabled, disabled

OID 1.3.6.1.4.1.3181.10.6.1.30.13 (systemPermitDebugAccess)

permit_incoming_alerts

When enabled it is possible receive alerts via from external devices via SNMP or HTTP(S). This feature may be used in combination with custom scripting to react to external events. To protect the system from unauthorized spam it is advised to disable this feature unless there is an application for it.

Values enabled, disabled

OID 1.3.6.1.4.1.3181.10.6.1.30.14 (systemPermitIncomingAlerts)

character_set

This parameter can be set to support languages with characters not found the normal Western European character set. Be sure to set your CLI terminal to the matching setting.

Values *ISO_8859_1* Western Europe character set
ISO_8859_5 Cyrillic character set

OID 1.3.6.1.4.1.3181.10.6.1.30.15 (systemCharacterSet)

configuration_save_mode	<p>In most cases the configuration of the device should be permanently saved and automatically be applied after a power up. In some cases, however, where public access to the device is granted it can be desirable to only save changes temporarily. In this mode all configuration changes that occurred after setting this mode will be saved in RAM only and will be forgotten on the next system reboot. Important: When this parameter changed to PERMANENTLY all outstanding changes are committed to SD card immediately. When this parameter is changed to temporarily, this already is not saved permanently. Use Management.Files.configuration.commit_config to save this setting before proceeding.</p> <p>Values <i>PERMANENTLY</i> Normal mode. A changes are saved on the SD card or internal memory</p> <p> <i>TEMPORARILY</i> Special mode where configuration is only saved in volatile RAM until next reboot or manual commit_config</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.30.16 (systemConfigurationSaveMode)</p>
--------------------------------	---

Group	script_schedule , dynamical size
Path	Device.System.script_schedule
Description	This dynamic table permits the setup of automated script execution based on precise time scheduling definition. Any number of scripts may be executed at any desired interval or at selected dates. Please ensure the time and date are properly set (via NTP) when using this feature.

name	<p>Unique name to reference this entry and to remember whose MAC address is entered.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.30.18.1.2 (scriptScheduleName)</p>
mode	<p>When set to disabled this entry is ignored. It is recommended to first set the mode to disabled before the associated time values are modified. When all values are properly set re-enable the entry.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.30.18.1.3 (scriptScheduleMode)</p>
cli_script	<p>Enter the name of the cli script that should be executed when the defined time occurs. Ensure that the script name selects a valid file. Several scripts may be assigned, with comma or blank separation.</p> <p>Value String, max. 512 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.30.18.1.4 (scriptScheduleCliScript)</p>

minutes	<p>Format: 3,14 select exact minutes hour:03 and hour:14. * is every minute. */5 defines every five minutes.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.30.18.1.5 (scriptScheduleMinutes)</p>						
hours	<p>Format: 0-23. Range and comma separation is permitted. * is every hour.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.30.18.1.6 (scriptScheduleHours)</p>						
days	<p>Format: 1-31. Range and comma separation is permitted. * is every day.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.30.18.1.7 (scriptScheduleDays)</p>						
months	<p>Format: 1-12 or Jan-Dec. Range and comma separation is permitted. * is every month.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.30.18.1.8 (scriptScheduleMonths)</p>						
weekdays	<p>Format: 0-6 or Sun-Sat. Range and comma separation is permitted. * is every day.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.30.18.1.9 (scriptScheduleWeekdays)</p>						
<table> <tr> <td>Group</td><td>compatibility</td></tr> <tr> <td>Path</td><td>Device.System.compatibility</td></tr> <tr> <td>Description</td><td>This section contains parameter that may be required to select certain compatibility functions that cannot be auto-detected by the system.</td></tr> </table>		Group	compatibility	Path	Device.System.compatibility	Description	This section contains parameter that may be required to select certain compatibility functions that cannot be auto-detected by the system.
Group	compatibility						
Path	Device.System.compatibility						
Description	This section contains parameter that may be required to select certain compatibility functions that cannot be auto-detected by the system.						
link_detection	<p>Usually the default setting POLL_AND_INTERRUPT should be selected. To attain fastest possible link change detection, as required by the RING protocols, select INT_ONLY. However, some older devices do not offer the faster interrupt only mode and cannot be used in this mode.</p> <p>Values</p> <table> <tr> <td><i>POLL_AND_INTERRUPT</i></td><td>Normal mode. When possible interrupts are used. Polling catches devices without interrupt capability.</td></tr> <tr> <td><i>INTERRUPT_ONLY</i></td><td>Fast interrupt is used to detect link changes. Some devices do not offer interrupts on all ports. Using this setting stops additional polling which results in even faster and more uniform detection time.</td></tr> </table> <p>OID 1.3.6.1.4.1.3181.10.6.1.30.17.1.2 (compatibilityLinkDetection)</p>	<i>POLL_AND_INTERRUPT</i>	Normal mode. When possible interrupts are used. Polling catches devices without interrupt capability.	<i>INTERRUPT_ONLY</i>	Fast interrupt is used to detect link changes. Some devices do not offer interrupts on all ports. Using this setting stops additional polling which results in even faster and more uniform detection time.		
<i>POLL_AND_INTERRUPT</i>	Normal mode. When possible interrupts are used. Polling catches devices without interrupt capability.						
<i>INTERRUPT_ONLY</i>	Fast interrupt is used to detect link changes. Some devices do not offer interrupts on all ports. Using this setting stops additional polling which results in even faster and more uniform detection time.						

14.5 System Status Parameters

Group Path	General Parameters		
	Device.System		
last_boot_time	The time and date when this device has booted.		
	Value	String, max. 32 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.30.100 (systemLastBootTime)	
uptime	Uptime since last reboot in seconds.		
	Value	PERIOD0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.1.30.101 (systemUptime) 1.3.6.1.2.1.1.3 (sysUpTime)	
used_mac_address	Contains the mac address used by this unit. Usually follows to MAC defined in the factory setting, but may be overwritten by the alternative_mac_address.		
	Format	MAC Address hh-hh-hh-hh-hh-hh (hh = hexadecimal number between 00 to ff)	
	OID	1.3.6.1.4.1.3181.10.6.1.30.102 (systemUsedMacAddress) 1.3.6.1.2.1.17.1.1 (dot1dBaseBridgeAddress) 1.0.8802.1.1.2.1.3.2 (lldpLocChassisId) 1.0.8802.1.1.2.1.3.8.1.2 (lldpLocManAddr) 1.3.6.1.2.1.2.2.1.6 (ifPhysAddress)	
used_boot_media			
	Values	SD_CARD	System booted from SD card
		INTERNAL_MEMORY	System booted from internal memory
		NFS	System booted via network file system
	OID	1.3.6.1.4.1.3181.10.6.1.30.103 (systemUsedBootMedia)	
temperature	Temperature value in centigrade.		
	Value	Number in range 0-255	
	OID	1.3.6.1.4.1.3181.10.6.1.30.104 (systemTemperature)	

climate_level	Annotated temperature level.		
	Values	<i>UNKNOWN</i> No thermometer available <i>CRITICAL_LOW</i> Temperature is below the specified operating range <i>LOW</i> Temperature is low <i>NORMAL</i> Normal operating temperature <i>INCREASED</i> Temperature higher than normal <i>HIGH</i> Temperature is high and should increase much more <i>CRITICAL_HIGH</i> Too high, device will switch all Gigabit Ethernet ports to Fast Ethernet. This down speed will prevail until climate level INCREASED to reached <i>SHUTDOWN</i> The device is extremely hot and will switch off the ports completely to protect itself. It will only recover once climate level HIGH is reached or the system is rebooted.	
	OID	1.3.6.1.4.1.3181.10.6.1.30.105 (systemClimateLevel)	

Group	firmware
Path	Device.System.firmware
Description	This section provides details about the running firmware.

running_version	Running firmware version.		
	Value	String, max. 32 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.30.106.1.2 (firmwareRunningVersion) 1.3.6.1.2.1.47.1.1.1.1.10 (entPhysicalSoftwareRev) 1.0.8802.1.1.2.1.5.4795.1.2.4.0 (lldpXMedLocSoftwareRev)	

build_date	Build date of the running firmware. Format: 2012-01-18 12:00:22.		
	Value	String, max. 32 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.30.106.1.3 (firmwareBuildDate)	

build_number	Build number of the running firmware retrieved from the repository.		
	Value	String, max. 8 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.30.106.1.4 (firmwareBuildNumber) 1.3.6.1.2.1.47.1.1.1.1.9 (entPhysicalFirmwareRev) 1.0.8802.1.1.2.1.5.4795.1.2.3.0 (lldpXMedLocFirmwareRev)	

patch_version	If extra patches are installed, their version(s) are indicated here.		
	Value	String, max. 32 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.30.106.1.5 (firmwarePatchVersion)	

Group	save_info	
Path	Device.System.save_info	
Description	This section provided status information about the internal parameter saving process.	
last_saved_parameter	Records the last written parameter.	
	Value	String, max. 128 characters.
	OID	1.3.6.1.4.1.3181.10.6.1.30.107.1.2 (saveInfoLastSavedParameter)
save_mode	Reflects Device.system.configuration_save_mode setting.	
	Values	<i>PERMANENTLY</i> Normal mode. A changes are saved on the SD card or internal memory <i>TEMPORARILY</i> Configuration is only saved in RAM
	OID	1.3.6.1.4.1.3181.10.6.1.30.107.1.3 (saveInfoSaveMode)
write_status	Indicates if last parameter was written to SD card or temporary RAM.	
	Values	<i>NOTHING_TO_SAVE</i> There have been no writes since last system boot <i>PROCESSING</i> Parameter is being processed. This should be very brief state and is typically not seen. If this state persists an error may be indicated <i>SAVED_TO_RAM</i> The parameter was internally processed, executed and saved in RAM copy of configuration <i>SAVED_TO_SDCARD</i> The parameter was successfully written to the SD card. This is the normal state.
	OID	1.3.6.1.4.1.3181.10.6.1.30.107.1.4 (saveInfoWriteStatus)
time_stamp	Records the time the write status was last changed.	
	Value	TIMESTAMP0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.30.107.1.5 (saveInfoTimeStamp)

15 Hardware Information

15.1 Key Features

Function

Fanless Layer 2+ Switch controlled by high speed 1Ghz ARM CPU.
Latest technology.

Green IT

State-of-the-Art chip technology supports Energy Efficient Ethernet (EEE) according to IEEE 802.3az.

Most energy efficient switch type.

Jumbo Frames

Supports Jumbo-Frames up to 10kBytes length.

Modular Hardware Design

(Industrial Switch only)

Modular in-field upgradable hardware design enclosed in sturdy stainless steel stackable unit.
Especially compact device.

Industry Switch can grow and adapt to customer needs. Very robust package despite modularity.

RGB LED

Full color led indicators permit extensive yet easy to remember status decoding without any tools.
Quiet mode turns off most led for unobtrusive operation. Lightshow mode helps to find a switch among others.

Quick status checking without any tools. Quiet and dark modes intended for office environment where obtrusive blinking is undesirable.

Input / Output Pins

(Industrial Switch only)

Two decoupled input pins and two relay outputs are available in the Industry Switch. Signal changes at the input pins will trigger events (Syslog, Traps). These event can also trigger user defined cli scripts file for flexible use. The relays may be triggered on power, redundancy or thermal problems. Relays and LEDs can be set to static or blink mode. Relays may also be controlled via scripts for full custom control.

May be used to control external ventilation or alarm systems. Input may connect to door contact or UPS error signal for example. Input can trigger any desired system action due to scripting feature.

15.2 Functional Description

This section contains information about hardware status and display configuration.

15.3 Hardware CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Device.	hardware.					Basic device configuration and information
			led_test		X	Runs a LED test whereby all LED light up in all possible colors for checking their function. The tests terminates within a few seconds.
			led_mode		R/W	The LED display can be configured to be less intrusive.
			power_supply_1_monitored		R/W	When disabled a missing power supply 1 will not turn the associated led red on failure. Do this when single power supply 2 operation is used or when the device is powered solely by PoE. This feature only applies to industrial switches.
			power_supply_2_monitored		R/W	When disabled a missing power supply 2 will not turn the associated led red on failure. Do this when single power supply 1 operation is used or when the device is powered solely by PoE. This feature only applies to industrial switches.
			factory_reset_button		R/W	When disabled the factory button will trigger the factory reset function when pressed for a long time. The IP discover function upon a short button click is not affected.
			cable_test_config[PORT].			The cable tester allows for detection of copper cable faults and can even detect where the fault is located. By using a OTDR SFP, measurements can also be done on fiber ports
			enable_auto_cable_test		R/W	When enabled a cable test is performed each time the link goes down. The test is only performed for copper ports, dual media ports in copper mode or when an OTDR SFP is detected.
			event_generation		R/W	When the cable termination status changes or a change in the fiber is detected an event can be raised.

reflection_threshold	R/W	Select a value up to 508 which is used to decide between a connected cable and a remotely disconnected cable. With actively terminated data ports, the detection is difficult and precise setup is required. Please refer to cable_test_status.reflection_value for further details. Applies to copper only.
reflection_hysteresis	R/W	Choose value to prevent oscillation when reflection value is slightly shifting. For OTDR measurement, the value is interpreted as minimum meters of change in a reflection for it to be considered a different reflection.
start_test_now	X	May be used to manually start a cable test. ATTENTION: If the port is in link up status it will be forced to link down first. This will disrupt the current data traffic. Therefore, type start_test_now = CONFIRM.
create_reference	X	Is used to start a OTDR reference measurement. Only applies to optical cables with the required SFP installed. Type create_reference = CONFIRM.
reference_data	R/W	The content of this field is created with the create_reference action command and should not be edited manually.
io_signal_config.		
signal_mode	R/W	Permit setting of I/O signal LEDs and relays to static or blink mode for increased visualization.
input_1_mode	R/W	When this function is activated the external alarm input 1 is monitored. Note: alarm inputs are not available in all product versions.
input_1_name	R/W	A customer specific name can be specified for input 1. This name will appear in the associated event messages. The name (up to the first blank) determines the attribute used in SmartOffice context.
input_2_mode	R/W	When this function is activated the external alarm input 2 is monitored. Note: alarm inputs are not available in all product versions.
input_2_name	R/W	A customer specific name can be specified for input 2. This name will appear in the associated event messages. The name (up to the first blank) determines the attribute used in SmartOffice context.

output_1_trigger	R/W	Defines on which condition the alarm relay 1 is activated. Note: alarm relays are not available in all product versions.
output_1_name	R/W	A customer specific name can be specified for alarm output 1. This name will appear in the associated event messages. The name (up to the first blank) determines the attribute used in SmartOffice context.
output_2_trigger	R/W	Defines on which condition the alarm relay 2 is activated. Note: alarm relays are not available in all product versions.
output_2_name	R/W	A customer specific name can be specified for alarm output 2. This name will appear in the associated event messages. The name (up to the first blank) determines the attribute used in SmartOffice context.
power_supply_1_status	R	Displays state of primary supply or only supply for single supply systems.
power_supply_2_status	R	Displays state of secondary supply if available.
running_on_poe	R	When set the unit currently operates on the PD input via PoE.
fan_status	R	Displays state of cooling fan. Indicates UNUSED in fanless devices.
sd_card_status	R	Current status of SD-card.
num_of_ports	R	Total number of Ethernet ports this hardware offers.
mask_of_existing_ports	R	Set bit for each port that physically existing and could be in use.
mask_of_sfp_ports	R	Marks which ports support SFPs.
mask_of_poe_ports	R	Marks which ports support PoE output.
module_info[4].		This section indicates which modules are inserted in the optional extension slots.
unit_type	R	Identifies the general type of module.
article_number	R	The article number of the module in this slot.
serial_number	R	The serial number of the module in this slot.
hardware_version	R	This device hardware revision number.
project_number	R	MICROSENS project number.
occupied_slots	R	Lists all slots contained in this module.
description	R	Feature summary of the module.

slot_info[8].		This section indicates which modules are inserted in the optional extension slots.
board_type	R	General type of board function
board_id	R	This identifies the board type for internal operation.
version_bits	R	Version bits from hardware or backplane.
port_info[PORT].		Used to map physical to logical port ids.
system_slot	R	Describes on which system slot this port index is located.
switch_port	R	Describes on which switch port this port index is located.
user_slot	R	Slot number as seen by customer.
user_port	R	Port number as seen by customer.
snmp_port	R	Slot and port representation as used in SNMP. Formula is Slot*100 + Port.
snmp_instance	R	Port instance counting from 0 to number of ports
hardware_port	R	Port number as used internally. Ports may not be in sequential order.
interface_type	R	Identifies port as copper or optical. Also used for snmp ifType definition
properties	R	Describes which functions the port can support.
port_names[PORT].		This table contains additional port information names suitable for use in snmp.
cli_name	R	Port name as used in cli and as required for ifName (read only)
port_description	R	Port name as required for ifDescription (read only)
port_leds[PORT].		This section indicates the state of all port related LEDs.
ethernet_color	R	Ethernet Link LED.
ethernet_blinking	R	Ethernet Link LED.
poe_color	R	Power over Ethernet LED. For optical ports this indicates signal detect status.
poe_blinking	R	Power over Ethernet LED. For optical ports this indicates signal detect status.
device_leds.		This section indicates the state of all LEDs which are not port related. Please note: Not every unit offers all LEDs.
system_1_color	R	This status corresponds to 'sys' LED on some devices.
system_1_blinking	R	This status corresponds to 'sys' LED on some devices.

system_2_color	R	Displays external management activity.
system_2_blinking	R	Displays external management activity.
power_on_1_color	R	This status corresponds to 'on' LED on some devices.
power_on_1_blinking	R	This status corresponds to 'on' LED on some devices.
power_on_2_color	R	Alternative power input LED.
power_on_2_blinking	R	Alternative power input LED.
ring_1_color	R	This LED is used when ring protection is enabled.
ring_1_blinking	R	This LED is used when ring protection is enabled.
ring_2_color	R	This LED is used when ring protection is enabled.
ring_2_blinking	R	This LED is used when ring protection is enabled.
signal_in_1_color	R	Indicates status of alarm input 1.
signal_in_1_blinking	R	Indicates status of alarm input 1.
signal_in_2_color	R	Indicates status of alarm input 2.
signal_in_2_blinking	R	Indicates status of alarm input 2.
signal_out_1_color	R	Indicates status of alarm relay output 1.
signal_out_1_blinking	R	Indicates status of alarm relay output 1.
signal_out_2_color	R	Indicates status of alarm relay output 2.
signal_out_2_blinking	R	Indicates status of alarm relay output 2.
cable_test_status[PORT].		This table display the result of the last cable test. Values are only available for copper ports while a link is down and if the cable test function is enabled or for optical ports with an OTDR SFP present
update_time_stamp	R	Indicates the time when this record was last updated.
pair_0_state	R	Indicates line termination test results for wire pair 0 (Pins 1/2). Applies to copper only.
pair_0_distance_to_fault	R	Distance to fault on wire pair 0 in centimeters. Indicates 0 when no fault is detected or the function is unused. Applies to copper only.
pair_1_state	R	Indicates line termination test results for wire pair 1 (Pins 3/6). Applies to copper only.
pair_1_distance_to_fault	R	Distance to fault on wire pair 1 in centimeters. Indicates 0 when no fault is detected or the function is unused. Applies to copper only.
pair_2_state	R	Indicates line termination test results for wire pair 2 (Pins 4/5). Applies to copper only.

pair_2_distance_to_fault	R	Distance to fault on wire pair 2 in centimeters. Indicates 0 when no fault is detected or the function is unused. Applies to copper only.
pair_3_state	R	Indicates line termination test results for wire pair 3 (Pins 7/8). Applies to copper only.
pair_3_distance_to_fault	R	Distance to fault on wire pair 3 in centimeters. Indicates 0 when no fault is detected or the function is unused. Applies to copper only.
reflection_value	R	A unitless value that indicates a measure of reflection level. For difficult to detect actively terminated devices perform a measurement with remotely plugged-in and then unplugged cable. Note the reflection values and choose a value in the middle as reflection_threshold configuration value. Applies to copper only.
cable_status	R	Indicates the concluded status summary. Applies to copper only.
current_otdr_reflections	R	Number and location of currently detected reflections for an active OTDR SFP on this port.
io_signal_status.		This section is only used for devices which offer external signal inputs and outputs.
input_1_alarm_active	R	Indicates true when the input 1 is logically active.
input_2_alarm_active	R	Indicates true when the input 2 is logically active.
output_1_relay_active	R	Indicates true when the output 1 relay is activated.
output_2_relay_active	R	Indicates true when the output 2 relay is activated.
tcam_status[256].		The TCAM is a programmable wire speed packet filter. The filter is controlled by the system automatically. This table indicates which filters have been set.
control_file	R	Reflects the name of the control file associated with this tam entry.
description	R	Descriptive text what explains what this TCAM entry will do.

15.4 Hardware Configuration Parameters

Group Path	General Parameters										
	Device.Hardware										
led_test	<p>Runs a LED test whereby all LED light up in all possible colors for checking their function. The tests terminates within a few seconds.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.31.1 (hardwareLedTest)</p>										
led_mode	<p>The LED display can be configured to be less intrusive.</p> <p>Values</p> <table> <tr> <td><i>DYNAMIC</i></td><td>LED display static states and blink when data is present on a port</td></tr> <tr> <td><i>STATIC</i></td><td>LED display static states but do not blink with data</td></tr> <tr> <td><i>QUIET</i></td><td>Display is reduced to sys and on LED. Port LEDs remain off</td></tr> <tr> <td><i>DARK</i></td><td>All LED are off. This mode is not recommended as the unit may mistakenly be deemed powered down</td></tr> <tr> <td><i>LIGHTSHOW</i></td><td>This mode is similar to a led_test but permanent. This may be turned on to easier locate a physical unit among others.</td></tr> </table> <p>OID 1.3.6.1.4.1.3181.10.6.1.31.2 (hardwareLedMode)</p>	<i>DYNAMIC</i>	LED display static states and blink when data is present on a port	<i>STATIC</i>	LED display static states but do not blink with data	<i>QUIET</i>	Display is reduced to sys and on LED. Port LEDs remain off	<i>DARK</i>	All LED are off. This mode is not recommended as the unit may mistakenly be deemed powered down	<i>LIGHTSHOW</i>	This mode is similar to a led_test but permanent. This may be turned on to easier locate a physical unit among others.
<i>DYNAMIC</i>	LED display static states and blink when data is present on a port										
<i>STATIC</i>	LED display static states but do not blink with data										
<i>QUIET</i>	Display is reduced to sys and on LED. Port LEDs remain off										
<i>DARK</i>	All LED are off. This mode is not recommended as the unit may mistakenly be deemed powered down										
<i>LIGHTSHOW</i>	This mode is similar to a led_test but permanent. This may be turned on to easier locate a physical unit among others.										
power_supply_1_monitored	<p>When disabled a missing power supply 1 will not turn the associated led red on failure. Do this when single power supply 2 operation is used or when the device is powered solely by PoE. This feature only applies to industrial switches.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.31.3 (hardwarePowerSupply1Monitored)</p>										
power_supply_2_monitored	<p>When disabled a missing power supply 2 will not turn the associated led red on failure. Do this when single power supply 1 operation is used or when the device is powered solely by PoE. This feature only applies to industrial switches.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.31.4 (hardwarePowerSupply2Monitored)</p>										
factory_reset_button	<p>When disabled the factory button will trigger the factory reset function when pressed for a long time. The IP discover function upon a short button click is not affected.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.31.5 (hardwareFactoryResetButton)</p>										

Group	cable_test_config , for each port[0..24]								
Path	Device.Hardware.cable_test_config[port]								
Description	The cable tester allows for detection of copper cable faults and can even detect where the fault is located. By using a OTDR SFP, measurements can also be done on fiber ports								
<hr/>									
enable_auto_cable_test	When enabled a cable test is performed each time the link goes down. The test is only performed for copper ports, dual media ports in copper mode or when an OTDR SFP is detected.								
	Values	enabled, disabled							
	OID	1.3.6.1.4.1.3181.10.6.1.31.6.1.2 (cableTestConfigEnableAutoCableTest)							
<hr/>									
event_generation	When the cable termination status changes or a change in the fiber is detected an event can be raised.								
	Values	<table><tr><td><i>DISABLED</i></td><td>No events are generated</td></tr><tr><td><i>ANY_CHANGE</i></td><td>Any termination or length change on any cable pair will trigger an event</td></tr><tr><td><i>CONNECTIONS_ONLY</i></td><td>Only change of connection events will be generated. (Remote device is plugged-in or unplugged)</td></tr></table>		<i>DISABLED</i>	No events are generated	<i>ANY_CHANGE</i>	Any termination or length change on any cable pair will trigger an event	<i>CONNECTIONS_ONLY</i>	Only change of connection events will be generated. (Remote device is plugged-in or unplugged)
<i>DISABLED</i>	No events are generated								
<i>ANY_CHANGE</i>	Any termination or length change on any cable pair will trigger an event								
<i>CONNECTIONS_ONLY</i>	Only change of connection events will be generated. (Remote device is plugged-in or unplugged)								
	OID	1.3.6.1.4.1.3181.10.6.1.31.6.1.3 (cableTestConfigEventGeneration)							
<hr/>									
reflection_threshold	Select a value up to 508 which is used to decide between a connected cable and a remotely disconnected cable. With actively terminated data ports, the detection is difficult and precise setup is required. Please refer to cable_test_status.reflection_value for further details. Applies to copper only.								
	Value	Number in range 0-65535							
	OID	1.3.6.1.4.1.3181.10.6.1.31.6.1.4 (cableTestConfigReflectionThreshold)							
<hr/>									
reflection_hysteresis	Choose value to prevent oscillation when reflection value is slightly shifting. For OTDR measurement, the value is interpreted as minimum meters of change in a reflection for it to be considered a different reflection.								
	Value	Number in range 0-65535							
	OID	1.3.6.1.4.1.3181.10.6.1.31.6.1.5 (cableTestConfigReflectionHysteresis)							
<hr/>									
start_test_now	May be used to manually start a cable test. ATTENTION: If the port is in link up status it will be forced to link down first. This will disrupt the current data traffic. Therefore, type start_test_now = CONFIRM.								
	Action	Excecute command with parameter string max. 10 characters.							
	OID	1.3.6.1.4.1.3181.10.6.1.31.6.1.6 (cableTestConfigStartTestNow)							

create_reference	Is used to start a OTDR reference measurement. Only applies to optical cables with the required SFP installed. Type create_reference = CONFIRM.								
	Action	Excecute command with parameter string max. 10 characters.							
	OID	1.3.6.1.4.1.3181.10.6.1.31.6.1.7 (cableTestConfigCreateReference)							
reference_data	The content of this field is created with the create_reference action command and should not be edited manually.								
	Value	String, max. 256 characters.							
	OID	1.3.6.1.4.1.3181.10.6.1.31.6.1.8 (cableTestConfigReferenceData)							
Group	io_signal_config								
Path	Device.Hardware.io_signal_config								
Description									
signal_mode	Permit setting of I/O signal LEDs and relays to static or blink mode for increased visualization.								
	Values	<table><tr><td>STATIC</td><td>LEDs and relays or either on or off. No blinking</td></tr><tr><td>LED_BLINK</td><td>The I/O related LEDs blink when active. The relays switch statically</td></tr><tr><td>RELAY_BLINK</td><td>Both, I/O related LEDs and relays blink when active</td></tr></table>		STATIC	LEDs and relays or either on or off. No blinking	LED_BLINK	The I/O related LEDs blink when active. The relays switch statically	RELAY_BLINK	Both, I/O related LEDs and relays blink when active
STATIC	LEDs and relays or either on or off. No blinking								
LED_BLINK	The I/O related LEDs blink when active. The relays switch statically								
RELAY_BLINK	Both, I/O related LEDs and relays blink when active								
	OID	1.3.6.1.4.1.3181.10.6.1.31.7.1.2 (ioSignalConfigSignalMode)							
input_1_mode	When this function is activated the external alarm input 1 is monitored. Note: alarm inputs are not available in all product versions.								
	Values	<table><tr><td>DISABLED</td><td>This input is not monitored and also not updated in SmartOffice.</td></tr><tr><td>ALARM_WHEN_HIGH</td><td>An alarm is raised when the signal is level is high. In SmartOffice the sensor value turns active when input level is high.</td></tr><tr><td>ALARM_WHEN_LOW</td><td>An alarm is raised when the signal is low (GND) or not connected. In SmartOffice the sensor value turns active when input level is low. (inverted)</td></tr></table>		DISABLED	This input is not monitored and also not updated in SmartOffice.	ALARM_WHEN_HIGH	An alarm is raised when the signal is level is high. In SmartOffice the sensor value turns active when input level is high.	ALARM_WHEN_LOW	An alarm is raised when the signal is low (GND) or not connected. In SmartOffice the sensor value turns active when input level is low. (inverted)
DISABLED	This input is not monitored and also not updated in SmartOffice.								
ALARM_WHEN_HIGH	An alarm is raised when the signal is level is high. In SmartOffice the sensor value turns active when input level is high.								
ALARM_WHEN_LOW	An alarm is raised when the signal is low (GND) or not connected. In SmartOffice the sensor value turns active when input level is low. (inverted)								
	OID	1.3.6.1.4.1.3181.10.6.1.31.7.1.3 (ioSignalConfigInput1Mode)							
input_1_name	A customer specific name can be specified for input 1. This name will appear in the associated event messages. The name (up to the first blank) determines the attribute used in SmartOffice context.								
	Value	String, max. 32 characters.							
	OID	1.3.6.1.4.1.3181.10.6.1.31.7.1.4 (ioSignalConfigInput1Name)							

input_2_mode	When this function is activated the external alarm input 2 is monitored. Note: alarm inputs are not available in all product versions.	
Values	<i>DISABLED</i>	This input is not monitored and also not updated in SmartOffice.
	<i>ALARM_WHEN_HIGH</i>	An alarm is raised when the signal is level is high. In SmartOffice the sensor value turns active when input level is high.
	<i>ALARM_WHEN_LOW</i>	An alarm is raised when the signal is low (GND) or not connected. In SmartOffice the sensor value turns active when input level is low. (inverted)
OID	1.3.6.1.4.1.3181.10.6.1.31.7.1.5 (ioSignalConfigInput2Mode)	
input_2_name	A customer specific name can be specified for input 2. This name will appear in the associated event messages. The name (up to the first blank) determines the attribute used in SmartOffice context.	
Value	String, max. 32 characters.	
OID	1.3.6.1.4.1.3181.10.6.1.31.7.1.6 (ioSignalConfigInput2Name)	
output_1_trigger	Defines on which condition the alarm relay 1 is activated. Note: alarm relays are not available in all product versions.	
Values	<i>DISABLED</i>	The relay is not energized. Normal when relay feature is not used
	<i>WHILE_RUNNING</i>	The relay is always energized while the system in operating but will turn off when all power is lost. This may be used to indicate complete power outage or major system failure. The relay will not blink in this mode regardless of signal_mode setting. The relay led indicates green.
	<i>REDUNDANCY_FAIL</i>	The relay is energized when a redundant power supply is failing but the system is still operating on another supply.
	<i>HIGH_TEMP</i>	The relay is energized when the climate_level is HIGH or worse to indicate a hot environment. This could be used to control external ventilation.
	<i>OFF</i>	The relay is not energized. The associated LED turns green and does not blink. This mode is intended for script usage.
	<i>ON</i>	The relay is energized and the associated LED turns red. When blink mode is used, the relay will blink as well. This mode is intended for script usage.
	<i>SMART_OFFICE</i>	The relay is made available as actor and can be used by the SmartOffice sub system like any other actor.
OID	1.3.6.1.4.1.3181.10.6.1.31.7.1.7 (ioSignalConfigOutput1Trigger)	

output_1_name	A customer specific name can be specified for alarm output 1. This name will appear in the associated event messages. The name (up to the first blank) determines the attribute used in SmartOffice context.	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.1.31.7.1.8 (ioSignalConfigOutput1Name)
output_2_trigger	Defines on which condition the alarm relay 2 is activated. Note: alarm relays are not available in all product versions.	
	Values	<div data-bbox="724 542 1414 595"><i>DISABLED</i> The relay is not energized. Normal when relay feature is not used</div> <div data-bbox="724 607 1414 817"><i>WHILE_RUNNING</i> The relay is always energized while the system is operating but will turn off when all power is lost. This may be used to indicate complete power outage or major system failure. The relay will not blink in this mode regardless of signal_mode setting. The relay led indicates green.</div> <div data-bbox="724 828 1414 907"><i>REDUNDANCY_FAIL</i> The relay is energized when a redundant power supply is failing but the system is still operating on another supply.</div> <div data-bbox="724 918 1414 1023"><i>HIGH_TEMP</i> The relay is energized when the climate_level is HIGH or worse to indicate a hot environment. This could be used to control external ventilation.</div> <div data-bbox="724 1034 1414 1140"><i>OFF</i> The relay is not energized. The associated LED turns green and does not blink. This mode is intended for script usage.</div> <div data-bbox="724 1151 1414 1256"><i>ON</i> The relay is energized and the associated LED turns red. When blink mode is used, the relay will blink as well. This mode is intended for script usage.</div> <div data-bbox="724 1267 1414 1346"><i>SMART_OFFICE</i> The relay is made available as actor and can be used by the SmartOffice sub system like any other actor.</div>
	OID	1.3.6.1.4.1.3181.10.6.1.31.7.1.9 (ioSignalConfigOutput2Trigger)
output_2_name	A customer specific name can be specified for alarm output 2. This name will appear in the associated event messages. The name (up to the first blank) determines the attribute used in SmartOffice context.	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.1.31.7.1.10 (ioSignalConfigOutput2Name)

15.5 Hardware Status Parameters

Group Path	General Parameters	
	Device.Hardware	
power_supply_1_status	Displays state of primary supply or only supply for single supply systems.	
	Values	<i>OK</i> Normal operating condition <i>OVERLOAD</i> Too much current drawn or short circuit <i>INPUT_LOW</i> Input voltage too low <i>FUSE_FAIL</i> Fuse blown <i>NOT_APPLICABLE</i> Secondary power supply is not an option for this product <i>UNMANAGED</i> Power supply monitoring for this supply is disabled <i>NOT_INSTALLED</i> Power supply is not installed
	OID	1.3.6.1.4.1.3181.10.6.1.31.100 (hardwarePowerSupply1Status)
power_supply_2_status	Displays state of secondary supply if available.	
	Values	<i>OK</i> Normal operating condition <i>OVERLOAD</i> Too much current drawn or short circuit <i>INPUT_LOW</i> Input voltage too low <i>FUSE_FAIL</i> Fuse blown <i>NOT_APPLICABLE</i> Secondary power supply is not an option for this product <i>UNMANAGED</i> Power supply monitoring for this supply is disabled <i>NOT_INSTALLED</i> Power supply is not installed
	OID	1.3.6.1.4.1.3181.10.6.1.31.101 (hardwarePowerSupply2Status)
running_on_poe	When set the unit currently operates on the PD input via PoE.	
	Values	true, false
	OID	1.3.6.1.4.1.3181.10.6.1.31.102 (hardwareRunningOnPoe)
fan_status	Displays state of cooling fan. Indicates UNUSED in fanless devices.	
	Values	<i>UNUSED</i> Fanless device without internal cooling fan or a device with unmanaged fan. <i>OK</i> Fan cooled device. Fan appears to be working fine <i>DEGRADED</i> Fan is operating with reduced effectiveness. Check soon <i>FAIL</i> Fan has failed and insufficient cooling is available. Replace fan as soon as possible <i>MISSING</i> Fan cooled device but fan is not installed
	OID	1.3.6.1.4.1.3181.10.6.1.31.103 (hardwareFanStatus)

sd_card_status	Current status of SD-card.		
	Values	EMPTY	No SD card is inserted
		INSERTED	SD card is inserted
		WRITE_PROTECTED	SD card cannot be written
		WRITING	Currently being written. Do not remove
	OID	1.3.6.1.4.1.3181.10.6.1.31.104 (hardwareSdCardStatus)	

num_of_ports	Total number of Ethernet ports this hardware offers.		
	Value	Number in range 0-255	
	OID	1.3.6.1.4.1.3181.10.6.1.31.105 (hardwareNumOfPorts) 1.3.6.1.2.1.17.1.2 (dot1dBaseNumPorts)	

mask_of_existing_ports	Set bit for each port that physically existing and could be in use.		
	Value	PORTMASK0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.1.31.106 (hardwareMaskOfExistingPorts)	

mask_of_sfp_ports	Marks which ports support SFPs.		
	Value	PORTMASK0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.1.31.107 (hardwareMaskOfSfpPorts)	

mask_of_poe_ports	Marks which ports support PoE output.		
	Value	PORTMASK0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.1.31.108 (hardwareMaskOfPoePorts)	

Group	slot_info, for all device slots[0..7]		
Path	Device.Hardware.slot_info[slot]		
Description	This section indicates which modules are inserted in the optional extension slots.		

board_type	General type of board function		
	Values	NOT_PRESENT	Possible slot is not installed
		UNDEFINED	Unspecified features
		POWER	Power supply module
		CPU	Main CPU module
		PORT	Port
		IO	Input/Output module
		10G_PORT	10G switch port module
		OID	1.3.6.1.4.1.3181.10.6.1.31.110.1.2 (slotInfoBoardType)

board_id	This identifies the board type for internal operation.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.31.110.1.3 (slotInfoBoardId)
version_bits	Version bits from hardware or backplane.	
	Value	Number in range 0-255
	OID	1.3.6.1.4.1.3181.10.6.1.31.110.1.4 (slotInfoVersionBits)
Group	port_info , for each port[0..24]	
Path	Device.Hardware.port_info[port]	
Description	Used to map physical to logical port ids.	
system_slot	Describes on which system slot this port index is located.	
	Value	Number in range 0-255
	OID	1.3.6.1.4.1.3181.10.6.1.31.111.1.2 (portInfoSystemSlot)
switch_port	Describes on which switch port this port index is located.	
	Value	Number in range 0-255
	OID	1.3.6.1.4.1.3181.10.6.1.31.111.1.3 (portInfoSwitchPort) 1.3.6.1.2.1.105.1.1.1.7 (pethPsePortPowerPriority)
user_slot	Slot number as seen by customer.	
	Value	Number in range 0-255
	OID	1.3.6.1.4.1.3181.10.6.1.31.111.1.4 (portInfoUserSlot)
user_port	Port number as seen by customer.	
	Value	Number in range 0-255
	OID	1.3.6.1.4.1.3181.10.6.1.31.111.1.5 (portInfoUserPort)
snmp_port	Slot and port representation as used in SNMP. Formula is Slot*100 + Port.	
	Value	Number in range 0-65535
	OID	1.3.6.1.4.1.3181.10.6.1.31.111.1.6 (portInfoSnmpPort) 1.3.6.1.2.1.2.2.1.1 (ifIndex) 1.3.6.1.2.1.10.7.2.1.1 (dot3StatsIndex) 1.3.6.1.2.1.16.1.1.1.1 (etherStatsIndex) 1.0.8802.1.1.2.1.3.7.1.1 (lldpLocPortNum) 1.0.8802.1.1.2.1.3.7.1.3 (lldpLocPortId) 1.3.6.1.2.1.105.1.1.1.2 (pethPsePortIndex) 1.3.6.1.2.1.17.1.4.1.2 (dot1dBasePortIfIndex) 1.3.6.1.2.1.17.1.4.1.1 (dot1dBasePort)

snmp_instance	Port instance counting from 0 to number of ports	
	Value	Number in range 0-255
	OID	1.3.6.1.4.1.3181.10.6.1.31.111.1.7 (portInfoSnmpInstance) 1.3.6.1.2.1.17.2.15.1.1 (dot1dStpPort)
hardware_port	Port number as used internally. Ports may not be in sequential order.	
	Value	Number in range 0-255
	OID	1.3.6.1.4.1.3181.10.6.1.31.111.1.8 (portInfoHardwarePort)
interface_type	Identifies port as copper or optical. Also used for snmp ifType definition	
	Values	<i>COPPER</i> Normal copper interface
		<i>OPTICAL</i> Optical interface
		<i>DUAL_MEDIA</i> Copper and optical interface supported
	OID	1.3.6.1.4.1.3181.10.6.1.31.111.1.9 (portInfoInterfaceType) 1.3.6.1.2.1.2.2.1.3 (ifType)
properties	Describes which functions the port can support.	
	Values	<i>NOT_DETECTED</i> Default value. Port not yet discovered or not existing
		<i>INTERNAL</i> This is an internal port no accessible to the user
		<i>10_MB</i> This port is capable of running at 10Mbit/s
		<i>100_MB</i> This port is capable of running at 100Mbit/s
		<i>1000_MB</i> This port is capable of running at 1000Mbit/s
		<i>RJ45</i> This port uses as RJ45 connector
		<i>SFP</i> This port uses a pluggable SFP
		<i>1X9</i> This port uses fixed optical SC connector
		<i>POE</i> This port is capable to supply Power over Ethernet (PoE)
		<i>POE_PLUS</i> This port is capable to supply Power over Ethernet Extended (PoE+)
		<i>PD</i> This port can accept PoE to operate the device
		<i>DUAL_MEDIA</i> This is a dual media port for optical or electrical operation
		<i>LINK_PORT</i> This is a link port which should not be disabled
		<i>CSFP</i> This port is the second port of double port compact SFP
	OID	1.3.6.1.4.1.3181.10.6.1.31.111.1.10 (portInfoProperties)

Group	port_names , for each port[0..24]	
Path	Device.Hardware.port_names[port]	
Description	This table contains additional port information names suitable for use in snmp.	
cli_name	Port name as used in cli and as required for ifName (read only)	
	Value	String, max. 8 characters.
	OID	1.3.6.1.4.1.3181.10.6.1.31.112.1.2 (portNamesCliName) 1.3.6.1.2.1.31.1.1.1.1 (ifName)
port_description	Port name as required for ifDescription (read only)	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.1.31.112.1.3 (portNamesPortDescription) 1.3.6.1.2.1.2.2.1.2 (ifDescr)
Group	port_leds , for all ports[0..31]	
Path	Device.Hardware.port_leds[port]	
Description	This section indicates the state of all port related LEDs.	
ethernet_color	Ethernet Link LED.	
	Values	<i>OFF</i> LED is off
		<i>BLUE</i> LED indicates blue
		<i>GREEN</i> LED indicates green
		<i>RED</i> LED indicates red
		<i>ORANGE</i> LED indicates orange (yellow)
		<i>CYAN</i> LED indicates cyan
		<i>MAGENTA</i> LED indicates magenta
		<i>WHITE</i> LED indicates white
		<i>NO_LED</i> This LED does physically not exist in this device
	OID	1.3.6.1.4.1.3181.10.6.1.31.113.1.2 (portLedsEthernetColor)
ethernet_blinking	Ethernet Link LED.	
	Values	true, false
	OID	1.3.6.1.4.1.3181.10.6.1.31.113.1.3 (portLedsEthernetBlinking)

poe_color Power over Ethernet LED. For optical ports this indicates signal detect status.

Values	<i>OFF</i>	LED is off
	<i>BLUE</i>	LED indicates blue
	<i>GREEN</i>	LED indicates green
	<i>RED</i>	LED indicates red
	<i>ORANGE</i>	LED indicates orange (yellow)
	<i>CYAN</i>	LED indicates cyan
	<i>MAGENTA</i>	LED indicates magenta
	<i>WHITE</i>	LED indicates white
	<i>NO_LED</i>	This LED does physically not exist in this device
OID	1.3.6.1.4.1.3181.10.6.1.31.113.1.4 (portLedsPoeColor)	

poe_blinking Power over Ethernet LED. For optical ports this indicates signal detect status.

Values	true, false
OID	1.3.6.1.4.1.3181.10.6.1.31.113.1.5 (portLedsPoeBlinking)

Group	cable_test_status , for each port[0..24]
Path	Device.Hardware.cable_test_status[port]
Description	This table display the result of the last cable test. Values are only available for copper ports while a link is down and if the cable test function is enabled or for optical ports with an OTDR SFP present

update_time_stamp Indicates the time when this record was last updated.

Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.1.31.115.1.2 (cableTestStatusUpdateTimeStamp)

pair_0_state Indicates line termination test results for wire pair 0 (Pins 1/2). Applies to copper only.

Values	<i>NOT_AVAILABLE</i>	No data available at this time
	<i>PAIR_OK</i>	A valid termination is detected. A cable seems to be plugged-in
	<i>PAIR_OPEN</i>	No cable termination detected. No cable seems to be plugged-in or a cable is broken
	<i>SAME_PAIR_SHORT</i>	A short circuit in this wire pair is detected
	<i>CROSS_PAIR_SHORT</i>	A short circuit with another wire pair is detected
	<i>TERMINATION_LOW</i>	A weak termination is detected.
	<i>TERMINATION_HIGH</i>	A too high termination is detected.
OID	1.3.6.1.4.1.3181.10.6.1.31.115.1.3 (cableTestStatusPair0State)	

pair_0_distance_to_fault	Distance to fault on wire pair 0 in centimeters. Indicates 0 when no fault is detected or the function is unused. Applies to copper only.	
	Value	Number in range 0-65535
	OID	1.3.6.1.4.1.3181.10.6.1.31.115.1.4 (cableTestStatusPair0DistanceToFault)
pair_1_state	Indicates line termination test results for wire pair 1 (Pins 3/6). Applies to copper only.	
	Values	<div> <div><i>NOT_AVAILABLE</i></div> <div>No data available at this time</div> </div> <div> <div><i>PAIR_OK</i></div> <div>A valid termination is detected. A cable seems to be plugged-in</div> </div> <div> <div><i>PAIR_OPEN</i></div> <div>No cable termination detected. No cable seems to be plugged-in or a cable is broken</div> </div> <div> <div><i>SAME_PAIR_SHORT</i></div> <div>A short circuit in this wire pair is detected</div> </div> <div> <div><i>CROSS_PAIR_SHORT</i></div> <div>A short circuit with another wire pair is detected</div> </div> <div> <div><i>TERMINATION_LOW</i></div> <div>A weak termination is detected.</div> </div> <div> <div><i>TERMINATION_HIGH</i></div> <div>A too high termination is detected.</div> </div>
	OID	1.3.6.1.4.1.3181.10.6.1.31.115.1.5 (cableTestStatusPair1State)
pair_1_distance_to_fault	Distance to fault on wire pair 1 in centimeters. Indicates 0 when no fault is detected or the function is unused. Applies to copper only.	
	Value	Number in range 0-65535
	OID	1.3.6.1.4.1.3181.10.6.1.31.115.1.6 (cableTestStatusPair1DistanceToFault)
pair_2_state	Indicates line termination test results for wire pair 2 (Pins 4/5). Applies to copper only.	
	Values	<div> <div><i>NOT_AVAILABLE</i></div> <div>No data available at this time</div> </div> <div> <div><i>PAIR_OK</i></div> <div>A valid termination is detected. A cable seems to be plugged-in</div> </div> <div> <div><i>PAIR_OPEN</i></div> <div>No cable termination detected. No cable seems to be plugged-in or a cable is broken</div> </div> <div> <div><i>SAME_PAIR_SHORT</i></div> <div>A short circuit in this wire pair is detected</div> </div> <div> <div><i>CROSS_PAIR_SHORT</i></div> <div>A short circuit with another wire pair is detected</div> </div> <div> <div><i>TERMINATION_LOW</i></div> <div>A weak termination is detected.</div> </div> <div> <div><i>TERMINATION_HIGH</i></div> <div>A too high termination is detected.</div> </div>
	OID	1.3.6.1.4.1.3181.10.6.1.31.115.1.7 (cableTestStatusPair2State)
pair_2_distance_to_fault	Distance to fault on wire pair 2 in centimeters. Indicates 0 when no fault is detected or the function is unused. Applies to copper only.	
	Value	Number in range 0-65535
	OID	1.3.6.1.4.1.3181.10.6.1.31.115.1.8 (cableTestStatusPair2DistanceToFault)

pair_3_state	Indicates line termination test results for wire pair 3 (Pins 7/8). Applies to copper only.	
Values	<i>NOT_AVAILABLE</i>	No data available at this time
	<i>PAIR_OK</i>	A valid termination is detected. A cable seems to be plugged-in
	<i>PAIR_OPEN</i>	No cable termination detected. No cable seems to be plugged-in or a cable is broken
	<i>SAME_PAIR_SHORT</i>	A short circuit in this wire pair is detected
	<i>CROSS_PAIR_SHORT</i>	A short circuit with another wire pair is detected
	<i>TERMINATION_LOW</i>	A weak termination is detected.
	<i>TERMINATION_HIGH</i>	A too high termination is detected.
OID	1.3.6.1.4.1.3181.10.6.1.31.115.1.9 (cableTestStatusPair3State)	

pair_3_distance_to_fault	Distance to fault on wire pair 3 in centimeters. Indicates 0 when no fault is detected or the function is unused. Applies to copper only.	
Value	Number in range 0-65535	
OID	1.3.6.1.4.1.3181.10.6.1.31.115.1.10 (cableTestStatusPair3DistanceToFault)	

reflection_value	A unitless value that indicates a measure of reflection level. For difficult to detect actively terminated devices perform a measurement with remotely plugged-in and then unplugged cable. Note the reflection values and choose a value in the middle as reflection_threshold configuration value. Applies to copper only.	
Value	Number in range 0-65535	
OID	1.3.6.1.4.1.3181.10.6.1.31.115.1.11 (cableTestStatusReflectionValue)	

cable_status	Indicates the concluded status summary. Applies to copper only.		
	Values		
	<i>NOT_AVAILABLE</i>		No data available at this time
	<i>NO_CABLE</i>		No valid termination is detected. There seems to be no cable plugged-in
	<i>PLUGGED_IN_LOCALLY</i>		A cable seems to be locally plugged-in. Probably the remote cable end is unplugged. When the remote device is using an active termination hardware then the detection may be incorrect.
	<i>PLUGGED_IN_REMOTELY</i>		A cable is locally plugged-in. It also seems to be plugged-in remotely. The measured reflection_value is less than configured reflection_limit. This condition may occur with active terminated devices.
	<i>TERMINATED_CABLE</i>		A cable is be plugged-in and least one cable pair is terminated. This indicates that the cable is plugged in at the far end as well.
	<i>TERMINATION_TOO_LOW</i>		Termination appears too low
	<i>DEFECTIVE</i>		At least one cable pair is in an error condition
	OID	1.3.6.1.4.1.3181.10.6.1.31.115.1.12 (cableTestStatusCableStatus)	

current_otdr_reflections	Number and location of currently detected reflections for an active OTDR SFP on this port.		
	Value	String, max. 256 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.31.115.1.13 (cableTestStatusCurrentOtdrReflections)	

Group	device_leds
Path	Device.Hardware.device_leds
Description	This section indicates the state of all LEDs which are not port related. Please note: Not every unit offers all LEDs.

system_1_color	This status corresponds to 'sys' LED on some devices.	
Values	<i>OFF</i>	LED is off
	<i>BLUE</i>	LED indicates blue
	<i>GREEN</i>	LED indicates green
	<i>RED</i>	LED indicates red
	<i>ORANGE</i>	LED indicates orange (yellow)
	<i>CYAN</i>	LED indicates cyan
	<i>MAGENTA</i>	LED indicates magenta
	<i>WHITE</i>	LED indicates white
	<i>NO_LED</i>	This LED does physically not exist in this device
OID	1.3.6.1.4.1.3181.10.6.1.31.114.1.2 (deviceLedsSystem1Color)	
system_1_blinking	This status corresponds to 'sys' LED on some devices.	
Values	true, false	
OID	1.3.6.1.4.1.3181.10.6.1.31.114.1.3 (deviceLedsSystem1Blinking)	
system_2_color	Displays external management activity.	
Values	<i>OFF</i>	LED is off
	<i>BLUE</i>	LED indicates blue
	<i>GREEN</i>	LED indicates green
	<i>RED</i>	LED indicates red
	<i>ORANGE</i>	LED indicates orange (yellow)
	<i>CYAN</i>	LED indicates cyan
	<i>MAGENTA</i>	LED indicates magenta
	<i>WHITE</i>	LED indicates white
	<i>NO_LED</i>	This LED does physically not exist in this device
OID	1.3.6.1.4.1.3181.10.6.1.31.114.1.4 (deviceLedsSystem2Color)	
system_2_blinking	Displays external management activity.	
Values	true, false	
OID	1.3.6.1.4.1.3181.10.6.1.31.114.1.5 (deviceLedsSystem2Blinking)	

power_on_1_color	This status corresponds to 'on' LED on some devices.		
Values	<i>OFF</i>	LED is off	
	<i>BLUE</i>	LED indicates blue	
	<i>GREEN</i>	LED indicates green	
	<i>RED</i>	LED indicates red	
	<i>ORANGE</i>	LED indicates orange (yellow)	
	<i>CYAN</i>	LED indicates cyan	
	<i>MAGENTA</i>	LED indicates magenta	
	<i>WHITE</i>	LED indicates white	
	<i>NO_LED</i>	This LED does physically not exist in this device	
OID	1.3.6.1.4.1.3181.10.6.1.31.114.1.6 (deviceLedsPowerOn1Color)		
power_on_1_blinking	This status corresponds to 'on' LED on some devices.		
Values	true, false		
OID	1.3.6.1.4.1.3181.10.6.1.31.114.1.7 (deviceLedsPowerOn1Blinking)		
power_on_2_color	Alternative power input LED.		
Values	<i>OFF</i>	LED is off	
	<i>BLUE</i>	LED indicates blue	
	<i>GREEN</i>	LED indicates green	
	<i>RED</i>	LED indicates red	
	<i>ORANGE</i>	LED indicates orange (yellow)	
	<i>CYAN</i>	LED indicates cyan	
	<i>MAGENTA</i>	LED indicates magenta	
	<i>WHITE</i>	LED indicates white	
	<i>NO_LED</i>	This LED does physically not exist in this device	
OID	1.3.6.1.4.1.3181.10.6.1.31.114.1.8 (deviceLedsPowerOn2Color)		
power_on_2_blinking	Alternative power input LED.		
Values	true, false		
OID	1.3.6.1.4.1.3181.10.6.1.31.114.1.9 (deviceLedsPowerOn2Blinking)		

ring_1_color	This LED is used when ring protection is enabled.	
Values	<i>OFF</i>	LED is off
	<i>BLUE</i>	LED indicates blue
	<i>GREEN</i>	LED indicates green
	<i>RED</i>	LED indicates red
	<i>ORANGE</i>	LED indicates orange (yellow)
	<i>CYAN</i>	LED indicates cyan
	<i>MAGENTA</i>	LED indicates magenta
	<i>WHITE</i>	LED indicates white
	<i>NO_LED</i>	This LED does physically not exist in this device
OID	1.3.6.1.4.1.3181.10.6.1.31.114.1.10 (deviceLedsRing1Color)	
ring_1_blinking	This LED is used when ring protection is enabled.	
Values	true, false	
OID	1.3.6.1.4.1.3181.10.6.1.31.114.1.11 (deviceLedsRing1Blinking)	
ring_2_color	This LED is used when ring protection is enabled.	
Values	<i>OFF</i>	LED is off
	<i>BLUE</i>	LED indicates blue
	<i>GREEN</i>	LED indicates green
	<i>RED</i>	LED indicates red
	<i>ORANGE</i>	LED indicates orange (yellow)
	<i>CYAN</i>	LED indicates cyan
	<i>MAGENTA</i>	LED indicates magenta
	<i>WHITE</i>	LED indicates white
	<i>NO_LED</i>	This LED does physically not exist in this device
OID	1.3.6.1.4.1.3181.10.6.1.31.114.1.12 (deviceLedsRing2Color)	
ring_2_blinking	This LED is used when ring protection is enabled.	
Values	true, false	
OID	1.3.6.1.4.1.3181.10.6.1.31.114.1.13 (deviceLedsRing2Blinking)	
signal_in_1_color	Indicates status of alarm input 1.	
Values	<i>OFF</i>	LED is off
	<i>BLUE</i>	LED indicates blue
	<i>GREEN</i>	LED indicates green
	<i>RED</i>	LED indicates red
	<i>ORANGE</i>	LED indicates orange (yellow)
	<i>CYAN</i>	LED indicates cyan
	<i>MAGENTA</i>	LED indicates magenta
	<i>WHITE</i>	LED indicates white
	<i>NO_LED</i>	This LED does physically not exist in this device
OID	1.3.6.1.4.1.3181.10.6.1.31.114.1.14 (deviceLedsSignalIn1Color)	

signal_in_1_blinking	Indicates status of alarm input 1.		
	Values	true, false	
	OID	1.3.6.1.4.1.3181.10.6.1.31.114.1.15 (deviceLedsSignalIn1Blinking)	
<hr/>			
signal_in_2_color	Indicates status of alarm input 2.		
	Values	<i>OFF</i> LED is off <i>BLUE</i> LED indicates blue <i>GREEN</i> LED indicates green <i>RED</i> LED indicates red <i>ORANGE</i> LED indicates orange (yellow) <i>CYAN</i> LED indicates cyan <i>MAGENTA</i> LED indicates magenta <i>WHITE</i> LED indicates white <i>NO_LED</i> This LED does physically not exist in this device	
	OID	1.3.6.1.4.1.3181.10.6.1.31.114.1.16 (deviceLedsSignalIn2Color)	
<hr/>			
signal_in_2_blinking	Indicates status of alarm input 2.		
	Values	true, false	
	OID	1.3.6.1.4.1.3181.10.6.1.31.114.1.17 (deviceLedsSignalIn2Blinking)	
<hr/>			
signal_out_1_color	Indicates status of alarm relay output 1.		
	Values	<i>OFF</i> LED is off <i>BLUE</i> LED indicates blue <i>GREEN</i> LED indicates green <i>RED</i> LED indicates red <i>ORANGE</i> LED indicates orange (yellow) <i>CYAN</i> LED indicates cyan <i>MAGENTA</i> LED indicates magenta <i>WHITE</i> LED indicates white <i>NO_LED</i> This LED does physically not exist in this device	
	OID	1.3.6.1.4.1.3181.10.6.1.31.114.1.18 (deviceLedsSignalOut1Color)	
<hr/>			
signal_out_1_blinking	Indicates status of alarm relay output 1.		
	Values	true, false	
	OID	1.3.6.1.4.1.3181.10.6.1.31.114.1.19 (deviceLedsSignalOut1Blinking)	

signal_out_2_color	Indicates status of alarm relay output 2.		
Values	OFF	LED is off	
	BLUE	LED indicates blue	
	GREEN	LED indicates green	
	RED	LED indicates red	
	ORANGE	LED indicates orange (yellow)	
	CYAN	LED indicates cyan	
	MAGENTA	LED indicates magenta	
	WHITE	LED indicates white	
	NO_LED	This LED does physically not exist in this device	
OID	1.3.6.1.4.1.3181.10.6.1.31.114.1.20 (deviceLedsSignalOut2Color)		

signal_out_2_blinking	Indicates status of alarm relay output 2.		
Values	true, false		
OID	1.3.6.1.4.1.3181.10.6.1.31.114.1.21 (deviceLedsSignalOut2Blinking)		

Group	io_signal_status
Path	Device.Hardware.io_signal_status
Description	This section is only used for devices which offer external signal inputs and outputs.

input_1_alarm_active	Indicates true when the input 1 is logically active.		
Values	true, false		
OID	1.3.6.1.4.1.3181.10.6.1.31.116.1.2 (ioSignalStatusInput1AlarmActive)		

input_2_alarm_active	Indicates true when the input 2 is logically active.		
Values	true, false		
OID	1.3.6.1.4.1.3181.10.6.1.31.116.1.3 (ioSignalStatusInput2AlarmActive)		

output_1_relay_active	Indicates true when the output 1 relay is activated.		
Values	true, false		
OID	1.3.6.1.4.1.3181.10.6.1.31.116.1.4 (ioSignalStatusOutput1RelayActive)		

output_2_relay_active	Indicates true when the output 2 relay is activated.		
Values	true, false		
OID	1.3.6.1.4.1.3181.10.6.1.31.116.1.5 (ioSignalStatusOutput2RelayActive)		

16 IP Stack

16.1 Key Features

Dual Stack

Parallel handling of IPv4 and IPv6 protocol.
Future-proof.

IPv4 Stack

Internet Protocol v4 handling with support of IPv4, ARP, DHCP, ICMP.

DHCP Options 66/67

Unit configuration or software updates controlled via DHCP option 66/67 mechanism. A CLI script can be downloaded which in turn may request further download or configuration changes

In large networks updates can be automated to take place as soon as a unit goes online. The script is a very powerful tool.

Ping, Trace Route

Standard IP test functions like Ping to check reachability and trace route to visualize packet routing is available. Since 10.6.1d these are also configurable including packet size and number of pings.

Essential tools in diagnosing basic IP connectivity.

IPv6 Management Access

Internet Protocol v6 handling with support of IPv6, DHCPv6, ICMPv6, NDP. IPv6 access to WEB, CLI, SNMP and NMP.

Permits management of unit via IPv6 access mechanisms.

IPv6 Transport

IPv6 traffic can be transported via the switch. Filter options for enhanced security available.

Switch may be used latest type of Ethernet networks.

Dynamic ARP Inspection

Incoming ARPs are being verified against IP/MAC relation database provided by DHCP snooping. In addition an access list (ACL) is used for verification. In addition too many ARPs can lead to the port being blocked to prevent ARP attacks.

Dynamic ARP Inspection helps make sure of user integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.

Secondary IPv4 Address

A secondary IP address may be assigned under which the management is alternatively available.
The default address for outgoing packets is user selectable.

16.2 Functional Description

The firmware implements dual stack functionality, supporting IPv4 and IPv6 simultaneously. The device internal management agent can be assigned with an IPv4 and IPv6 address and communicate via both protocols.

16.2.1 IPv4 Stack

For IPv4 access, static IP address, subnet mask and gateway can be configured. Alternatively these settings can be retrieved via DHCP.

16.3 IP CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Device.						
	ip.					Basic device global IP configuration for management access.
			ping_test		X	Supply an IP address to ping for reachability testing.
			trace_route		X	Supply an IP address to trace route testing.
			dns_lookup		X	Supply a hostname or web address to query for its IP address.
			arp_table		X	Displays the content of the ARP table used for management access.
			hostname		R/W	Defines the local hostname.
			domain_name		R/W	Defines an optional domain name used during name resolution.
			local_mtu		R/W	Defines MTU value for locally generated data.
			ip_version_priority		R/W	The priority applies when a name server is queried or in general when a hostname is used and both IPv4 and IPv6 could be used.
	v4_config.					This section configures IP version 4 fixed IP settings or enables use of DHCP alternatively.
			dhcp_mode		R/W	Enable DHCP to automatically retrieve an IP address and subnet mask. Also DHCP may be used to supply a CLI script file reference to be used on assignment.
			static_device_ip		R/W	Static device IP address. When DHCP is enabled, DHCP has preference over this setting.
			static_subnet_mask		R/W	Static subnet mask. When DHCP is enabled, DHCP has preference over this setting.
			static_gateway		R/W	Static default gateway IP address. When DHCP is enabled, DHCP has preference over this setting.
			static_dns_server		R/W	Static domain name server IP address. When DHCP is enabled, DHCP has preference over this setting.
			secondary_device_ip		R/W	Alternative IP address for management access. Not required in most installations.

secondary_subnet_mask	R/W	This subnet mask applies to secondary ip address.
default_address_selection	R/W	This parameter defines which own ip address is used for outgoing packets generated by the device. This only applies when a secondary_device_ip is configured.
v6_config.		This section configures IP version 6 fixed IP settings or enables use of automatic configuration alternatively.
enable_ipv6	R/W	General enable of IPv6 management access functionality.
enable_icmp_auto_address	R/W	Decides if an ICMP assigned IPv6 address is accepted.
enable_dhcp_auto_address	R/W	Decides if an DHCP assigned IPv6 address is accepted.
static_dns_server	R/W	Static domain name server reached via IPv6 address.
static_gateway	R/W	Static default gateway IP address.
v6_address[DYNAMIC].		Defines as many static IPv6 address entries as desired.
ip	R/W	Static IPv6 address in CIDR notation with definition of the subnet size. Example: 2001:db8:1111::123/64
v4_status.		This section shows a summary of IPv4 settings as they are currently active. These may reflect the statically configured values or may be dynamically assigned using DHCP.
dynamic_device_ip	R	Currently used device IP address.
dynamic_subnet_mask	R	Currently used subnet mask.
dynamic_gateway	R	Currently used gateway IP address.
dynamic_dns_server_1	R	Currently used domain name server IP address.
dynamic_dns_server_2	R	Alternate currently used domain name server IP address.
dynamic_dns_server_3	R	Alternate currently used domain name server IP address.
dynamic_dns_server_4	R	Alternate currently used domain name server IP address.
outgoing_device_ip	R	Reflects the value v4_config.default_address_selection setting.
v6_base_status.		This section shows a summary of IPv6 settings as they are currently active. These may reflect the statically configured values or may be dynamically assigned using DHCP or auto_address.
dynamic_gateway	R	Currently used gateway IP address.
dynamic_dns_server_1	R	Currently used domain name server IP address.
dynamic_dns_server_2	R	Alternate currently used domain name server IP address.

dynamic_dns_server_3	R	Alternate currently used domain name server IP address.
dynamic_dns_server_4	R	Alternate currently used domain name server IP address.
v6_status[8].		This section shows a summary of IPv6 settings as they are currently active. These may reflect the statically configured values or may be dynamically assigned using DHCP or ICMP.
ip	R	IPv6 address.
scope	R	Indicates the scope this IP is valid.
state	R	Indicates the state of this IP.

16.4 IP Configuration Parameters

Group Path	General Parameters Device.IP
ping_test	<p>Supply an IP address to ping for reachability testing.</p> <p>Action Execute command with parameter string max. 64 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.22.1 (ipPingTest)</p>
trace_route	<p>Supply an IP address to trace route testing.</p> <p>Action Execute command with parameter string max. 64 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.22.2 (ipTraceRoute)</p>
dns_lookup	<p>Supply a hostname or web address to query for its IP address.</p> <p>Action Execute command with parameter string max. 64 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.22.3 (ipDnsLookup)</p>
arp_table	<p>Displays the content of the ARP table used for management access.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.22.4 (ipArpTable)</p>
hostname	<p>Defines the local hostname.</p> <p>Value String, max. 64 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.22.5 (ipHostname)</p>
domain_name	<p>Defines an optional domain name used during name resolution.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.22.6 (ipDomainName)</p>
local_mtu	<p>Defines MTU value for locally generated data.</p> <p>Value Number in range 128-9000</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.22.7 (ipLocalMtu)</p>
ip_version_priority	<p>The priority applies when a name server is queried or in general when a hostname is used and both IPv4 and IPv6 could be used.</p> <p>Values <i>IP_V4_PRIORITY</i> Prefer IPv4 protocol <i>IP_V6_PRIORITY</i> Prefer IPv6 protocol</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.22.8 (ipIpVersionPriority)</p>

Group	v6_address , dynamical size						
Path	Device.IP.v6_address						
Description	Defines as many static IPv6 address entries as desired.						
ip	Static IPv6 address in CIDR notation with definition of the subnet size. Example: 2001:db8:1111::123/64						
Value	String, max. 50 characters.						
OID	1.3.6.1.4.1.3181.10.6.1.22.11.1.2 (v6AddressIp)						
<hr/>							
Group	v4_config						
Path	Device.IP.v4_config						
Description	This section configures IP version 4 fixed IP settings or enables use of DHCP alternatively.						
dhcp_mode	Enable DHCP to automatically retrieve an IP address and subnet mask. Also DHCP may be used to supply a CLI script file reference to be used on assignment.						
Values	<table> <tr> <td><i>DISABLED</i></td><td>Do not use DHCP. Use static values instead</td></tr> <tr> <td><i>USE_DHCP</i></td><td>Use dynamic DHCP settings assigned for device</td></tr> <tr> <td><i>DHCP_WITH_SCRIPT</i></td><td>Use dynamic DHCP settings assigned for device and load script file from server and execute it. (Option 66/67)</td></tr> </table>	<i>DISABLED</i>	Do not use DHCP. Use static values instead	<i>USE_DHCP</i>	Use dynamic DHCP settings assigned for device	<i>DHCP_WITH_SCRIPT</i>	Use dynamic DHCP settings assigned for device and load script file from server and execute it. (Option 66/67)
<i>DISABLED</i>	Do not use DHCP. Use static values instead						
<i>USE_DHCP</i>	Use dynamic DHCP settings assigned for device						
<i>DHCP_WITH_SCRIPT</i>	Use dynamic DHCP settings assigned for device and load script file from server and execute it. (Option 66/67)						
OID	1.3.6.1.4.1.3181.10.6.1.22.9.1.2 (v4ConfigDhcpMode)						
<hr/>							
static_device_ip	Static device IP address. When DHCP is enabled, DHCP has preference over this setting.						
Format	IPv4 Address <i>ddd.ddd.ddd.ddd</i> (<i>ddd</i> = decimal number between 000 to 255)						
OID	1.3.6.1.4.1.3181.10.6.1.22.9.1.3 (v4ConfigStaticDeviceIp)						
<hr/>							
static_subnet_mask	Static subnet mask. When DHCP is enabled, DHCP has preference over this setting.						
Format	IPv4 Address <i>ddd.ddd.ddd.ddd</i> (<i>ddd</i> = decimal number between 000 to 255)						
OID	1.3.6.1.4.1.3181.10.6.1.22.9.1.4 (v4ConfigStaticSubnetMask)						
<hr/>							

static_gateway	<p>Static default gateway IP address. When DHCP is enabled, DHCP has preference over this setting.</p> <p>Format IPv4 Address <i>ddd.ddd.ddd.ddd</i> (ddd = decimal number between 000 to 255)</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.22.9.1.5 (v4ConfigStaticGateway)</p>
static_dns_server	<p>Static domain name server IP address. When DHCP is enabled, DHCP has preference over this setting.</p> <p>Format IPv4 Address <i>ddd.ddd.ddd.ddd</i> (ddd = decimal number between 000 to 255)</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.22.9.1.6 (v4ConfigStaticDnsServer)</p>
secondary_device_ip	<p>Alternative IP address for management access. Not required in most installations.</p> <p>Format IPv4 Address <i>ddd.ddd.ddd.ddd</i> (ddd = decimal number between 000 to 255)</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.22.9.1.7 (v4ConfigSecondaryDeviceIp)</p>
secondary_subnet_mask	<p>This subnet mask applies to secondary ip address.</p> <p>Format IPv4 Address <i>ddd.ddd.ddd.ddd</i> (ddd = decimal number between 000 to 255)</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.22.9.1.8 (v4ConfigSecondarySubnetMask)</p>
default_address_selection	<p>This parameter defines which own ip address is used for outgoing packets generated by the device. This only applies when a secondary_device_ip is configured.</p> <p>Values <i>PRIMARY</i> Normal setting. Uses the v4_status.current dynamic_device_ip. This is either the static_device_ip or the ip assigned via DHCP. <i>SECONDARY</i> Use the secondary_device_ip</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.22.9.1.9 (v4ConfigDefaultAddressSelection)</p>

Group	v6_config
Path	Device.IP.v6_config
Description	This section configures IP version 6 fixed IP settings or enables use of automatic configuration alternatively.

enable_ipv6	General enable of IPv6 management access functionality. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.1.22.10.1.2 (v6ConfigEnableIpv6)
enable_icmp_auto_address	Decides if an ICMP assigned IPv6 address is accepted. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.1.22.10.1.3 (v6ConfigEnableIcmpAutoAddress)
enable_dhcp_auto_address	Decides if an DHCP assigned IPv6 address is accepted. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.1.22.10.1.4 (v6ConfigEnableDhcpAutoAddress)
static_dns_server	Static domain name server reached via IPv6 address. Format IPv6 Address <i>hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh</i> (<i>hhhh</i> = hexadecimal number between 0000 to ffff) OID 1.3.6.1.4.1.3181.10.6.1.22.10.1.5 (v6ConfigStaticDnsServer)
static_gateway	Static default gateway IP address. Format IPv6 Address <i>hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh</i> (<i>hhhh</i> = hexadecimal number between 0000 to ffff) OID 1.3.6.1.4.1.3181.10.6.1.22.10.1.6 (v6ConfigStaticGateway)

16.5 IP Status Parameters

Group	v6_status , for all IPv6 addresses [0..7]		
Path	Device.IP.v6_status[IPv6_addresses]		
Description	This section shows a summary of IPv6 settings as they are currently active. These may reflect the statically configured values or may be dynamically assigned using DHCP or ICMP.		
<hr/>			
ip	IPv6 address.		
	Format	IPv6 Address hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh (hhhh = hexadecimal number between 0000 to ffff)	
	OID	1.3.6.1.4.1.3181.10.6.1.22.102.1.2 (v6StatusIp)	
<hr/>			
scope	Indicates the scope this IP is valid.		
	Values	<i>LINK</i> Link_local address, identified by the FE80:: , is used by nodes when communicating with neighboring nodes on the same link. A link local address is automatically configured. <i>SITE</i> Scope Site <i>GLOBAL</i> Scope Global <i>OTHER</i> Other Scope	
	OID	1.3.6.1.4.1.3181.10.6.1.22.102.1.3 (v6StatusScope)	
<hr/>			
state	Indicates the state of this IP.		
	Values	<i>STATELESS</i> Stateless <i>STATEFUL</i> Stateful <i>BOTH</i> Stateless and Stateful <i>OTHER</i> Other	
	OID	1.3.6.1.4.1.3181.10.6.1.22.102.1.4 (v6StatusState)	
<hr/>			
Group	v4_status		
Path	Device.IP.v4_status		
Description	This section shows a summary of IPv4 settings as they are currently active. These may reflect the statically configured values or may be dynamically assigned using DHCP.		

dynamic_device_ip	Currently used device IP address.
Format	IPv4 Address <i>ddd.ddd.ddd.ddd</i> (ddd = decimal number between 000 to 255)
OID	1.3.6.1.4.1.3181.10.6.1.22.100.1.2 (v4StatusDynamicDeviceIp)
dynamic_subnet_mask	Currently used subnet mask.
Format	IPv4 Address <i>ddd.ddd.ddd.ddd</i> (ddd = decimal number between 000 to 255)
OID	1.3.6.1.4.1.3181.10.6.1.22.100.1.3 (v4StatusDynamicSubnetMask)
dynamic_gateway	Currently used gateway IP address.
Format	IPv4 Address <i>ddd.ddd.ddd.ddd</i> (ddd = decimal number between 000 to 255)
OID	1.3.6.1.4.1.3181.10.6.1.22.100.1.4 (v4StatusDynamicGateway)
dynamic_dns_server_1	Currently used domain name server IP address.
Format	IPv4 Address <i>ddd.ddd.ddd.ddd</i> (ddd = decimal number between 000 to 255)
OID	1.3.6.1.4.1.3181.10.6.1.22.100.1.5 (v4StatusDynamicDnsServer1)
dynamic_dns_server_2	Alternate currently used domain name server IP address.
Format	IPv4 Address <i>ddd.ddd.ddd.ddd</i> (ddd = decimal number between 000 to 255)
OID	1.3.6.1.4.1.3181.10.6.1.22.100.1.6 (v4StatusDynamicDnsServer2)
dynamic_dns_server_3	Alternate currently used domain name server IP address.
Format	IPv4 Address <i>ddd.ddd.ddd.ddd</i> (ddd = decimal number between 000 to 255)
OID	1.3.6.1.4.1.3181.10.6.1.22.100.1.7 (v4StatusDynamicDnsServer3)
dynamic_dns_server_4	Alternate currently used domain name server IP address.
Format	IPv4 Address <i>ddd.ddd.ddd.ddd</i> (ddd = decimal number between 000 to 255)
OID	1.3.6.1.4.1.3181.10.6.1.22.100.1.8 (v4StatusDynamicDnsServer4)

outgoing_device_ip	Reflects the value v4_config.default_address_selection setting.
Format	IPv4 Address <i>ddd.ddd.ddd.ddd</i> (<i>ddd</i> = decimal number between 000 to 255)
OID	1.3.6.1.4.1.3181.10.6.1.22.100.1.9 (v4StatusOutgoingDeviceIp)
Group Path Description	v6_base_status Device.IP.v6_base_status This section shows a summary of IPv6 settings as they are currently active. These may reflect the statically configured values or may be dynamically assigned using DHCP or auto_address.
dynamic_gateway	Currently used gateway IP address.
Format	IPv6 Address <i>hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh</i> (<i>hhhh</i> = hexadecimal number between 0000 to ffff)
OID	1.3.6.1.4.1.3181.10.6.1.22.101.1.2 (v6BaseStatusDynamicGateway)
dynamic_dns_server_1	Currently used domain name server IP address.
Format	IPv6 Address <i>hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh</i> (<i>hhhh</i> = hexadecimal number between 0000 to ffff)
OID	1.3.6.1.4.1.3181.10.6.1.22.101.1.3 (v6BaseStatusDynamicDnsServer1)
dynamic_dns_server_2	Alternate currently used domain name server IP address.
Format	IPv6 Address <i>hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh</i> (<i>hhhh</i> = hexadecimal number between 0000 to ffff)
OID	1.3.6.1.4.1.3181.10.6.1.22.101.1.4 (v6BaseStatusDynamicDnsServer2)
dynamic_dns_server_3	Alternate currently used domain name server IP address.
Format	IPv6 Address <i>hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh</i> (<i>hhhh</i> = hexadecimal number between 0000 to ffff)
OID	1.3.6.1.4.1.3181.10.6.1.22.101.1.5 (v6BaseStatusDynamicDnsServer3)

dynamic_dns_server_4	Alternate currently used domain name server IP address.
Format	IPv6 Address <i>hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh</i> (<i>hhhh</i> = hexadecimal number between 0000 to ffff)
OID	1.3.6.1.4.1.3181.10.6.1.22.101.1.6 (v6BaseStatusDynamicDnsServer4)

17 Port-specific Functions

17.1 Key Features

Administration

Port control. For each port a 64 character long alias name can be assigned .

Use names to match corporate data base naming conventions. Names appear for example in SNMP traps and Syslogs.

Ethernet Twisted-Pair

Auto-Negotiation of speed 10/100/1000, duplex mode, flow-control, Auto MDI/MDI-X

Cable Tester

Integrated cable checker help discover broken cables. Technology is based on time domain reflection measurements of the cable. For each wire pair the termination status is determined. The cable length is calculated and cable shortcuts can be detected.

Supports installation without need for additional tool.

Ethernet Fixed Fiber

100/1000, duplex mode, flow-control

Ethernet SFP

Support for pluggable optical port (SFP) permits use with various wave length, fiber types and link distances. Double SFP version MicroSwitch. Up to 8 SFP in Industry Switch.

Link cable may be local or tens of kilometers away. Plug in according to needs.

Dual Media Ports

Some ports can operate with copper or optical cable. Preferences and priorities can be selected.

Additional flexibility

Loop Protection

Local loop protection detects parallel links to the same switch or loops between local ports to avoid endless packet storms.

Safeguards against miscabling. Temporarily shuts down offending port to prevent Ethernet loop condition.

SFP Auto Speed

Automatically reconfigures port data rate to match the highest rate available with the plugged-in SFP. This feature requires original MICROSENS SFPs.

Eases deployment in mixed data rate networks by eliminating manual intervention to set port speed. Note that for optical interfaces auto negotiation does not apply.

17.2 Functional Description

17.2.1 Connection Parameters

Port specific functions vary depending on the port type, mainly determined by the type of media used.

17.2.2 Ethernet Copper Ports

Ethernet copper ports normally support multiple speed, duplex and flow-control options for maximum (backwards) compatibility.

Auto-Negotiation

When two ports are connected by a Twisted-Pair cable, both ports exchange their capabilities and select that common mode of operation that provides highest performance to establish the connection. The port mode is selected according to the following order (descending performance):

1. Gigabit Ethernet: 1000Base-T, full duplex
2. Fast Ethernet: 100Base-TX, full duplex
3. Fast Ethernet: 100Base-TX, half duplex
4. Standard Ethernet: 10Base-T, full duplex
5. Standard Ethernet: 10Base-T, half duplex

The Auto-Negotiation mechanism is the default mode of operation. When both ports do not share a common mode, no link is established. The result of the Auto-Negotiation process is shown in the port status registers.

Manual Settings

When Auto-Negotiation is enabled, the settings for speed, duplex and flow-control determine, if the corresponding ability is advertised via Auto-Negotiation to the link partner.

When Auto-Negotiation is disabled, the connection parameters can be adjusted manually.

1000Base-T always requires Auto-Negotiation enabled.

ATTENTION: When Auto-Negotiation is disabled, the administrator must take care that both ports connected on the same segment have identical connection parameters. A mismatch e.g. in duplex settings will cause unreliable behaviour of the connection.

If the remote device does not have Auto-Negotiation capability, the device uses parallel detect function to determine the speed of the remote device for 100Base-TX and 10Base-T mode. If a link is established based on the parallel detect function, then it is required to establish the link at half-duplex mode only.

ATTENTION: When Auto-Negotiation is disabled on one side of the link only, with the opposite port having Auto-Negotiation enabled, this may result in a mismatch of duplex settings causing unreliable behaviour of the connection.

Auto-MDIX

When connecting two Ethernet ports, depending on the port pinout (MDI or MDI-X) different kind of cables (straight or crossover) would be required. To overcome this restriction, Ethernet copper port implement Auto-MDIX for the automatic detection and adaption of internal wiring depending on the opposite partner.

ATTENTION: The Auto-MDIX function is only available if Auto-Negotiation is enabled on the port.

Energy Efficient Ethernet



Ethernet links in 1000Base-T mode require permanently a significant amount of power, even if no data is transmitted. To reduce power consumption, 1000Base-T segments with Energy Efficient Ethernet support (IEEE Std. 802.3az) can enter low power idle mode if no data is transmitted. This mode can reduce power consumption significantly.

INFO: Energy Efficient Ethernet must be supported by both ports of a segment. If only one port supports EEE, standard power mode is used.

17.2.3 Ethernet Fiber Ports

Ethernet fiber ports may support multiple speed, duplex and flow-control options, but Auto-Negotiation is only defined for 1000_MBit connections and not supporting speed selection. For 100_MBit links, the speed, duplex and flow-control parameters must always be configured manually.

ATTENTION: The administrator must take care that both ports connected on the same segment have identical connection parameters. A mismatch e.g. in duplex settings will cause unreliable behaviour of the connection.

17.2.4 Dual Media Ports

A dual media port supports both fiber and copper media. As both physical ports are internally connected to one switch port, only one media can be active at a time.

If both physical ports are connected simultaneously, the active media must be selected. This can be configured by a fixed setting (*force_fiber* or *force_copper*) or by specifying the priority (*fiber_priority* will choose fiber and *copper_priority* will choose copper).

ATTENTION: A fixed setting for a dual media port will apply even if only one media is connected. If copper is selected as forced mode, then no fiber connection will be established, even if the copper port is not used (and vice versa).

17.3 Port CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Device.	port.	config[PORT].	Basic port specific settings			
			This section defines the basic configuration parameter for each port.			
			alias	R/W		Alternative descriptive port name, user definable.
			port_operation	R/W		Enables the port for operation. When disabled, port is shut down.
			role	R/W		Defines is a port is a regular local user port or a link to the network. This setting is references in various sanity checks throughout the system. When in doubt leave at default setting.
			speed	R/W		When Auto-Negotiation is disabled sets the ports data rate to the selected speed. When Auto-Negotiation is enabled it determines the highest data rate advertised on port.
			mtu	R/W		MTU used only to have a place holder for SNMP ifTable
			loop_protection	R/W		Loop protection detects Ethernet loops that can occur when cables are plugged in a way that the data send out of a port come back to the switch on another port. This will result in a data loop of endless packets. Such a loop condition seriously affects network performance and must be avoided.
			auto_negotiation	R/W		Enables Auto-Negotiation mode. When Auto-Negotiation mode is enabled, the parameters speed, full_duplex and flow_control determine the advertised port abilities. When Auto-Negotiation is disabled, the parameters speed, full_duplex and flow_control determine the fixed port configuration. Auto-Negotiation is not available for fiber ports in 100 Mbps mode and must be switched off.
			full_duplex	R/W		When Auto-Negotiation is disabled sets port to full duplex operation (when disabled, port is in half duplex mode). When Auto-Negotiation is enabled, it determines the advertisement of full duplex capability.

flowcontrol	R/W	When Auto-Negotiation is disabled sets port into flow control mode. When Auto-Negotiation is enabled, it determines the advertisement of flow control capability. Flow control is only supported when port is in full duplex mode.
mdi_mode	R/W	Enables Auto MDI/MDI-X mode to automatically adapt port pinout to cable type used. When set to forced, port pinout is fixed.
energy_efficiency	R/W	Enable Energy Efficient Ethernet mode is only available for copper ports in 1000Base-T mode.
dual_media_mode	R/W	Define media selection for dual media ports. This function is only available on ports with dual media Phy.
allowed_outgoing_ports	R/W	This bitmask may be used to limit the outgoing traffic to certain ports. This feature is also known as port based vlan. Syntax: slot/port, slot/port or use hex value for quick setup = 0x3f (ports 1-6)
monitor.		Port monitoring is a test tool which permits reading data from on port on another port for trouble shooting purposes.
mode	R/W	Defines in which mode of port monitoring operation is used. Default is DISABLED for normal operation.
source	R/W	Source port(2) of which the traffic is to be monitored. CLI Syntax: 1/1 for first port. 1/1,1/3 for first and third port
destination	R/W	Port on which the traffic monitored on the source port shall be copied to. Normally a network sniffer is connected to this port. Please observe that possibly the VLAN setting of the destination port must match the that of the monitored ports. CLI Syntax: 1/1 for first port.
restart_port	X	This function may be used to briefly disabled and enable the port. This may be used to restart port authentication for example. Please supply port number as parameter. The shorthand port format like 1 for 1/1 may be used. Syntax examples: restart_port = 1/2,1/5.
uplink_ports	R	Indicates which port(s) are connected to the network. The setting is derived from default setting and may be overridden by port.role setting.
downlink_ports	R	Indicates to which port(s) a downstream switch is connected. The setting is derived from default setting and may be overridden by port.role setting.

status[PORT].		This status table indicates current port status and (negotiated) settings. It also displays if a port is logically blocked due to a certain protocol condition.
link_up	R	False: Link is down, True: Link is up. For dual media ports this indicates the status of the active media.
last_link_change	R	Time when the link_up status changed the last time. Value may appear illogical if the system time is not properly set.
link_state	R	Logical port status.
rx_activity	R	Indicates true when data activity on the receiver is detected.
tx_activity	R	Indicates true when data activity on the transmitter is detected.
media_used	R	indicates which media is used for dual media ports
speed_used	R	Actual (negotiated) port data rate.
looped_port	R	Usually empty. When a port loop is detected through loop protection function then the looped port is indicated here.
full_duplex_used	R	False: Half duplex, True: Full duplex.
flowcontrol_used	R	False: No flow control, True: Use flow control.
mdi_used	R	False: MDI pinout, True: MDI-X pinout.
eee_active	R	When true Energy Efficient Ethernet is supported by both ends of the link and is active.
blocking_algorithm	R	Flags indicate blocking request by which algorithm per port.
learning_algorithm	R	Flags indicate learning request by which algorithm per port.
forwarding_algorithm	R	Flags indicate forwarding request by which algorithm per port.
unauthorized_algorithm	R	Flags indicate use of unauthorized vlan request by which algorithm per port.

17.4 Port Configuration Parameters

Group Path	General Parameters								
	Device.Port								
restart_port	<p>This function may be used to briefly disabled and enable the port. This may be used to restart port authentication for example. Please supply port number as parameter. The shorthand port format like 1 for 1/1 may be used. Syntax examples: restart_port = 1/2,1/5.</p> <p>Action Execute command with parameter string max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.81.3 (portRestartPort)</p>								
Group Path Description	config, for each port[0..24] Device.Port.config[port] This section defines the basic configuration parameter for each port.								
alias	<p>Alternative descriptive port name, user definable.</p> <p>Value String, max. 64 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.81.1.1.2 (configAlias) 1.0.8802.1.1.2.1.3.7.1.4 (lldpLocPortDesc) 1.3.6.1.2.1.31.1.1.1.18 (ifAlias)</p>								
port_operation	<p>Enables the port for operation. When disabled, port is shut down.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.81.1.1.3 (configPortOperation) 1.3.6.1.2.1.2.2.1.7 (ifAdminStatus)</p>								
role	<p>Defines is a port is a regular local user port or a link to the network. This setting is references in various sanity checks throughout the system. When in doubt leave at default setting.</p> <p>Values</p> <table> <tr> <td><i>DEFAULT</i></td><td>The default port role according to hardware type is used.</td></tr> <tr> <td><i>LOCAL</i></td><td>This is a regular local port</td></tr> <tr> <td><i>UPLINK</i></td><td>This port attaches to the network</td></tr> <tr> <td><i>DOWNLINK</i></td><td>This port is the downstream port to the link of a subsequent switch</td></tr> </table> <p>OID 1.3.6.1.4.1.3181.10.6.1.81.1.1.4 (configRole)</p>	<i>DEFAULT</i>	The default port role according to hardware type is used.	<i>LOCAL</i>	This is a regular local port	<i>UPLINK</i>	This port attaches to the network	<i>DOWNLINK</i>	This port is the downstream port to the link of a subsequent switch
<i>DEFAULT</i>	The default port role according to hardware type is used.								
<i>LOCAL</i>	This is a regular local port								
<i>UPLINK</i>	This port attaches to the network								
<i>DOWNLINK</i>	This port is the downstream port to the link of a subsequent switch								

speed	<p>When Auto-Negotiation is disabled sets the ports data rate to the selected speed. When Auto-Negotiation is enabled it determines the highest data rate advertised on port.</p>
Values	<p><i>10_MBIT</i> Port speed 10 Mbps (Standard Ethernet)</p> <p><i>100_MBIT</i> Port Speed 100 Mbps (Fast Ethernet)</p> <p><i>1000_MBIT</i> Port Speed 1000 Mbps (Gigabit Ethernet)</p> <p><i>SFP_AUTO</i> Use only with SFP port. Selects the fastest data rate which the inserted SFP supports</p>
OID	1.3.6.1.4.1.3181.10.6.1.81.1.1.5 (configSpeed)
mtu	<p>MTU used only to have a place holder for SNMP ifTable</p>
Values	<p><i>1522_BYTE</i> Max packet size set to 1522 byte</p> <p><i>2048_BYTE</i> Max packet size set to 2048 byte</p> <p><i>10240_BYTE</i> Max packet size set to 10240 byte (jumbo frames)</p>
OID	1.3.6.1.4.1.3181.10.6.1.81.1.1.6 (configMtu) 1.3.6.1.2.1.2.2.1.4 (ifMtu)
loop_protection	<p>Loop protection detects Ethernet loops that can occur when cables are plugged in a way that the data send out of a port come back to the switch on another port. This will result in a data loop of endless packets. Such a loop condition seriously affects network performance and must be avoided.</p>
Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.1.81.1.1.7 (configLoopProtection)
auto_negotiation	<p>Enables Auto-Negotiation mode. When Auto-Negotiation mode is enabled, the parameters speed, full_duplex and flow_control determine the advertised port abilities. When Auto-Negotiation is disabled, the parameters speed, full_duplex and flow_control determine the fixed port configuration. Auto-Negotiation is not available for fiber ports in 100 Mbps mode and must be switched off.</p>
Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.1.81.1.1.8 (configAutoNegotiation)
full_duplex	<p>When Auto-Negotiation is disabled sets port to full duplex operation (when disabled, port is in half duplex mode). When Auto-Negotiation is enabled, it determines the advertisement of full duplex capability.</p>
Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.1.81.1.1.9 (configFullDuplex)
flowcontrol	<p>When Auto-Negotiation is disabled sets port into flow control mode. When Auto-Negotiation is enabled, it determines the advertisement of flow control capability. Flow control is only supported when port is in full duplex mode.</p>
Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.1.81.1.1.10 (configFlowcontrol)

mdi_mode	Enables Auto MDI/MDI-X mode to automatically adapt port pinout to cable type used. When set to forced, port pinout is fixed.
Values	<div> <i>AUTO</i> MDI/MDI-X automatic detection </div> <div> <i>FORCE_MDI_STD</i> Port pinout set to normal MDI configuration </div> <div> <i>FORCE_MDIX</i> Port pinout set to crossover MDI-X configuration </div>
OID	1.3.6.1.4.1.3181.10.6.1.81.1.1.11 (configMdiMode)
energy_efficiency	Enable Energy Efficient Ethernet mode is only available for copper ports in 1000Base-T mode.
Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.1.81.1.1.12 (configEnergyEfficiency)
dual_media_mode	Define media selection for dual media ports. This function is only available on ports with dual media Phy.
Values	<div> <i>FIBER_PRIORITY</i> Auto detect media type. Fiber has priority over copper when both media are detected </div> <div> <i>COPPER_PRIORITY</i> Auto detect media type. Copper has priority over fiber when both media are detected </div> <div> <i>FORCE_FIBER</i> Port set to fiber media </div> <div> <i>FORCE_COPPER</i> Port set to copper media </div>
OID	1.3.6.1.4.1.3181.10.6.1.81.1.1.13 (configDualMediaMode)
allowed_outgoing_ports	This bitmask may be used to limit the outgoing traffic to certain ports. This feature is also known as port based vlan. Syntax: slot/port, slot/port or use hex value for quick setup = 0x3f (ports 1-6)
Value	PORTMASK0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.1.81.1.1.14 (configAllowedOutgoingPorts)

Group	monitor
Path	Device.Port.monitor
Description	Port monitoring is a test tool which permits reading data from on port on another port for trouble shooting purposes.

mode	Defines in which mode of port monitoring operation is used. Default is DISABLED for normal operation.		
	Values	DISABLED	Port monitoring function is disabled. This is normal operation.
		TX_ONLY	Port monitoring function is enabled and all data transmitted at source port are also transmitted out of the destination port.
		RX_ONLY	Port monitoring function is enabled and all data received at source port are also transmitted out of the destination port.
		RX_AND_TX	Port monitoring function is enabled for receive and transmit data of source port. Both types of data will be send out of the destination port.
	OID	1.3.6.1.4.1.3181.10.6.1.81.2.1.2 (monitorMode)	
<hr/>			
source	Source port(2) of which the traffic is to be monitored. CLI Syntax: 1/1 for first port. 1/1,1/3 for first and third port		
	Value	PORTMASK0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.1.81.2.1.3 (monitorSource)	
<hr/>			
destination	Port on which the traffic monitored on the source port shall be copied to. Normally a network sniffer is connected to this port. Please observe that possibly the VLAN setting of the destination port must match the that of the monitored ports. CLI Syntax: 1/1 for first port.		
	Value	PORT0-255	
	OID	1.3.6.1.4.1.3181.10.6.1.81.2.1.4 (monitorDestination)	

17.5 Port Status Parameters

Group	General Parameters
Path	Device.Port
uplink_ports	<p>Indicates which port(s) are connected to the network. The setting is derived from default setting and may be overridden by port.role setting.</p> <p>Value PORTMASK0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.81.100 (portUplinkPorts)</p>
downlink_ports	<p>Indicates to which port(s) a downstream switch is connected. The setting is derived from default setting and may be overridden by port.role setting.</p> <p>Value PORTMASK0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.81.101 (portDownlinkPorts)</p>
Group	status , for all ports[0..31]
Path	Device.Port.status[port]
Description	This status table indicates current port status and (negotiated) settings. It also displays if a port is logically blocked due to a certain protocol condition.
link_up	<p>False: Link is down, True: Link is up. For dual media ports this indicates the status of the active media.</p> <p>Values true, false</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.81.102.1.2 (statusLinkUp) 1.3.6.1.2.1.2.2.1.8 (ifOperStatus)</p>
last_link_change	<p>Time when the link_up status changed the last time. Value may appear illogical if the system time is not properly set.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.81.102.1.3 (statusLastLinkChange) 1.3.6.1.2.1.2.2.1.9 (ifLastChange)</p>

link_state	Logical port status.		
	Values	LINK_DOWN	Link is not established. No communication. Ethernet LED is off
		BLOCKING	Port is blocked. No communication. Ethernet LED indicates yellow.
		LEARNING	Port is learning MAC addresses. No communication. Ethernet LED indicates yellow.
		FORWARDING	Port is forwarding data. Ethernet LED indicates green.
		UNAUTH_VLAN	Port is forwarding data on the unauthorized_vlan only. Ethernet LED indicates green.
	OID	1.3.6.1.4.1.3181.10.6.1.81.102.1.4 (statusLinkState)	
<hr/>			
rx_activity	Indicates true when data activity on the receiver is detected.		
	Values	true, false	
	OID	1.3.6.1.4.1.3181.10.6.1.81.102.1.5 (statusRxActivity)	
<hr/>			
tx_activity	Indicates true when data activity on the transmitter is detected.		
	Values	true, false	
	OID	1.3.6.1.4.1.3181.10.6.1.81.102.1.6 (statusTxActivity)	
<hr/>			
media_used	indicates which media is used for dual media ports		
	Values	NONE	Neither cable nor fiber are active
		COPPER	A copper cable is used
		FIBER	A fiber connection is used
	OID	1.3.6.1.4.1.3181.10.6.1.81.102.1.7 (statusMediaUsed)	
<hr/>			
speed_used	Actual (negotiated) port data rate.		
	Values	DOWN	Port is down. No communication
		10_MBIT	10Mbit/s is used
		100_MBIT	100Mbit/s is used
		1000_MBIT	1Gbit/s is used
		10_GBIT	10Gbit/s is used
	OID	1.3.6.1.4.1.3181.10.6.1.81.102.1.8 (statusSpeedUsed)	
		1.3.6.1.2.1.2.2.1.5 (ifSpeed)	
<hr/>			
looped_port	Usually empty. When a port loop is detected through loop protection function then the looped port is indicated here.		
	Value	PORTMASK0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.1.81.102.1.9 (statusLoopedPort)	

full_duplex_used	False: Half duplex, True: Full duplex.																		
Values	<i>NONE</i> Port is down <i>FULL</i> Full duplex mode <i>HALF</i> Half duplex mode																		
OID	1.3.6.1.4.1.3181.10.6.1.81.102.1.10 (statusFullDuplexUsed) 1.3.6.1.2.1.10.7.2.1.19 (dot3StatsDuplexStatus)																		
flowcontrol_used	False: No flow control, True: Use flow control.																		
Values	true, false																		
OID	1.3.6.1.4.1.3181.10.6.1.81.102.1.11 (statusFlowcontrolUsed)																		
mdi_used	False: MDI pinout, True: MDI-X pinout.																		
Values	true, false																		
OID	1.3.6.1.4.1.3181.10.6.1.81.102.1.12 (statusMdiUsed)																		
eee_active	When true Energy Efficient Ethernet is supported by both ends of the link and is active.																		
Values	true, false																		
OID	1.3.6.1.4.1.3181.10.6.1.81.102.1.13 (statusEeeActive)																		
blocking_algorithm	Flags indicate blocking request by which algorithm per port.																		
Values	<table> <tr> <td><i>PORT_IS_ENABLED</i></td><td>Port is enabled and can be set to this state</td></tr> <tr> <td><i>8021X_APPLIES</i></td><td>Port authentication applies this state</td></tr> <tr> <td><i>RSTP_APPLIES</i></td><td>RSTP-algorithm applies this state</td></tr> <tr> <td><i>RING_APPLIES</i></td><td>Ring mechanism applies this state</td></tr> <tr> <td><i>COUPLING_APPLIES</i></td><td>Ring Coupling mechanism applies this state</td></tr> <tr> <td><i>LOOP_PREVENTION_APPLIES</i></td><td>Loop Prevention applies this state</td></tr> <tr> <td><i>MAC_AUTH_APPLIES</i></td><td>MAC authentication applies to this state</td></tr> <tr> <td><i>BPDU_GUARD_APPLIES</i></td><td>BPDU guard function applies this state</td></tr> <tr> <td><i>DHCP_FILTER_APPLIES</i></td><td>DHCP filter function applies this state</td></tr> </table>	<i>PORT_IS_ENABLED</i>	Port is enabled and can be set to this state	<i>8021X_APPLIES</i>	Port authentication applies this state	<i>RSTP_APPLIES</i>	RSTP-algorithm applies this state	<i>RING_APPLIES</i>	Ring mechanism applies this state	<i>COUPLING_APPLIES</i>	Ring Coupling mechanism applies this state	<i>LOOP_PREVENTION_APPLIES</i>	Loop Prevention applies this state	<i>MAC_AUTH_APPLIES</i>	MAC authentication applies to this state	<i>BPDU_GUARD_APPLIES</i>	BPDU guard function applies this state	<i>DHCP_FILTER_APPLIES</i>	DHCP filter function applies this state
<i>PORT_IS_ENABLED</i>	Port is enabled and can be set to this state																		
<i>8021X_APPLIES</i>	Port authentication applies this state																		
<i>RSTP_APPLIES</i>	RSTP-algorithm applies this state																		
<i>RING_APPLIES</i>	Ring mechanism applies this state																		
<i>COUPLING_APPLIES</i>	Ring Coupling mechanism applies this state																		
<i>LOOP_PREVENTION_APPLIES</i>	Loop Prevention applies this state																		
<i>MAC_AUTH_APPLIES</i>	MAC authentication applies to this state																		
<i>BPDU_GUARD_APPLIES</i>	BPDU guard function applies this state																		
<i>DHCP_FILTER_APPLIES</i>	DHCP filter function applies this state																		
OID	1.3.6.1.4.1.3181.10.6.1.81.102.1.14 (statusBlockingAlgorithm)																		

learning_algorithm

Flags indicate learning request by which algorithm per port.

Values*PORT_IS_ENABLED*

Port is enabled and can be set to this state

8021X_APPLIES

Port authentication applies this state

RSTP_APPLIES

RSTP-algorithm applies this state

RING_APPLIES

Ring mechanism applies this state

COUPLING_APPLIES

Ring Coupling mechanism applies this state

LOOP_PREVENTION_APPLIES

Loop Prevention applies this state

MAC_AUTH_APPLIES

MAC authentication applies to this state

BPDU_GUARD_APPLIES

BPDU guard function applies this state

DHCP_FILTER_APPLIES

DHCP filter function applies this state

OID

1.3.6.1.4.1.3181.10.6.1.81.102.1.15 (statusLearningAlgorithm)

forwarding_algorithm

Flags indicate forwarding request by which algorithm per port.

Values*PORT_IS_ENABLED*

Port is enabled and can be set to this state

8021X_APPLIES

Port authentication applies this state

RSTP_APPLIES

RSTP-algorithm applies this state

RING_APPLIES

Ring mechanism applies this state

COUPLING_APPLIES

Ring Coupling mechanism applies this state

LOOP_PREVENTION_APPLIES

Loop Prevention applies this state

MAC_AUTH_APPLIES

MAC authentication applies to this state

BPDU_GUARD_APPLIES

BPDU guard function applies this state

DHCP_FILTER_APPLIES

DHCP filter function applies this state

OID

1.3.6.1.4.1.3181.10.6.1.81.102.1.16 (statusForwardingAlgorithm)

unauthorized_algorithm	Flags indicate use of unauthorized vlan request by which algorithm per port.		
	Values		
	<i>PORT_IS_ENABLED</i>		Port is enabled and can be set to this state
	<i>8021X_APPLIES</i>		Port authentication applies this state
	<i>RSTP_APPLIES</i>		RSTP-algorithm applies this state
	<i>RING_APPLIES</i>		Ring mechanism applies this state
	<i>COUPLING_APPLIES</i>		Ring Coupling mechanism applies this state
	<i>LOOP_PREVENTION_APPLIES</i>		Loop Prevention applies this state
	<i>MAC_AUTH_APPLIES</i>		MAC authentication applies to this state
	<i>BPDU_GUARD_APPLIES</i>		BPDU guard function applies this state
	<i>DHCP_FILTER_APPLIES</i>		DHCP filter function applies this state
	OID	1.3.6.1.4.1.3181.10.6.1.81.102.1.17 (statusUnauthorizedAlgorithm)	

18 SFP Transceiver

18.1 Key Features

SFP Management

SFP are automatically detected and their inventory data is displayed. Insertion and removal generates events that may be forwarded as Syslogs or Traps.

Use of SFP permits mix and match with any fiber type and distance requirements.

Power Monitoring

The optical transmit and receive power is permanently monitored and events can be generated when the receive power level varies for more than a customer defined threshold. Automated delta detection eliminates the need to individually measure and configure each port during installation.

Provides detection of optical problems which normal loss of signal monitoring would not catch. Automated setup ensures the feature is actually used.

CSFP Support

Some switch versions supports double port Compact-SFP optical interfaces. These SFP contain two independent single fiber channels and are displayed for two ports with independent optical data.

Highest possible port density. Two optical ports in Installation Switch for redundant network links.

micro OTDR Support

Support for SFP based OTDR (optical time domain reflectometer) measurement to automatically detect changes in the fiber topology. This feature is especially suitable for the NM3 MSP1000 management module.

The OTDR function permit detection of critical changes to a fiber (attack) and help diagnose breaks in the fiber. It detects the distance of the fiber break from the device. This permits purposeful and quicker repair.

18.2 Functional Description

ATTENTION: This section is only applicable for devices with hardware support for SFP (Small Formfactor Pluggable) optical transceivers.

18.2.1 Basic Transceiver Information

SFP transceivers are intelligent modules that provide information about their abilities and status. These information include manufacturer, art.-no, serial-no., optical connector type, optical wavelength etc.

The specifications for the SFP transceivers are defined by the SFF Committee in the document SFF-8074i "SFP (Small Formfactor Pluggable) Transceiver". Please see this document for more detailed information.

18.2.2 Digital Diagnostics Interface

SFP transceivers implementing the Digital Diagnostics Interface provide additional information about the power levels of the optical ports. This information can be used to monitor the quality of the optical link by checking the received power level for a given fiber segment. If this level changes over time significantly, an alarm event can be triggered.

The specifications for the diagnostic interface are defined by the SFF Committee in the document SFF-8472 "*Diagnostic Monitoring Interface for Optical Xcvrs*". Please see this document for more detailed information.

INFO: *This feature is only available when using SFP transceivers implementing the Digital Diagnostics Interface. MICROSENS transceivers indicate this ability by the letter 'D' in the article number.*

part_number	R	Shows the part number of this SFP. This will differ from the MICROSENS order code unless also MICROSENS is indicated as manufacturer.
revision	R	Internal revision code of this SFP.
serial_number	R	Serial number of the SFP.
mfg_date_code	R	Manufacturing date code.
warnings	R	
alarms	R	
tx_power	R	Indicates the optical output in dBm. Some SFP cannot display this value. For electrical SFP N/A (not applicable) is shown.
rx_power	R	Indicates the optical input in dBm. Some SFP cannot display this value. For electrical SFP N/A (not applicable) is shown.
temperature	R	Displays the temperature inside the SFP. This is usually higher than the system temperature.
max_length_9_um	R	Displays nominal maximum reach of this SFP on a standard single mode fiber.
max_length_50_um	R	Displays nominal maximum reach of this SFP on a 50 micro meter multimode fiber.
max_length_62_um	R	Displays nominal maximum reach of this SFP on a 62.5 micro meter multimode fiber.
max_length_copper	R	Displays nominal maximum reach of this SFP on a copper cable. Only applies to electrical SFP.
tuning_range	R	For wavelength tunable optics additional details are shown here.
power_consumption	R	Typical power consumption values are shown if available from the interface.
additional_information	R	Some special SFP can supply additional measurement data. For example OTDR reflection data can be listed here.

18.4 sfp Configuration Parameters

Group	config
Path	Device.sfp.config
Description	These setting apply to each SFP in the system.
loss_of_signal_event	When enabled a loss of optical signal or the return of the signal will create an event.
Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.1.34.1.1.2 (configLossOfSignalEvent)
optical_delta_detect	An optical receive power level change of more than delta_threshold between two successive read cycles generates an event.
Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.1.34.1.1.3 (configOpticalDeltaDetect)
delta_threshold	Defines the dB difference required to trigger an event. Only 1 dB steps are permitted. A value of 0 detects any change. This setting is only for testing. Recommended value: 2.
Value	Number in range 0-6
OID	1.3.6.1.4.1.3181.10.6.1.34.1.1.4 (configDeltaThreshold)

18.5 sfp Status Parameters

Group	information , for all SFP ports[0..47]	
Path	Device.sfp.information[port]	
Description	This table displays data which are read from the inserted SFPs.	
port	Indicates the physical port in which this SFP is inserted.	
	Value	PORTMASK0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.2 (informationPort)
location	Textual description of SFP location.	
	Value	String, max. 16 characters.
	OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.3 (informationLocation)
status	Should indicate OK. LOSS_OF_SIGNAL is shown when the optical receive power level is below the critical lower limit.	
	Values	
	<i>UNKNOWN</i>	This is show when no data could be retrieved.
	<i>OK</i>	Optical operation conditions are OK.
	<i>LASER_DISABLED</i>	Laser is disabled. No data can be sent. The port may be disabled.
	<i>LOSS_OF_SIGNAL</i>	This flag is set when the optical receive power level is below the critical lower limit.
	<i>TX_FAILURE</i>	The laser circuit inside the SFP has detected an error. Try to replug the SFP to unlock this condition.
	<i>READ_ERROR</i>	Management read access to the SFP has failed.
	OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.4 (informationStatus)

type	This parameter shows which type of optics are installed		
Values	EMPTY	No SFP is inserted.	
	UNKNOWN	An SFP is inserted but its type could not be decoded.	
	SFP	A normal SFP is inserted.	
	GBIC	A GBIC is inserted.	
	SFF	An SFF fixed optical interface is installed.	
	DWDM_SFP	A DWDM wavelength selected SFP is inserted.	
	XFP	A XFP is inserted.	
	CSFP_A	A compact double SFP is inserted. This is port A of the CSFP.	
	CSFP_B	A compact double SFP is inserted. This is port B of the CSFP.	
	DWDM_XFP	A DWDM wavelength selected XFP is inserted.	
	SFP_PLUS	A SFP plus is inserted	
OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.5 (informationType)		

connector	Shows which connector is used with this SFP.		
Values	UNKNOWN	Connector type cannot be decoded.	
	LC	LC connector is used.	
	SC	SC connector is used.	
	MT_RJ	MT_RJ connector is used.	
	RJ45	Electrical RJ45 connector is used.	
	MU	MU connector is used.	
OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.6 (informationConnector)		

wavelength	Nominal wavelength if this SFP. May also indicate ITU channel for DWDM optics.		
Value	String, max. 20 characters.		
OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.7 (informationWavelength)		

tx_technology	Distinguishes between multimode and single mode SFP. For DWDM SFP more details including grid are shown.		
Value	String, max. 32 characters.		
OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.8 (informationTxTechnology)		

rx_technology	Distinguishes between normal PIN receivers and more sensitive APD receivers.		
Value	String, max. 16 characters.		
OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.9 (informationRxTechnology)		

nominal_bitrate	Nominal bitrate rounded to nearest 100Mbit. Usually the SFP can be operated at lower speed as well.		
Value	String, max. 16 characters.		
OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.10 (informationNominalBitrate)		

manufacturer	Shows the manufacturer of this SFP.		
	Value	String, max. 20 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.11 (informationManufacturer)	
part_number	Shows the part number of this SFP. This will differ from the MICROSENS order code unless also MICROSENS is indicated as manufacturer.		
	Value	String, max. 20 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.12 (informationPartNumber)	
revision	Internal revision code of this SFP.		
	Value	String, max. 8 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.13 (informationRevision)	
serial_number	Serial number of the SFP.		
	Value	String, max. 20 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.14 (informationSerialNumber)	
mfg_date_code	Manufacturing date code.		
	Value	String, max. 16 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.15 (informationMfgDateCode)	
warnings	Values	NONE	No warnings are present
		TX_POWER_LOW	Transmit power is near low limit indicating laser aging
		TX_POWER_HIGH	Transmit power is near high limit
		TX_BIAS_LOW	Internal SFP warning
		TX_BIAS_HIGH	Internal SFP warning
		VCC_LOW	Operating voltage near limit
		VCC_HIGH	Operating voltage near limit
		TEMP_LOW	The SFP is cold
		TEMP_HIGH	The SFP is running warm
		RX_POWER_LOW	Marginal optical input signal may introduce bit errors
		RX_POWER_HIGH	High input signal is may cause bit errors
	OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.16 (informationWarnings)	

alarms

Values	<i>NONE</i>	No alarms are present
	<i>TX_POWER_TOO_LOW</i>	Transmit power is too low due to laser error or transmitter disable
	<i>TX_POWER_TOO_HIGH</i>	Transmit power is too high due to laser error
	<i>TX_BIAS_TOO_LOW</i>	Internal SFP error
	<i>TX_BIAS_TOO_HIGH</i>	Internal SFP error
	<i>VCC_TOO_LOW</i>	Operating voltage error
	<i>VCC_TOO_HIGH</i>	Operating voltage error
	<i>TEMP_TOO_LOW</i>	The SFP is too cold
	<i>TEMP_TOO_HIGH</i>	The SFP is running too hot
	<i>RX_POWER_TOO_LOW</i>	No optical input signal
	<i>RX_POWER_TOO_HIGH</i>	Input signal is too high for error free operation
OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.17 (informationAlarms)	

tx_power

Indicates the optical output in dBm. Some SFP cannot display this value. For electrical SFP N/A (not applicable) is shown.

Value	String, max. 16 characters.
OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.18 (informationTxPower)

rx_power

Indicates the optical input in dBm. Some SFP cannot display this value. For electrical SFP N/A (not applicable) is shown.

Value	String, max. 16 characters.
OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.19 (informationRxPower)

temperature

Displays the temperature inside the SFP. This is usually higher than the system temperature.

Value	String, max. 16 characters.
OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.20 (informationTemperature)

max_length_9_um

Displays nominal maximum reach of this SFP on a standard single mode fiber.

Value	String, max. 8 characters.
OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.21 (informationMaxLength9Um)

max_length_50_um

Displays nominal maximum reach of this SFP on a 50 micro meter multimode fiber.

Value	String, max. 8 characters.
OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.22 (informationMaxLength50Um)

max_length_62_um	Displays nominal maximum reach of this SFP on a 62.5 micro meter multimode fiber.
Value	String, max. 8 characters.
OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.23 (informationMaxLength62Um)
max_length_copper	Displays nominal maximum reach of this SFP on a copper cable. Only applies to electrical SFP.
Value	String, max. 8 characters.
OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.24 (informationMaxLengthCopper)
tuning_range	For wavelength tunable optics additional details are shown here.
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.25 (informationTuningRange)
power_consumption	Typical power consumption values are shown if available from the interface.
Value	String, max. 20 characters.
OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.26 (informationPowerConsumption)
additional_information	Some special SFP can supply additional measurement data. For example OTDR reflection data can be listed here.
Value	String, max. 128 characters.
OID	1.3.6.1.4.1.3181.10.6.1.34.100.1.27 (informationAdditionalInformation)

19 Power-over-Ethernet (PoE)

19.1 Key Features

PoE and PoE+ support

Up to 30W can be provided to the attached device. The total amount for power per unit depends on power supply and device type.

With PoE cabling can be simplified. Typical use is an IP phone. PoE+ can be required by high-end phones with large displays.

PoE Control

PoE / PoE+ voltage is turned on only after powered device (PD) is detected and classified on port. Output voltage and power is monitored. Port power is shut down if limits are exceeded. Events are generated to alert on PoE problems.

Automated operation. Monitoring is provided when needed. SNMP trap will inform about problems.

PoE+ Enable

PoE+ should only be enabled through LLDP-MED protocol. The unit supports this but also permits PoE+ activation via configuration to support devices that do not support LLDP-MED.

Support the Standard but also permit use with older non-standard devices.

Emergency Port

Port can be assigned priority. Should PoE power limitation occur, the priority (emergency) port(s) are not shut down.

Permits for the connection of an emergency phone.

PD Operation

PD enabled switches can be configured to operate on PoE. In this mode no other power supply is required. When one or two regular power supplies can be connected, then the PoE input can act as secondary backup supply.

Simple setup may omit power supply. PoE input may be used as backup source.

19.2 Functional Description

ATTENTION: This section is only applicable on devices supporting Power-over-Ethernet according to IEEE Std. 802.3af or 802.3at.

Switches with Power-over-Ethernet (PoE) functionality can power connected end-devices. Devices capable of sourcing electrical power are characterized as 'Power Sourcing Equipment' (PSE). End-devices being powered are characterized as 'Powered Device' (PD).

19.2.1 Power Sourcing Equipment (PSE)

Detection

When sourcing power via a network port, special care must be taken to prevent any damaging of non-PoE capable ports. For this reason, a PoE enabled port will never apply a DC voltage to the pins without carefully detecting and classifying the PoE capabilities of the connected device.

In first step a low test voltage is applied to check if the impedance of the connected device is in the correct range for PoE. This is called 'Detection'.

INFO: Some non-PoE capable devices may present a low impedance path to the PSE. This is detected and shown as "SHORT_CIRCUIT" in the port PoE status. PoE power will not be applied to those devices.

Classification

If device detection was successful, a second test voltage sequence is applied to retrieve the PoE class of the device. This process is called 'Classification'.

If a valid class is detected and this class is permitted on the port, then finally the PoE voltage is applied and the connected device gets powered up.

The following classes are supported:

Class	Max. PD Power	Description
0	0.44 to 12.94W	Default PoE class
1	0.44 to 3.84W	Optional, very low power
2	3.84 to 6.49W	Optional, low power
3	6.49 to 12.95W	Optional, mid power
4	12.95 to 25.50W	reserved, high power (PoE plus only)

Power Sourcing

If a connected device is powered, the voltage and current values are permanently monitored. If the voltage or current exceeds or falls below the limits permitted for the power class, the PoE power is shut down automatically to prevent any damage to the device.

PoE (IEEE Std. 802.3af)

First PoE standard version defining a maximum power sourcing of 15.4W per port. The typical supply voltage is 48VDC in a range between 44 to 57VDC.

Valid PD classes are in the range of 0 to 3. Class 4 is reserved.

PoE plus (IEEE Std. 802.3at)

Second edition of the PoE standard, often referred as 'PoE plus', defining a maximum power sourcing of 25.5W per port. While the voltage range remains unchanged between 44 and 57VDC, the minimum voltage for the PSE is 50VDC, with a typical value of 54VDC.

To clearly distinguish the extended power mode from standard PoE, the formerly reserved class 4 is used.

INFO: This option is only available to devices supporting Power-over-Ethernet plus according to IEEE Std. 802.3at.

19.3 POE CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Device.	poe.					Power over Ethernet (POE) settings and statistics.
			poe_max_power_available	R/W		Defines the total power that this units power supply can support. This value is used to balance the PoE output power delivered. Please adjust according to connected power supply rating.
			restart_poe_port	X		This function may be used to briefly drop the power on a PoE port in order to reboot the attached device. Please supply port number as parameter. The shorthand port format like 1 for 1/1 may be used. Syntax examples: poe.restart_poe_port = 1/2,1/5 or poe.restart_poe_port = 1-3 or equivalent poe.restart_poe_port = 1/1-1/3.
			restart_energy_port	X		This function may be used to restart measurement of energy consumption per port. Please supply port number as parameter. The shorthand port format like 1 for 1/1 may be used. Syntax examples: poe.restart_energy_port = 1/2,1/5 or poe.restart_energy_port = 1-3 or equivalent poe.restart_energy_port = 1/1-1/3.
			config[PORT].			Power over Ethernet function permits the powering of connected units which do not use their own local power supply.
			mode	R/W		Used to enable or disable PoE function.
	config[PORT].		priority_port	R/W		Ports without priority may be switched off under a power contention situation.
			enable_poe_plus	R/W		Allow between 15-30W power consumption.
			total_power_consumed	R		The sum of power currently delivered to all ports. (units: mW)
			status[PORT].			This table list the current PoE port conditions.
			condition	R		PoE status and conditions.

determined_class	R	Determined and negotiated PoE class.
output_current	R	Current delivered to the attached device. (units: mA)
output_voltage	R	Voltage delivered to the attached device. (units: mV)
output_power	R	Calculated power delivered to the attached device. (units: mW)
power_denied_counter	R	Incremented whenever a PoE request was denied regardless of reason.
over_current_counter	R	Incremented whenever an over_current condition was detected.
short_circuit_counter	R	Incremented whenever a short circuit was detected.
energy_supplied[PORT].		This table list the power provided via PoE ports. The values are automatically updated in the given interval.
time_of_value_restart	R	Time stamp when the statistics counter had been restarted.
time_since_value_restart	R	How long ago have the statistics counter been restarted.
last_second	R	Energy supplied in the last second. Value in Joule.
accumulated	R	Energy supplied since last value reset. Value in Wh. (1Wh = 3600 Joule = 3600Ws).

19.4 POE Configuration Parameters

Group	General Parameters
Path	Device.POE
poe_max_power_available	<p>Defines the total power that this units power supply can support. This value is used to balance the PoE output power delivered. Please adjust according to connected power supply rating.</p> <p>Value Number in range 0-500</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.33.1 (poePoeMaxPowerAvailable) 1.3.6.1.2.1.105.1.3.1.1.2 (pethMainPsePower)</p>
restart_poe_port	<p>This function may be used to briefly drop the power on a PoE port in order to reboot the attached device. Please supply port number as parameter. The shorthand port format like 1 for 1/1 may be used. Syntax examples: poe.restart_poe_port = 1/2,1/5 or poe.restart_poe_port = 1-3 or equivalent poe.restart_poe_port = 1/1-1/3.</p> <p>Action Execute command with parameter string max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.33.2 (poeRestartPoePort)</p>
restart_energy_port	<p>This function may be used to restart measurement of energy consumption per port. Please supply port number as parameter. The shorthand port format like 1 for 1/1 may be used. Syntax examples: poe.restart_energy_port = 1/2,1/5 or poe.restart_energy_port = 1-3 or equivalent poe.restart_energy_port = 1/1-1/3.</p> <p>Action Execute command with parameter string max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.33.3 (poeRestartEnergyPort)</p>
Group	config , for each port[0..24]
Path	Device.POE.config[port]
Description	Power over Ethernet function permits the powering of connected units which do not use their own local power supply.

mode	Used to enable or disable PoE function.		
	Values	<i>DISABLED</i> PoE function is disabled on this port. <i>AUTOMATIC</i> PoE function is enabled on this port. Attached device is expected to adhere to PoE or POE+ standards. <i>CLASS_0</i> Limits PoE delivery to approximately 13W. <i>CLASS_1</i> Limits PoE delivery to approximately 4W. <i>CLASS_2</i> Limits PoE delivery to approximately 7W. <i>CLASS_3</i> Limits PoE delivery to approximately 13W. <i>CLASS_4</i> Limits PoE delivery to approximately 13W or 26W for when PoE_plus is enabled. <i>FORCED_ON</i> Forces PoE bypassing the regular negotiation protocol. Use with not compliant legacy PoE devices. WARNING: Do not select when attached device does not support PoE. Hardware damage is possible.	
	OID	1.3.6.1.4.1.3181.10.6.1.33.4.1.2 (configMode) 1.3.6.1.2.1.105.1.1.1.3 (pethPsePortAdminEnable)	
priority_port	Ports without priority may be switched off under a power contention situation.		
	Values	enabled, disabled	
	OID	1.3.6.1.4.1.3181.10.6.1.33.4.1.3 (configPriorityPort) 1.3.6.1.2.1.105.1.1.1.7 (pethPsePortPowerPriority)	
enable_poe_plus	Allow between 15-30W power consumption.		
	Values	<i>DISABLED</i> PoE+ function is disabled on this port. <i>ENABLED</i> PoE+ function is enabled on this port. <i>LLDP_CONTROLLED</i> PoE+ function is enabled only when requested via LLDP-MED	
	OID	1.3.6.1.4.1.3181.10.6.1.33.4.1.4 (configEnablePoePlus)	

19.5 POE Status Parameters

Group	General Parameters		
Path	Device.POE		
total_power_consumed	The sum of power currently delivered to all ports. (units: mW)		
	Value	Number in range 0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.1.33.100 (poeTotalPowerConsumed) 1.3.6.1.2.1.105.1.3.1.1.4 (pethMainPseConsumptionPower)	

Group	status, for all ports[0..31]		
Path	Device.POE.status[port]		
Description	This table list the current PoE port conditions.		

condition	PoE status and conditions.		
	Values	<div><div>DISABLED</div><div>POWER_OFF</div><div>DISCOVERING</div><div>POWERED</div><div>CLASS_MISMATCH</div><div>SHORT_CIRCUIT</div><div>REJECTED</div><div>OVER_CURRENT</div><div>OVER_TEMP</div><div>VOLTAGE_TOO_LOW</div></div> <div><div>PoE function is disabled</div><div>PoE inactive / not required</div><div>discovering POE partner</div><div>PoE is active and OK</div><div>Requested class was higher than max_class parameter permits</div><div>The cable to the device has a short circuit. The attached unit may not support PoE. No harm will occur due to short circuit protection.</div><div>POE rejected</div><div>Overcurrent</div><div>over temperature fault. PoE may be power down.</div><div>Operating voltage to unit is too low for full PoE operation</div></div>	
	OID	1.3.6.1.4.1.3181.10.6.1.33.101.1.2 (statusCondition) 1.3.6.1.2.1.105.1.1.1.6 (pethPsePortDetectionStatus)	

determined_class	Determined and negotiated PoE class.		
	Values	IS_CLASS_0	approx. 12.5W
		IS_CLASS_1	approx. 4W
		IS_CLASS_2	approx. 6.5W
		IS_CLASS_3	approx. 12.5W
		IS_CLASS_4	approx. 15W or 30W if poe_plus is enabled.
		IS_OVERLOAD	too much power for selected class is required.
		PROBES_NOT_EQUAL	
		IS_UNKNOWN	
	OID	1.3.6.1.4.1.3181.10.6.1.33.101.1.3 (statusDeterminedClass) 1.3.6.1.2.1.105.1.1.1.10 (pethPsePortPowerClassifications)	

output_current	Current delivered to the attached device. (units: mA)		
	Value	Number in range 0-65535	
	OID	1.3.6.1.4.1.3181.10.6.1.33.101.1.4 (statusOutputCurrent)	

output_voltage	Voltage delivered to the attached device. (units: mV)		
	Value	Number in range 0-65535	
	OID	1.3.6.1.4.1.3181.10.6.1.33.101.1.5 (statusOutputVoltage)	

output_power	Calculated power delivered to the attached device. (units: mW)		
	Value	Number in range 0-65535	
	OID	1.3.6.1.4.1.3181.10.6.1.33.101.1.6 (statusOutputPower)	

power_denied_counter	Incremented whenever a PoE request was denied regardless of reason.		
	Value	Number in range 0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.1.33.101.1.7 (statusPowerDeniedCounter) 1.3.6.1.2.1.105.1.1.1.12 (pethPsePortPowerDeniedCounter)	

over_current_counter	Incremented whenever an over_current condition was detected.		
	Value	Number in range 0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.1.33.101.1.8 (statusOverCurrentCounter) 1.3.6.1.2.1.105.1.1.1.13 (pethPsePortOverLoadCounter)	

short_circuit_counter	Incremented whenever a short circuit was detected.		
	Value	Number in range 0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.1.33.101.1.9 (statusShortCircuitCounter) 1.3.6.1.2.1.105.1.1.1.14 (pethPsePortShortCounter)	

Group Path Description	energy_supplied , for all ports[0..31] Device.POE.energy_supplied[port] This table list the power provided via PoE ports. The values are automatically updated in the given interval.	
time_of_value_restart	Time stamp when the statistics counter had been restarted.	Value TIMESTAMP0-0xFFFFFFFF OID 1.3.6.1.4.1.3181.10.6.1.33.102.1.2 (energySuppliedTimeOfValueRestart)
time_since_value_restart	How long ago have the statistics counter been restarted.	Value PERIOD0-0xFFFFFFFF OID 1.3.6.1.4.1.3181.10.6.1.33.102.1.3 (energySuppliedTimeSinceValueRestart)
last_second	Energy supplied in the last second. Value in Joule.	Value Number in range 0-0xFFFFFFFF OID 1.3.6.1.4.1.3181.10.6.1.33.102.1.4 (energySuppliedLastSecond)
accumulated	Energy supplied since last value reset. Value in Wh. (1Wh = 3600 Joule = 3600Ws).	Value Number in range 0-0xFFFFFFFF OID 1.3.6.1.4.1.3181.10.6.1.33.102.1.5 (energySuppliedAccumulated)

20 MAC Table

20.1 Key Features

MAC Table

The device supports up to 8192 MAC addresses. MAC addresses may be learned or manually configured.

Large number of MACs permits use in large networks.

MAC Filter

Various display filter permit access to table of MAC addresses known to the switch. Predefined plus custom filter to search mac table are provided.

Management access is useful for trouble shooting.

SNMP Access

D-BRIDGE and Q-BRIDGE MIBs are supported.

Permits use with automated security systems such as MACMON or ArpGuard.

MAC Limit

Limit number of allowed MAC addresses per port. Independent of other port access control functions.

MAC Limit per VLAN

Limit number of allowed MAC addresses per port and VLAN. Independent of other port access control functions.

Configurable MAC Aging Time

MAC aging time can be configured between 15s and 1 hour. Defaults to 5 minutes.

20.2 Functional Description

MAC Address Table

The switch provides detailed information about which MAC source address is learned on which port.

20.3 MAC CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Device.						
	mac.					MAC Address Monitoring
			filter_port		X	Filter MAC table to show only MACs associated with a given port range. The shorthand port format like 1 for 1/1 may be used. Syntax examples: mac.filter_port = 1/2,1/5 or mac.filter_port = 1-3,5.
			filter_user_ports		X	Filter MAC table to show only MACs associated with user ports. This excluded the links. This view eliminates MACs which are not of local interest. No parameter is required.
			filter_vlan		X	Filter MAC table to show only MACs associated with a given VLAN range. Supply VLAN ID as parameter. Syntax example: mac.filter_vlan = 1-4,1000-2000.
			filter_mac		X	Filter MAC table to find a specific MAC address and return the associated port and VLAN. Supply MAC address as parameter. Enter only the first 3 value pairs of the MAC to search for vendor MACs. Syntax example: mac.filter_mac = 01:22:3A.
			filter_custom		X	Filter MAC table according to supplied rules: [-m MAC] [-s SEPARATOR] [-p PORTS] [-v VLANS] or do not enter any parameter and see all MACs.
			filter_multicast_vlan		X	Filter MAC table to show only multicast MACs associated with a given VLAN range. Supply VLAN ID as parameter. Syntax example: mac.filter_multicast_vlan = 1-4,1000-2000.
			filter_multicast_port		X	Filter MAC table to show only multicast MACs associated with a given port range. Supply port as parameter. The shorthand port format like 1 for 1/1 may be used. Syntax examples: mac.filter_multicast_port = 1/2,1/5 or mac.filter_multicast_port = 1-3,5.

clear_learned_mac_table	X	Wipe out all learned MAC addresses. Static entries are kept intact. No parameter required.
clear_mac_table_for_vlan	X	Wipe out all MAC addresses for a given VLAN. Please provide the VLAN ID as parameter.
hide_macs_on_link_ports	R/W	When enabled only MACs on local access ports are listed in the MAC table. The MAC entries associated with link ports are excluded. This may significantly reduce the number of shown entries and also speed MAC table reading via SNMP.
global_aging_time	R/W	The MAC aging timeout can be configured in steps of 15 seconds. The nearest value is taken.
number_of_entries	R	Total number of MAC address entries in the table.
number_of_igmp_entries	R	Number of multicast MAC address entries in the table related to IGMP or MLD snooping.
used_aging_time	R	The actually used aging time which may be modified by RSTP or local setting <code>mac.global_aging_time</code>
number_of_hidden_entries	R	When the <code>mac.hide_macs_on_link_ports</code> parameter is enabled, this value indicates how many MACs associated with link ports are not shown.
mac_table[8192].		This table lists all MAC addresses maintained by the device. This is an unfiltered list.
mac	R	MAC address entry
port	R	Port number for MAC address
state	R	Entry state indicates further details.
vlan	R	if non zero this MAC is part of this VLAN.
currently_authorized_macs[256].		This table lists all MAC addresses currently authorized via port access control.
mac	R	MAC address entry
port	R	Port number for MAC address
state	R	Entry state indicates further details.
vlan	R	if non zero this MAC is part of this VLAN.
database	R	Internal database index

20.4 MAC Configuration Parameters

Group Path	General Parameters
	Device.MAC
filter_port	<p>Filter MAC table to show only MACs associated with a given port range. The shorthand port format like 1 for 1/1 may be used. Syntax examples: mac.filter_port = 1/2,1/5 or mac.filter_port = 1-3,5.</p> <p>Action Execute command with parameter string max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.86.1 (macFilterPort)</p>
filter_user_ports	<p>Filter MAC table to show only MACs associated with user ports. This excluded the links. This view eliminates MACs which are not of local interest. No parameter is required.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.86.2 (macFilterUserPorts)</p>
filter_vlan	<p>Filter MAC table to show only MACs associated with a given VLAN range. Supply VLAN ID as parameter. Syntax example: mac.filter_vlan = 1-4,1000-2000.</p> <p>Action Execute command with parameter string max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.86.3 (macFilterVlan)</p>
filter_mac	<p>Filter MAC table to find a specific MAC address and return the associated port and VLAN. Supply MAC address as parameter. Enter only the first 3 value pairs of the MAC to search for vendor MACs. Syntax example: mac.filter_mac = 01:22:3A.</p> <p>Action Execute command with parameter string max. 25 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.86.4 (macFilterMac)</p>
filter_custom	<p>Filter MAC table according to supplied rules: [-m MAC] [-s SEPARATOR] [-p PORTS] [-v VLANS] or do not enter any parameter and see all MACs.</p> <p>Action Execute command with parameter string max. 45 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.86.5 (macFilterCustom)</p>
filter_multicast_vlan	<p>Filter MAC table to show only multicast MACs associated with a given VLAN range. Supply VLAN ID as parameter. Syntax example: mac.filter_multicast_vlan = 1-4,1000-2000.</p> <p>Action Execute command with parameter string max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.86.6 (macFilterMulticastVlan)</p>

filter_multicast_port	<p>Filter MAC table to show only multicast MACs associated with a given port range. Supply port as parameter. The shorthand port format like 1 for 1/1 may be used. Syntax examples: mac.filter_multicast_port = 1/2,1/5 or mac.filter_multicast_port = 1-3,5.</p> <p>Action Execute command with parameter string max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.86.7 (macFilterMulticastPort)</p>
clear_learned_mac_table	<p>Wipe out all learned MAC addresses. Static entries are kept intact. No parameter required.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.86.8 (macClearLearnedMacTable)</p>
clear_mac_table_for_vlan	<p>Wipe out all MAC addresses for a given VLAN. Please provide the VLAN ID as parameter.</p> <p>Action Execute command with parameter string max. 5 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.86.9 (macClearMacTableForVlan)</p>
hide_macs_on_link_ports	<p>When enabled only MACs on local access ports are listed in the MAC table. The MAC entries associated with link ports are excluded. This may significantly reduce the number of shown entries and also speed MAC table reading via SNMP.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.86.10 (macHideMacsOnLinkPorts)</p>
global_aging_time	<p>The MAC aging timeout can be configured in steps of 15 seconds. The nearest value is taken.</p> <p>Value Number in range 15-3825</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.86.11 (macGlobalAgingTime) 1.3.6.1.2.1.17.4.2 (dot1dTpAgingTime)</p>

20.5 MAC Status Parameters

Group Path	General Parameters Device.MAC
number_of_entries	<p>Total number of MAC address entries in the table.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.86.100 (macNumberOfEntries)</p>
number_of_igmp_entries	<p>Number of multicast MAC address entries in the table related to IGMP or MLD snooping.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.86.101 (macNumberOfIgmpEntries)</p>
used_aging_time	<p>The actually used aging time which may be modified by RSTP or local setting mac.global_aging_time</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.86.102 (macUsedAgingTime)</p>
number_of_hidden_entires	<p>When the mac.hide_macs_on_link_ports parameter is enabled, this value indicates how many MACs associated with link ports are not shown.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.86.103 (macNumberOfHiddenEntires)</p>

21 Remote Monitoring (RMON)

21.1 Key Features

RMON counters

35 integrated counters per port for detailed traffic analysis and network trouble shooting.

RMON values may be used with automated test system through the RMON MIB and Etherlike-MIB.

Port Utilization

For each port the utilization in % is shown independantly for each direction. A current utilization is shown as well as averaged values over 30s and 5 minutes.

The values help to judge if a higher port speed should be used. High percent values indicate the port is overutilized.

Port Mirroring

Data of one or more ports can be copied onto anohter port. On the monitoring port the data can be analyzed with an external device.

Eases protocol trouble shooting. Can also be used to monitor user traffic.

21.2 Functional Description

RMON Counters

The switch provides detailed statistic information about traffic type and throughput. These counters can be retrieved per port and direction (ingress or egress)

21.3 RMON CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description	
Device.	rmon.	RMON Remote Monitoring					
		clear_all_counter		X		When executed all roman counters of all ports are reset to 0. This has no service implications.	
	ingress[PORT].	entry_status		R		Indicated whether this ports table is updated and valid.	
		in_good_octets_lo		R		Number of bytes received without error (low)	
		in_good_octets_hi		R		Number of bytes received without error (high)	
		in_bad_octets		R		Number of bytes received with error.	
		in_total_packets		R		Number of packets on any type received.	
		in_unicasts		R		Number of unicast packets received.	
		in_non_unicasts		R		Number of packets which are non unicast type.	
		in_broadcasts		R		Number of broadcast packets received.	
		in_multicasts		R		Number of multicast packets received.	
		in_pause		R		Number of pause frames received.	
		in_total_receive_errors		R		Number of packets received with any kind of error.	
		in_undersize		R		Number of undersized frames received.	
		in_oversize		R		Number of oversized frames received.	
		in_fragments		R		Number of fragmented frames received.	
		in_jabber		R		Number of jabbers received.	
		in_fcs_errors		R		Number of checksum errors.	
		in_discarded		R		Number of frames discard due to lack of internal buffer space.	
		egress[PORT].	Statistics regarding outbound traffic				
			out_good_octets_lo		R		Number of bytes transmitted without error (low)
			out_good_octets_hi		R		Number of bytes transmitted without error (high)

out_unicasts	R	Number of unicast packets transmitted
out_non_unicasts	R	Number of packets which are non unicast type
out_broadcasts	R	Number of broadcast packets transmitted
out_multicasts	R	Number of multicast packets transmitted
out_pause	R	Number of pause frames transmitted
out_deferred	R	Number of deferred frames due to a busy condition. This is not an error condition.
out_total_collisions	R	Number of all collisions that have occurred on that port. A collision may occur on a half-duplex interface detecting an incoming packet at the time it was trying to transmit a packet.
out_single_collisions	R	Number of times the port has experienced a single collision when attempting to transmit a packet.
out_multiple_collisions	R	Number of times the port has experienced a multiple collision when attempting to transmit a packet.
out_excessive_collisions	R	Number of times a packet could not be sent due to repeated collisions on the same packet..
out_late_collisions	R	Number of times a late collision has occurred. A late collision occurs when the switch detects an incoming packet after it has already transmitted more than 64 bytes of its current outgoing packet. This indicates a half duplex - full duplex mismatch.
out_fcs_errors	R	Number of checksum errors
out_dropped_packets	R	Number of good outgoing frames that were dropped due to outgoing policies
histogram[PORT].		The histogram indicates the packet size distribution for incoming data per port.
in_64_octets	R	Number of minimum size frames received
in_65_to_127_octets	R	Number of frames with size between 65 and 127 bytes received
in_128_to_255_octets	R	Number of frames with size between 128 and 255 bytes received
in_256_to_511_octets	R	Number of frames with size between 256 and 511 bytes received
in_512_to_1023_octets	R	Number of frames with size between 512 and 1023 bytes received
in_1024_to_max_octets	R	Number of frames with size above 1023 bytes received
utilization[PORT].		Calculates averaged data utilization values for each port.
ingress_now	R	Percentage of received utilization in the last second.

ingress_30s	R	Percentage of received utilization averaged over last 30s.
ingress_5min	R	Percentage of received utilization averaged over last 5 minutes.
egress_now	R	Percentage of outgoing utilization in the last second.
egress_30s	R	Percentage of outgoing utilization averaged over last 30s.
egress_5min	R	Percentage of outgoing utilization averaged over last 5 minutes.

21.4 RMON Configuration Parameters

Group Path	General Parameters
	Device.RMON
clear_all_counter	<p>When executed all roman counters of all ports are reset to 0. This has no service implications.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.85.1 (rmonClearAllCounter)</p>

21.5 RMON Status Parameters

Group	ingress, for all ports[0..31]	
Path	Device.RMON.ingress[port]	
Description	Statistics regarding inbound traffic	
entry_status	Indicated whether this ports table is updated and valid.	
	Values	<i>INVALID</i> The port is disabled and statistics data are no longer updated <i>VALID</i> The port is active and the statistics data are valid
	OID	1.3.6.1.4.1.3181.10.6.1.85.100.1.2 (ingressEntryStatus) 1.3.6.1.2.1.16.1.1.1.21 (etherStatsStatus)
in_good_octets_lo	Number of bytes received without error (low)	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.100.1.3 (ingressInGoodOctetsLo) 1.3.6.1.2.1.2.2.1.10 (ifInOctets) 1.3.6.1.2.1.16.1.1.1.4 (etherStatsOctets)
in_good_octets_hi	Number of bytes received without error (high)	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.100.1.4 (ingressInGoodOctetsHi)
in_bad_octets	Number of bytes received with error.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.100.1.5 (ingressInBadOctets) 1.3.6.1.2.1.16.1.1.1.8 (etherStatsCRCAlignErrors) 1.3.6.1.2.1.10.7.2.1.2 (dot3StatsAlignmentErrors)
in_total_packets	Number of packets on any type received.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.100.1.6 (ingressInTotalPackets) 1.3.6.1.2.1.16.1.1.1.5 (etherStatsPkts)
in_unicasts	Number of unicast packets received.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.100.1.7 (ingressInUnicasts) 1.3.6.1.2.1.2.2.1.11 (ifInUcastPkts)
in_non_unicasts	Number of packets which are non unicast type.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.100.1.8 (ingressInNonUnicasts) 1.3.6.1.2.1.2.2.1.12 (ifInNUcastPkts)

in_broadcasts	Number of broadcast packets received.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.100.1.9 (ingressInBroadcasts) 1.3.6.1.2.1.16.1.1.1.6 (etherStatsBroadcastPkts)
in_multicasts	Number of multicast packets received.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.100.1.10 (ingressInMulticasts) 1.3.6.1.2.1.16.1.1.1.7 (etherStatsMulticastPkts)
in_pause	Number of pause frames received.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.100.1.11 (ingressInPause) 1.3.6.1.2.1.10.7.10.1.3 (dot3InPauseFrames)
in_total_receive_errors	Number of packets received with any kind of error.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.100.1.12 (ingressInTotalReceiveErrors)
in_undersize	Number of undersized frames received.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.100.1.13 (ingressInUndersize) 1.3.6.1.2.1.16.1.1.1.9 (etherStatsUndersizePkts)
in_oversize	Number of oversized frames received.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.100.1.14 (ingressInOversize) 1.3.6.1.2.1.16.1.1.1.10 (etherStatsOversizePkts) 1.3.6.1.2.1.10.7.2.1.13 (dot3StatsFrameTooLongs) 1.3.6.1.2.1.17.1.4.1.5 (dot1dBasePortMtuExceededDiscards)
in_fragments	Number of fragmented frames received.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.100.1.15 (ingressInFragments) 1.3.6.1.2.1.16.1.1.1.11 (etherStatsFragments)
in_jabber	Number of jabbers received.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.100.1.16 (ingressInJabber) 1.3.6.1.2.1.16.1.1.1.12 (etherStatsJabbers)

in_fcs_errors	Number of checksum errors.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.100.1.17 (ingressInFcsErrors) 1.3.6.1.2.1.2.2.1.14 (ifInErrors) 1.3.6.1.2.1.10.7.2.1.3 (dot3StatsFCSErrors)
in_discarded	Number of frames discard due to lack of internal buffer space.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.100.1.18 (ingressInDiscarded) 1.3.6.1.2.1.2.2.1.13 (ifInDiscards)
Group	egress , for all ports[0..31]	
Path	Device.RMON.egress[port]	
Description	Statistics regarding outbound traffic	
out_good_octets_lo	Number of bytes transmitted without error (low)	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.101.1.2 (egressOutGoodOctetsLo) 1.3.6.1.2.1.2.2.1.16 (ifOutOctets)
out_good_octets_hi	Number of bytes transmitted without error (high)	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.101.1.3 (egressOutGoodOctetsHi)
out_unicasts	Number of unicast packets transmitted	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.101.1.4 (egressOutUnicasts) 1.3.6.1.2.1.2.2.1.17 (ifOutUcastPkts)
out_non_unicasts	Number of packets which are non unicast type	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.101.1.5 (egressOutNonUnicasts) 1.3.6.1.2.1.2.2.1.18 (ifOutNUcastPkts)
out_broadcasts	Number of broadcast packets transmitted	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.101.1.6 (egressOutBroadcasts)
out_multicasts	Number of multicast packets transmitted	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.101.1.7 (egressOutMulticasts)

out_pause	Number of pause frames transmitted
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.1.85.101.1.8 (egressOutPause) 1.3.6.1.2.1.10.7.10.1.4 (dot3OutPauseFrames)
out_deferred	Number of deferred frames due to a busy condition. This is not an error condition.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.1.85.101.1.9 (egressOutDeferred) 1.3.6.1.2.1.10.7.2.1.7 (dot3StatsDeferredTransmissions)
out_total_collisions	Number of all collisions that have occurred on that port. A collision may occur on a half-duplex interface detecting an incoming packet at the time it was trying to transmit a packet.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.1.85.101.1.10 (egressOutTotalCollisions) 1.3.6.1.2.1.16.1.1.1.13 (etherStatsCollisions)
out_single_collisions	Number of times the port has experienced a single collision when attempting to transmit a packet.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.1.85.101.1.11 (egressOutSingleCollisions) 1.3.6.1.2.1.10.7.2.1.4 (dot3StatsSingleCollisionFrames)
out_multiple_collisions	Number of times the port has experienced a multiple collision when attempting to transmit a packet.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.1.85.101.1.12 (egressOutMultipleCollisions) 1.3.6.1.2.1.10.7.2.1.13 (dot3StatsMultipleCollisionFrames)
out_excessive_collisions	Number of times a packet could not be sent due to repeated collisions on the same packet..
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.1.85.101.1.13 (egressOutExcessiveCollisions) 1.3.6.1.2.1.10.7.2.1.9 (dot3StatsExcessiveCollisions)
out_late_collisions	Number of times a late collision has occurred. A late collision occurs when the switch detects an incoming packet after it has already transmitted more than 64 bytes of its current outgoing packet. This indicates a half duplex - full duplex mismatch.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.1.85.101.1.14 (egressOutLateCollisions) 1.3.6.1.2.1.10.7.2.1.8 (dot3StatsLateCollisions)

out_fcs_errors	Number of checksum errors
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.1.85.101.1.15 (egressOutFcsErrors) 1.3.6.1.2.1.2.2.1.20 (ifOutErrors)
out_dropped_packets	Number of good outgoing frames that were dropped due to outgoing policies
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.1.85.101.1.16 (egressOutDroppedPackets) 1.3.6.1.2.1.2.2.1.19 (ifOutDiscards) 1.3.6.1.2.1.16.1.1.1.3 (etherStatsDropEvents) 1.3.6.1.2.1.17.1.4.1.4 (dot1dBasePortDelayExceededDiscards)
Group Path Description	histogram , for all ports[0..31] Device.RMON.histogram[port] The histogram indicates the packet size distribution for incoming data per port.
in_64_octets	Number of minimum size frames received
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.1.85.102.1.2 (histogramIn64Octets) 1.3.6.1.2.1.16.1.1.1.14 (etherStatsPkts64Octets)
in_65_to_127_octets	Number of frames with size between 65 and 127 bytes received
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.1.85.102.1.3 (histogramIn65To127Octets) 1.3.6.1.2.1.16.1.1.1.15 (etherStatsPkts65to127Octets)
in_128_to_255_octets	Number of frames with size between 128 and 255 bytes received
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.1.85.102.1.4 (histogramIn128To255Octets) 1.3.6.1.2.1.16.1.1.1.16 (etherStatsPkts128to255Octets)
in_256_to_511_octets	Number of frames with size between 256 and 511 bytes received
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.1.85.102.1.5 (histogramIn256To511Octets) 1.3.6.1.2.1.16.1.1.1.17 (etherStatsPkts256to511Octets)

in_512_to_1023_octets	Number of frames with size between 512 and 1023 bytes received	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.102.1.6 (histogramIn512To1023Octets) 1.3.6.1.2.1.16.1.1.1.18 (etherStatsPkts512to1023Octets)
in_1024_to_max_octets	Number of frames with size above 1023 bytes received	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.1.85.102.1.7 (histogramIn1024ToMaxOctets) 1.3.6.1.2.1.16.1.1.1.19 (etherStatsPkts1024to1518Octets)
Group Path Description	utilization , for all ports[0..31] Device.RMON.utilization[port] Calculates averaged data utilization values for each port.	
ingress_now	Percentage of received utilization in the last second.	
	Value	Number in range 0-255
	OID	1.3.6.1.4.1.3181.10.6.1.85.103.1.2 (utilizationIngressNow)
ingress_30s	Percentage of received utilization averaged over last 30s.	
	Value	Number in range 0-255
	OID	1.3.6.1.4.1.3181.10.6.1.85.103.1.3 (utilizationIngress30s)
ingress_5min	Percentage of received utilization averaged over last 5 minutes.	
	Value	Number in range 0-255
	OID	1.3.6.1.4.1.3181.10.6.1.85.103.1.4 (utilizationIngress5min)
egress_now	Percentage of outgoing utilization in the last second.	
	Value	Number in range 0-255
	OID	1.3.6.1.4.1.3181.10.6.1.85.103.1.5 (utilizationEgressNow)
egress_30s	Percentage of outgoing utilization averaged over last 30s.	
	Value	Number in range 0-255
	OID	1.3.6.1.4.1.3181.10.6.1.85.103.1.6 (utilizationEgress30s)
egress_5min	Percentage of outgoing utilization averaged over last 5 minutes.	
	Value	Number in range 0-255
	OID	1.3.6.1.4.1.3181.10.6.1.85.103.1.7 (utilizationEgress5min)

22 MSP 1000

22.1 Key Features

Forward Migration

The new NM3 management module brings all the benefits of the G6 system the to the MSP1000 Optical WDM System. All features of the previous generation are retained and even legacy TeraMile and LastMile products are supported and can be upgraded.

More than 10 year old installations can be upgraded to the latest management standards and security algorithms.

Inventory

Automatic detection of inserted modules. Detailed inventory information are collected and presented.

Configuration and Status

All MSP 1000 modules as well as legacy TeraMile and LastMile modules can fully be configured and managed. This is possible via all management interfaces such as SNMP, Web, CLI and NMP Manager.

Alarm Correlation

In combination with NMP trap based alarms can be shown in an active list that only shows active alarm conditions. Once rectified they are removed from the alarm list.

This shows a live network alarm summary without the need to look at each trap individually.

Active and Passive mode

In passive mode the NM3 learns the settings of all inserted modules and keeps track of them. In active mode the NM3 forces its locally defined configuration onto the other modules.

Advantage of passive mode is that it works like the previous generation. Advantage of the active mode is that a replaced transponder will automatically be reconfigured to match the requirement of the installation. This simplifies service cases.

22.2 Functional Description

MSP1000

MSP 1000 Optical Transport Platform network management related parameter.

INFO: This feature is only available for NM3/NM3+ Network Management modules for MSP1000.

22.3 MSP1000 CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Device.	mSP1000.					All config and status options related to the optical multi service platform MSP1000.
	system_config.					
			nms_operation_mode	R/W		Read and learn in PASSIVE mode or ACTIVE mode forcing configuration upon the other modules.
			core_mode	R/W		Use V2 unless used with an older system running in V1 mode. Only change when instructed.
			node_id	R/W		Node Id used when NMS is used in combination with SEEmiles V5 management software. When in doubt use default node id 60000.
			disable_legacy_access	R/W		When set network access via SEEmiles is no longer possible.
	slot_config[12].					
			module	R/W		Defines which module is expected to be placed in this slot. This should be identical to the actual hardware. The value may be set prior to actual roll-out to preconfigure the system.
			sparepart_mode	R/W		When enabled the module is operating normally but will not generate any alarms. This is useful for modules that are inserted but only used as spare and are not properly connected at this time. This way unnecessary alarms are avoided.
			port_1_alias	R/W		User defined port name for easier reference.
			port_2_alias	R/W		User defined port name for easier reference.
			port_3_alias	R/W		User defined port name for easier reference.
			port_4_alias	R/W		User defined port name for easier reference.
	x2g_config[12].					This table is used to define any X2G or OFX-3 modules in the system.

port_1_datarate	R/W	This parameter defines the data rate used to setup the internal retimer to provide 3R regeneration. Note that internally interconnected ports must be set to the same rate.
port_2_datarate	R/W	This parameter defines the data rate used to setup the internal retimer to provide 3R regeneration. Note that internally interconnected ports must be set to the same rate.
port_3_datarate	R/W	This parameter defines the data rate used to setup the internal retimer to provide 3R regeneration. Note that internally interconnected ports must be set to the same rate.
port_4_datarate	R/W	This parameter defines the data rate used to setup the internal retimer to provide 3R regeneration. Note that internally interconnected ports must be set to the same rate.
cross_connect	R/W	This parameter defines the data path through the module. It is also used to setup a permanent bit error rate test.
deactivate_port_1	R/W	When enabled, the optical interface is disabled and communication is cut.
deactivate_port_2	R/W	When enabled, the optical interface is disabled and communication is cut.
deactivate_port_3	R/W	When enabled, the optical interface is disabled and communication is cut.
deactivate_port_4	R/W	When enabled, the optical interface is disabled and communication is cut.
front_panel_mode	R/W	Determines what is displayed on the front panel, when available. Also controls the modules local buttons.
loss_of_signal_handling	R/W	When set to LOCAL a loss of input signal will not affect another port. When set to PERCOLATE, a loss of signal will turn off the transmitter of the currently associated port.
optimized_for_8b10b	R/W	Enable this feature when Ethernet or FibreChannel is used. Do not set when SDH is used on any port.
bert_pattern	R/W	Defines the bit pattern with which the build-in bit error rate tester (BERT) operates when cross connect is set to BERT.
sfp_delta_interval	R/W	This enables and defines the interval in which the optical receive power level of each SFP is read and compared to previous value.
sfp_delta_threshold	R/W	This defines how much the optical receive power level can differ between successive reads before a warning trap is generated.

backup_trigger	R/W	Defines under which optical signal condition an automated backup is initiated.
stay_with_last_link	R/W	When set the backup switch remains in last position even when signal returns. Still the backup warning turns off after the delay set under backup_end parameter expires.
backup_end	R/W	Defines how long the signal must remain steady before proper operation is assumed and the backup is terminated.
permit_link_override	R/W	Permits the manual selection of a failed link using the link selection. Defaults to false to safeguard against accidental link selection which would result in loss of connection.
txg_config[12].		This table is used to define any TXG or XCM-2 modules in the system.
txg_datarate	R/W	This parameter defines the data rate used to setup the internal retimer to provide 3R regeneration. Note that internally interconnected ports must be set to the same rate.
txg_operation_mode	R/W	This parameter defines the data path through the module when an internal cross connect is available. It is also used to setup a permanent bit error rate test. (most settings apply to X2G, TXG, OFX-3, XCM-2 only)
port_1_itu_channel	R/W	Tunable laser are supported. Select the wavelength from the supplied 100GHZ ITU-T grid. If the wavelength is not supported by the XFP, a warning event will be received.
port_2_itu_channel	R/W	Tunable laser are supported. Select the wavelength from the supplied 100GHZ ITU-T grid. If the wavelength is not supported by the XFP, a warning event will be received.
deactivate_port_1	R/W	When enabled, the optical interface is disabled and communication is cut.
deactivate_port_2	R/W	When enabled, the optical interface is disabled and communication is cut.
front_panel_mode	R/W	Determines what is displayed on the front panel, when available. Also controls the modules local buttons.
loss_of_signal_handling	R/W	When set to LOCAL a loss of input signal will not affect another port. When set to PERCOLATE, a loss of signal will turn off the transmitter of the other port.
bert_pattern	R/W	Defines the bit pattern with which the build-in bit error rate tester (BERT) operates when cross connect is set to BERT.

sfp_delta_interval	R/W	This enables and defines the interval in which the optical receive power level of each SFP/XFP is read and compared to previous value.
sfp_delta_threshold	R/W	This defines how much the optical receive power level can differ between successive reads before a warning trap is generated.
cxg_plus_config[12].		This table is used to define any CXG+ or OFC-10 modules in the system.
cxg_port_1_2_datarate	R/W	The CXG relies on the features of the XFP to define its data rate. Since various XFP offer different rates with the same settings, only a general setting is provided. Both ports must operate at the same rate.
cxg_port_3_4_datarate	R/W	The CXG relies on the features of the XFP to define its data rate. Since various XFP offer different rates with the same settings, only a general setting is provided. Both ports must operate at the same rate.
port_1_itu_channel	R/W	Tunable laser are supported. Select the wavelength from the supplied 100GHZ ITU-T grid. If the wavelength is not supported by the XFP, a warning event will be received.
port_2_itu_channel	R/W	Tunable laser are supported. Select the wavelength from the supplied 100GHZ ITU-T grid. If the wavelength is not supported by the XFP, a warning event will be received.
port_3_itu_channel	R/W	Tunable laser are supported. Select the wavelength from the supplied 100GHZ ITU-T grid. If the wavelength is not supported by the XFP, a warning event will be received.
port_4_itu_channel	R/W	Tunable laser are supported. Select the wavelength from the supplied 100GHZ ITU-T grid. If the wavelength is not supported by the XFP, a warning event will be received.
deactivate_port_1	R/W	When enabled, the optical interface is disabled and communication is cut.
deactivate_port_2	R/W	When enabled, the optical interface is disabled and communication is cut.
deactivate_port_3	R/W	When enabled, the optical interface is disabled and communication is cut.
deactivate_port_4	R/W	When enabled, the optical interface is disabled and communication is cut.
front_panel_mode	R/W	Determines what is displayed on the front panel, when available. Also controls the modules local buttons.

loss_of_signal_handling	R/W	When set to LOCAL a loss of input signal will not affect another port. When set to PERCOLATE, a loss of signal will turn off the transmitter of the other port.
sfp_delta_interval	R/W	This enables and defines the interval in which the optical receive power level of each SFP/XFP is read and compared to previous value.
sfp_delta_threshold	R/W	This defines how much the optical receive power level can differ between successive reads before a warning trap is generated.
cxg_config[12].		This table is used to define any CXG or XCM-3 modules in the system.
cxg_port_1_2_datarate	R/W	The CXG relies on the features of the XFP to define its data rate. Since various XFP offer different rates with the same settings, only a general setting is provided. Both ports must operate at the same rate.
port_1_itu_channel	R/W	Tunable laser are supported. Select the wavelength from the supplied 100GHZ ITU-T grid. If the wavelength is not supported by the XFP, a warning event will be received.
port_2_itu_channel	R/W	Tunable laser are supported. Select the wavelength from the supplied 100GHZ ITU-T grid. If the wavelength is not supported by the XFP, a warning event will be received.
deactivate_port_1	R/W	When enabled, the optical interface is disabled and communication is cut.
deactivate_port_2	R/W	When enabled, the optical interface is disabled and communication is cut.
front_panel_mode	R/W	Determines what is displayed on the front panel, when available. Also controls the modules local buttons.
loss_of_signal_handling	R/W	When set to LOCAL a loss of input signal will not affect another port. When set to PERCOLATE, a loss of signal will turn off the transmitter of the other port.
sfp_delta_interval	R/W	This enables and defines the interval in which the optical receive power level of each SFP/XFP is read and compared to previous value.
sfp_delta_threshold	R/W	This defines how much the optical receive power level can differ between successive reads before a warning trap is generated.
t4g_config[12].		This table is used to define any T4G or OFC-4 modules in the system.

t4g_port_1_2_datarate	R/W	The CXG relies on the features of the XFP to define its data rate. Since various XFP offer different rates with the same settings, only a general setting is provided. Both ports must operate at the same rate.
t4g_port_3_4_datarate	R/W	Tunable laser are supported. Select the wavelength from the supplied 100GHZ ITU-T grid. If the wavelength is not supported by the XFP, a warning event will be received.
t4g_operation_mode	R/W	This parameter defines the data path through the module when an internal cross connect is available. It is also used to setup a permanent bit error rate test. (most settings apply to X2G, TXG, OFX-3, XCM-2 only)
deactivate_port_1	R/W	When enabled, the optical interface is disabled and communication is cut.
deactivate_port_2	R/W	When enabled, the optical interface is disabled and communication is cut.
deactivate_port_3	R/W	When enabled, the optical interface is disabled and communication is cut.
deactivate_port_4	R/W	When enabled, the optical interface is disabled and communication is cut.
front_panel_mode	R/W	Determines what is displayed on the front panel, when available. Also controls the modules local buttons.
loss_of_signal_handling	R/W	When set to LOCAL a loss of input signal will not affect another port. When set to PERCOLATE, a loss of signal will turn off the transmitter of the other port.
bert_pattern	R/W	Defines the bit pattern with which the build-in bit error rate tester (BERT) operates when cross connect is set to BERT.
sfp_delta_interval	R/W	This enables and defines the interval in which the optical receive power level of each SFP/XFP is read and compared to previous value.
sfp_delta_threshold	R/W	This defines how much the optical receive power level can differ between successive reads before a warning trap is generated.
m2g_config[12].		This table is used to define any M2G or TDM-2 modules in the system.
channel_1_datarate	R/W	Devices the data rate of the first TDM channel (port 1)
channel_2_datarate	R/W	Devices the data rate of the second TDM channel (port 2)
port_1_copper_sfp	R/W	Set when local copper RJ45 SFP is used and connection cannot be established.

port_2_copper_sfp	R/W	Set when local copper RJ45 SFP is used and connection cannot be established.
sfp_delta_interval	R/W	This enables and defines the interval in which the optical receive power level of each SFP/XFP is read and compared to previous value.
sfp_delta_threshold	R/W	This defines how much the optical receive power level can differ between successive reads before a warning trap is generated.
link_backup_trigger	R/W	Defines under which optical signal condition an automated backup is initiated.
stay_with_last_link	R/W	When set the backup switch remains in last position even when signal returns. Still the backup warning turns off after the delay set under backup_end parameter expires.
backup_end	R/W	Defines how long the signal must remain steady before proper operation is assumed and the backup is terminated.
permit_link_override	R/W	Permits the manual selection of a failed link using the link selection. Defaults to false to safeguard against accidental link selection which would result in loss of connection.
om1_config[12].		
wavelength_port_a	R/W	Defines which wavelength band is measured. Use 1550 setting when a WDM link is measured.
low_threshold_port_a	R/W	Defines the lower optical signal level in dBm. A signal level below this threshold will trigger an event.
high_threshold_port_a	R/W	Defines the upper optical signal level in dBm. A signal level above this threshold will trigger an event.
wavelength_port_b	R/W	Defines which wavelength band is measured. Use 1550 setting when a WDM link is measured.
low_threshold_port_b	R/W	Defines the lower optical signal level in dBm. A signal level below this threshold will trigger an event.
high_threshold_port_b	R/W	Defines the upper optical signal level in dBm. A signal level above this threshold will trigger an event.
front_panel_mode	R/W	Determines what is displayed on the front panel, when available. Also controls the modules local buttons.
lp1_config[12].		
wavelength_port_a	R/W	Defines which wavelength band is measured. Use 1550 setting when a WDM link is measured.
low_threshold_port_a	R/W	Defines the lower optical signal level in dBm. A signal level below this threshold will trigger an event and a backup when configured.

high_threshold_port_a	R/W	Defines the upper optical signal level in dBm. A signal level above this threshold will trigger an event and a backup when configured.
wavelength_port_b	R/W	Defines which wavelength band is measured. Use 1550 setting when a WDM link is measured.
low_threshold_port_b	R/W	Defines the lower optical signal level in dBm. A signal level below this threshold will trigger an event and a backup when configured.
high_threshold_port_b	R/W	Defines the upper optical signal level in dBm. A signal level above this threshold will trigger an event and a backup when configured.
backup_criteria	R/W	Defines under which optical signal condition an automated backup is initiated.
stay_with_last_link	R/W	When set the backup switch remains in last position even when signal return. Still the backup warning turns off after the delay set under backup_end parameter expires.
backup_end	R/W	Defines how long the signal must remain steady before proper operation is assumed and the backup is terminated.
front_panel_mode	R/W	Determines what is displayed on the front panel, when available. Also controls the modules local buttons.
em_config[12].		Configuration for EDFA amplifier modules EM2 and EM3.
edfa_operation_mode	R/W	Defines which wavelength band is measured. Use 1550 setting when a WDM link is measured.
loss_of_signal_handling	R/W	Defines if loss of input signal turns off the EDFA pump (PERCOLATE) or not (LOCAL)
signal_gain	R/W	Desired signal gain in dB.
max_output_power	R/W	Maximum output power permitted to exit the module.
low_threshold_edfa_in	R/W	This corresponds to the unamplified input signal before entering the EDFA section. Defines the lower optical signal level in dBm. A signal level below this threshold will trigger an event.
high_threshold_edfa_in	R/W	This corresponds to the unamplified input signal before entering the EDFA section. Defines the upper optical signal level in dBm. A signal level above this threshold will trigger an event.
low_threshold_port_b	R/W	Port B is the unamplified return path through the module. Defines the lower optical signal level in dBm. A signal level below this threshold will trigger an event.

high_threshold_port_b	R/W	Port B is the unamplified return path through the module. Defines the upper optical signal level in dBm. A signal level above this threshold will trigger an event.
front_panel_mode	R/W	Determines what is displayed on the front panel, when available. Also controls the modules local buttons.
module_control[12].		
enter_password	X	This command will set the module password. Only required when the nms_operation_mode is set to passive mode. Enter the password before configuration or actions can be accepted by the module.
reboot_module	X	This command will restart the module. All communication will be disrupted! Syntax: reboot_module = CONFIRM.
warm_start	X	This command will warm start the module. Communication shall not be disrupted. (Firmware dependent) Syntax: warm_start = CONFIRM.
clear_counter	X	This command will clear all module and port related statistics counter.
switch_off_backup	X	For a module that supports backup and which currently is in backup condition this command will revert to normal operation. If this would disrupt traffic a warning is returned and nothing is executed. To override this warning and switch back nonetheless type switch_off_backup = CONFIRM
switch_to_backup	X	For a module that supports backup this command will switch to the backup link. If this would disrupt traffic because backup link is not available a warning is returned and nothing is executed. To override this warning and switch over nonetheless type switch_to_backup = CONFIRM
automatic_backup	X	This command returns a manually overridden backup module to normal automatic mode. No parameter are required.
write_display	X	Writes to the front panel display of the module. Only for modules that offer a front panel display.
led_test	X	This will start the modules LED test and will return the LED back up automatic mode after a few seconds. May be also be used to identify a certain module.
loop_off	X	Turns all loops off
loop_port_1	X	Tries to engage a loop at port 1. Note not all modules support loops. View port status to check success.
loop_port_2	X	Tries to engage a loop at port 2. Note not all modules support loops. View port status to check success.

loop_port_3	X	Tries to engage a loop at port 3. Note not all modules support loops. View port status to check success.
loop_port_4	X	Tries to engage a loop at port 4. Note not all modules support loops. View port status to check success.
bert_restart	X	Resynchronizes BERT. Only has an effect if a BERT is available on the module and configured to be active.
bert_insert_error	X	Inserts an error in the data pattern. This can be used to confirm that a BERT is actually operating. Only has an effect if a BERT is available on the module and configured to be active.
bert_clear_counter	X	Clears the BERT counter. Only has an effect if a BERT is available on the module and configured to be active.
system_status.		
any_error_condition	R	True when any error condition is currently present in any module.
any_test_mode	R	True when any module is in loopback test or has a backup engaged.
any_spare_part	R	True when any module is marked as spare part.
used_node_id	R	Actually used node id as discovered from device
local_rack	R	Indicates in which rack the management module over which this information is retrieved is inserted.
local_slot	R	Indicates in which slot the management module over which this information is retrieved is inserted.
module_inventory[12].		
expected_module	R	Name of module configured for this slot.
module	R	Name of module actually discovered in this slot. This name should be equal to the above name otherwise configuration may not apply properly.
type	R	General functional type of module inserted.
board_code	R	Internal code of actually inserted module.
additional_info	R	Additional information that may be saved in some modules during production.
serial_number	R	Serial number as stored within the hardware.
occupied_slots	R	Number of slots taken by this module. Usually 1.
project_number	R	Internal hardware project number
build_version	R	Precise build code for hardware version tracking.
production_date	R	Production data of the module

mfg_test_info	R	Internal information for quality management. Manufacturing Site / Test Site / Test Person
number_of_optical_ports	R	Indicates the number of actively monitored optical ports of this type of module.
number_of_sfp_ports	R	Indicates the number of optical SFP or SFP+ ports of this type of module.
number_of_xfp_ports	R	Indicates the number of optical XFP ports of this type of module.
core_firmware_version	R	Core operating system software version.
core_firmware_date	R	Core operating system software creation date.
appl_firmware_version	R	Application software version.
appl_firmware_date	R	Application software creation date.
module_status[12].		This table holds a record for each module in the system. Note that not all modules deliver every kind of status.
module	R	Name of module actually discovered in this slot.
system_ok	R	True when the module has booted and appears ok.
error_condition	R	True when any error condition is currently present.
test_mode	R	True when module is in loopback test or a backup is engaged.
spare_part	R	True when module is marked as spare part.
uptime	R	Uptime since last reboot in seconds.
time_since_counter_reset	R	How long ago have the statistics counter been restarted.
temperature	R	Temperature value in centigrade.
too_hot	R	True when module is running too hot.
backup_state	R	Indicates if a backup is active and in which state.
backup_counter	R	Counts the number of times this module has initiated a backup (if backup feature is available for this module type).
backup_duration	R	How long the backup has been activated in total since last value reset.
port_status[48].		This table holds a record for each optical port of the system. Note that not all modules deliver every kind of statistic.
module	R	Name of module in which this port is present.
location	R	Textual description of port location.
snmp_port	R	Slot and port representation as used in SNMP. Formula is Slot*10000 + Port*10.

alias	R	Configured alias nickname of this port.
admin_status	R	Reflects the administrative setting of this port.
oper_status	R	Indicates the combined operation port status.
detailed_status	R	Indicates detailed issues related to the port.
port_datarate	R	Reflects the data rate setting of this port.
update_time_stamp	R	Indicates the time when this record was last updated.
time_since_value_reset	R	Time since when the following statistics have been accumulated. They restart upon module power up or on forced value reset.
time_since_last_error	R	Time since last input signal loss or input signal too high.
time_signal_too_low	R	Total time the input signal was below threshold.
signal_too_low_counter	R	Number of times a transition to signal too low has occurred.
time_signal_too_high	R	Total time the input signal was above high threshold.
signal_too_high_counter	R	Number of times a transition to signal too high has occurred.
low_threshold	R	Defined signal too low threshold.
current_input_signal	R	Actual current signal level.
high_threshold	R	Defined signal too high threshold.
em_status[12].		Optical amplifier status
system_ok	R	True when no errors are present
errors	R	Indicates various optical error conditions.
hardware_code	R	Details codes about the installed hardware components.
time_since_power_error	R	How long ago since the last time the output power was in error condition.
time_with_power_loss	R	Accumulated time the output power has been down.
input_signal_low_counter	R	Number of times a loss of signal has occurred.
input_power	R	Optical input power of port A.
signal_gain	R	Indicates how strong the input signal is amplified.
optimal_flat_gain	R	Indicates the best gain setting for an even amplification across the wavelength channels
back_reflection	R	The value should be low and indicates cable issues if not.
signal_output_power	R	Indicated the actually achieved optical signal output power.
total_output_power	R	Indicated the actually achieved optical output power leaving the module (including noise).

min_output_power	R	Indicates the minimum optical output level that must be send out
max_output_power	R	Indicates the maximum optical output level that can be send out
cfg_output_power	R	Indicated the desired configured optical output power
bert_status[12].		Displays the results of the bit error rate tester (BERT) if it is present and enabled in a slot
location	R	Textual description of BERT port location.
bert_operation	R	Indicates the general bit error rate tester operational status.
total_errors	R	Number of errored bits. Only valid when BERT is synchronized.
time_since_last_error	R	Seconds elapsed since the last error was detected.
total_test_time	R	Accumulated time how long the test was run since last value clear.
errored_time	R	Accumulated seconds in which at least on errored bit was detected.
bit_error_rate	R	Averaged bit error rate during test interval.
ber_since_last_error	R	Bit error rate since last error.
theoretical_ber	R	Theoretical best possible error rate in the given time frame of the current test interval.
availability	R	Relation of transmitted vs. Errored bits.

22.4 MSP1000 Configuration Parameters

Group	slot_config , for all module slots[0..11]
Path	Device.MSP1000.slot_config[slot]
Description	

module

Defines which module is expected to be placed in this slot. This should be identical to the actual hardware. The value may be set prior to actual roll-out to preconfigure the system.

Values	<i>UNDEFINED</i>	Undefined setting. Please select proper module type
	<i>EMPTY</i>	This slot is not used
	<i>LEGACY</i>	Module is too old to be supported by this software
	<i>PASSIVE</i>	A passive filter module is inserted which is not manageable
	<i>X2G</i>	Universal double transponder with cross connect for up to 2.7G (legacy name OFX-3)
	<i>TXG</i>	Precision 10G XFP transponder with FEC data rates and BERT (legacy name XCM-2)
	<i>CXG_</i>	8G/10G XFP transponder (legacy name XCM-3)
	<i>T4G</i>	SAN optimized double transponder up to 4G (legacy name OFC-4)
	<i>EM2</i>	EDFA optical amplifier (legacy name OAM-2)
	<i>EM3</i>	EDFA optical amplifier (legacy name OAM-3)
	<i>OM1</i>	Precise optical power measurement for 2 channel (legacy name OPM-2)
	<i>LP1</i>	Optical line protection switch with power level measurement (legacy name BXM-2)
	<i>OS1</i>	Optical switch controlled via management
	<i>M2G</i>	Dual Gigabit multiplexer with 2.5G link and optional backup (legacy name TDM-2)
	<i>CXGP</i>	8G/10G/16G SFP+ dual transponder (legacy name OFC-10)
	<i>NM1</i>	Network Management Module (legacy name NMS-3)
	<i>NM2</i>	Network Management Module with 2 SFP ports (legacy name NMS-4)
	<i>NM3_</i>	Network Management Module with switch and 2 SFP ports (legacy name NMS-6)
	<i>NM3P</i>	Network Management Module with switch, 2 SFP ports and IO signals (legacy name NMS-7)
	<i>XCM1</i>	10G XFP transponder (legacy name XCM-1)
	<i>TDM4</i>	4x100M/ESCON time division multiplexer (legacy name TDM-4)
	<i>WCM2</i>	DWDM high performance transponder up to 2.7G (not support by this system)
	<i>FC8_FILTER</i>	CWDM passive filter, 8 ports, 1470-1610nm
	<i>FC8A_FILTER</i>	CWDM passive filter, 8 ports, 1270-1430nm
	<i>FC8X_FILTER</i>	CWDM passive filter, 8 ports, 1470-1610nm, extension port
	<i>B4S_FILTER</i>	DWDM passive band filter, lower 4 bands, extension port
	<i>B4X_FILTER</i>	DWDM passive band filter, upper 4 bands
	<i>B8M_FILTER</i>	DWDM passive band filter, 8 bands, multiplexer
	<i>B8D_FILTER</i>	DWDM passive band filter, 8 bands, demultiplexer
	<i>FD4_FILTER</i>	DWDM passive filter, 4 ports, 100 GHz grid
	<i>DC1_FILTER</i>	Passive dispersion compensation module
	<i>SE1</i>	Shelf Expansion module (passive, only in slot 1)
OID	1.3.6.1.4.1.3181.10.6.1.94.2.1.2 (slotConfigModule)	

sparepart_mode	<p>When enabled the module is operating normally but will not generate any alarms. This is useful for modules that are inserted but only used as spare and are not properly connected at this time. This way unnecessary alarms are avoided.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.2.1.3 (slotConfigSparepartMode)</p>
port_1_alias	<p>User defined port name for easier reference.</p> <p>Value String, max. 15 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.2.1.4 (slotConfigPort1Alias)</p>
port_2_alias	<p>User defined port name for easier reference.</p> <p>Value String, max. 15 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.2.1.5 (slotConfigPort2Alias)</p>
port_3_alias	<p>User defined port name for easier reference.</p> <p>Value String, max. 15 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.2.1.6 (slotConfigPort3Alias)</p>
port_4_alias	<p>User defined port name for easier reference.</p> <p>Value String, max. 15 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.2.1.7 (slotConfigPort4Alias)</p>
Group Path Description	<p>x2g_config, for all module slots[0..11]</p> <p>Device.MSP1000.x2g_config[slot]</p> <p>This table is used to define any X2G or OFX-3 modules in the system.</p>

port_1_datarate

This parameter defines the data rate used to setup the internal retimer to provide 3R regeneration. Note that internally interconnected ports must be set to the same rate.

Values	<i>TRANSPARENT</i>	Transparent. No clock recovery is used
	<i>100M_ETH</i>	Port speed 125 Mbps (Fast Ethernet)
	<i>1G_ETH</i>	Port speed 1250 Mbps (Gigabit Ethernet)
	<i>1X_FC</i>	Port speed 1062 Mbps (1G Fibre Channel)
	<i>2X_FC</i>	Port speed 2125 Mbps (2G Fibre Channel)
	<i>OC_3</i>	Port speed 155 Mbps (OC-3 / STM-1)
	<i>OC_12</i>	Port speed 622 Mbps (OC-12 / STM-4)
	<i>OC_48</i>	Port speed 2048 Mbps (OC-48 / STM-16)
	<i>OTU1</i>	Port speed 2.67G, FEC RS 255/238, STS48/STM-16 (X2G, OFX-3 only)
	<i>FIX100</i>	Port speed 100M, (special)
	<i>ESCON</i>	Port speed 200M, (ESCON)
	<i>SDI</i>	Port speed 270M, (SDI)
	<i>HDTV</i>	Port speed 1450M, (HDTV)
	<i>M2G</i>	Port speed 2550M, to repeat M2G or TDM4
OID	1.3.6.1.4.1.3181.10.6.1.94.3.1.2 (x2gConfigPort1Datarate)	

port_2_datarate

This parameter defines the data rate used to setup the internal retimer to provide 3R regeneration. Note that internally interconnected ports must be set to the same rate.

Values	<i>TRANSPARENT</i>	Transparent. No clock recovery is used
	<i>100M_ETH</i>	Port speed 125 Mbps (Fast Ethernet)
	<i>1G_ETH</i>	Port speed 1250 Mbps (Gigabit Ethernet)
	<i>1X_FC</i>	Port speed 1062 Mbps (1G Fibre Channel)
	<i>2X_FC</i>	Port speed 2125 Mbps (2G Fibre Channel)
	<i>OC_3</i>	Port speed 155 Mbps (OC-3 / STM-1)
	<i>OC_12</i>	Port speed 622 Mbps (OC-12 / STM-4)
	<i>OC_48</i>	Port speed 2048 Mbps (OC-48 / STM-16)
	<i>OTU1</i>	Port speed 2.67G, FEC RS 255/238, STS48/STM-16 (X2G, OFX-3 only)
	<i>FIX100</i>	Port speed 100M, (special)
	<i>ESCON</i>	Port speed 200M, (ESCON)
	<i>SDI</i>	Port speed 270M, (SDI)
	<i>HDTV</i>	Port speed 1450M, (HDTV)
	<i>M2G</i>	Port speed 2550M, to repeat M2G or TDM4
OID	1.3.6.1.4.1.3181.10.6.1.94.3.1.3 (x2gConfigPort2Datarate)	

port_3_datarate

This parameter defines the data rate used to setup the internal retimer to provide 3R regeneration. Note that internally interconnected ports must be set to the same rate.

Values	<i>TRANSPARENT</i>	Transparent. No clock recovery is used
	<i>100M_ETH</i>	Port speed 125 Mbps (Fast Ethernet)
	<i>1G_ETH</i>	Port speed 1250 Mbps (Gigabit Ethernet)
	<i>1X_FC</i>	Port speed 1062 Mbps (1G Fibre Channel)
	<i>2X_FC</i>	Port speed 2125 Mbps (2G Fibre Channel)
	<i>OC_3</i>	Port speed 155 Mbps (OC-3 / STM-1)
	<i>OC_12</i>	Port speed 622 Mbps (OC-12 / STM-4)
	<i>OC_48</i>	Port speed 2048 Mbps (OC-48 / STM-16)
	<i>OTU1</i>	Port speed 2.67G, FEC RS 255/238, STS48/STM-16 (X2G, OFX-3 only)
	<i>FIX100</i>	Port speed 100M, (special)
	<i>ESCON</i>	Port speed 200M, (ESCON)
	<i>SDI</i>	Port speed 270M, (SDI)
	<i>HDTV</i>	Port speed 1450M, (HDTV)
	<i>M2G</i>	Port speed 2550M, to repeat M2G or TDM4
OID	1.3.6.1.4.1.3181.10.6.1.94.3.1.4 (x2gConfigPort3Datarate)	

port_4_datarate

This parameter defines the data rate used to setup the internal retimer to provide 3R regeneration. Note that internally interconnected ports must be set to the same rate.

Values	<i>TRANSPARENT</i>	Transparent. No clock recovery is used
	<i>100M_ETH</i>	Port speed 125 Mbps (Fast Ethernet)
	<i>1G_ETH</i>	Port speed 1250 Mbps (Gigabit Ethernet)
	<i>1X_FC</i>	Port speed 1062 Mbps (1G Fibre Channel)
	<i>2X_FC</i>	Port speed 2125 Mbps (2G Fibre Channel)
	<i>OC_3</i>	Port speed 155 Mbps (OC-3 / STM-1)
	<i>OC_12</i>	Port speed 622 Mbps (OC-12 / STM-4)
	<i>OC_48</i>	Port speed 2048 Mbps (OC-48 / STM-16)
	<i>OTU1</i>	Port speed 2.67G, FEC RS 255/238, STS48/STM-16 (X2G, OFX-3 only)
	<i>FIX100</i>	Port speed 100M, (special)
	<i>ESCON</i>	Port speed 200M, (ESCON)
	<i>SDI</i>	Port speed 270M, (SDI)
	<i>HDTV</i>	Port speed 1450M, (HDTV)
	<i>M2G</i>	Port speed 2550M, to repeat M2G or TDM4
OID	1.3.6.1.4.1.3181.10.6.1.94.3.1.5 (x2gConfigPort4Datarate)	

cross_connect	This parameter defines the data path through the module. It is also used to setup a permanent bit error rate test.	
	Values	
	<i>DISCONNECT</i>	All ports are disconnected
	<i>NORMAL</i>	Default Converter setting. P1-P2 and P3-P4
	<i>ALTERNATE</i>	Converter I P1-P3 and P2-P4
	<i>BACKUP</i>	Point to Point Backup. Normal: P1-P3, Backup: P1-P4
	<i>RING_BACKUP_WEST</i>	Ring Backup West. Normal: P1-P3, Backup: P1-P4 (X2G, OFX-3 only)
	<i>RING_BACKUP_EAST</i>	Ring Backup East. Normal: P1-P4, Backup: P1-P3 (X2G, OFX-3 only)
	<i>MULTICAST</i>	Multicast Rx of P1 is copied to P2, P3, P4 (X2G, OFX-3 only)
	<i>DROP_CONTINUE</i>	P3-P4 plus Rx of P3 is copied to P1, Rx of P4 copy is copied to P2 (X2G, OFX-3 only)
	<i>ADD_DROP_WEST</i>	Add/Drop West. P1-P3 and P3-P4 (X2G, OFX-3 only)
	<i>ADD_DROP_EAST</i>	Add/Drop East. P1-P4 and P2-P3 (X2G, OFX-3 only)
	<i>CROSS_OVER</i>	Cross Over. P1-P4 and P2-P3 (X2G, OFX-3 only)
	<i>SWITCH_P1_P2</i>	Connection P1-P2. Other ports disconnected
	<i>SWITCH_P1_P3</i>	Connection P1-P3. Other ports disconnected
	<i>SWITCH_P1_P4</i>	Connection P1-P4. Other ports disconnected
	<i>BERT_PORT_4</i>	Bit Error Rate Test on P4 (X2G, OFX-3 only)
	OID	1.3.6.1.4.1.3181.10.6.1.94.3.1.6 (x2gConfigCrossConnect)
deactivate_port_1	When enabled, the optical interface is disabled and communication is cut.	
	Values	enabled, disabled
	OID	1.3.6.1.4.1.3181.10.6.1.94.3.1.7 (x2gConfigDeactivatePort1)
deactivate_port_2	When enabled, the optical interface is disabled and communication is cut.	
	Values	enabled, disabled
	OID	1.3.6.1.4.1.3181.10.6.1.94.3.1.8 (x2gConfigDeactivatePort2)
deactivate_port_3	When enabled, the optical interface is disabled and communication is cut.	
	Values	enabled, disabled
	OID	1.3.6.1.4.1.3181.10.6.1.94.3.1.9 (x2gConfigDeactivatePort3)
deactivate_port_4	When enabled, the optical interface is disabled and communication is cut.	
	Values	enabled, disabled
	OID	1.3.6.1.4.1.3181.10.6.1.94.3.1.10 (x2gConfigDeactivatePort4)

front_panel_mode	Determines what is displayed on the front panel, when available. Also controls the modules local buttons.	
Values	<i>NORMAL</i>	Displays module name and error conditions
	<i>EXTENDED</i>	Cyclical shows various system information and error conditions
	<i>NORMAL_LOCKED</i>	Like NORMAL but the module buttons are disabled
	<i>EXTENDED_LOCKED</i>	Like EXTENDED but the module buttons are disabled
	<i>REMOTE</i>	Display is not updated and can be controlled from remote management system
OID	1.3.6.1.4.1.3181.10.6.1.94.3.1.11 (x2gConfigFrontPanelMode)	
loss_of_signal_handling	When set to LOCAL a loss of input signal will not affect another port. When set to PERCOLATE, a loss of signal will turn off the transmitter of the currently associated port.	
Values	<i>LOCAL</i>	Laser is always turned on when port is enabled
	<i>PERCOLATE</i>	Laser is turned off when receiver of associated port is down
OID	1.3.6.1.4.1.3181.10.6.1.94.3.1.12 (x2gConfigLossOfSignalHandling)	
optimized_for_8b10b	Enable this feature when Ethernet or FibreChannel is used. Do not set when SDH is used on any port.	
Values	enabled, disabled	
OID	1.3.6.1.4.1.3181.10.6.1.94.3.1.13 (x2gConfigOptimizedFor8b10b)	
bert_pattern	Defines the bit pattern with which the build-in bit error rate tester (BERT) operates when cross connect is set to BERT.	
Values	<i>2_7</i>	BERT pattern which repeats every 2 ⁷ bits is used
	<i>2_23</i>	BERT pattern which repeats every 2 ²³ bits is used
	<i>2_31</i>	BERT pattern which repeats every 2 ³¹ bits is used
	<i>CJ_PAT</i>	BERT pattern for 8B10 code testing (X2G, OFX-3 only)
	<i>CR_PAT</i>	BERT pattern for 8B10 code testing (X2G, OFX-3 only)
	<i>8B_10B_CNT</i>	BERT pattern for 8B10 code testing (X2G, OFX-3 only)
OID	1.3.6.1.4.1.3181.10.6.1.94.3.1.14 (x2gConfigBertPattern)	

sfp_delta_interval

This enables and defines the interval in which the optical receive power level of each SFP is read and compared to previous value.

Values

<i>DISABLED</i>	Optical receiver power delta detection is disabled
<i>1_SEC</i>	Optical receive power is compared every second
<i>5_SEC</i>	Optical receive power is compared every 5 seconds
<i>10_SEC</i>	Optical receive power is compared every 10 seconds
<i>30_SEC</i>	Optical receive power is compared every 30 seconds
<i>60_SEC</i>	Optical receive power is compared every minute
<i>240_SEC</i>	Optical receive power is compared every 4 minutes

OID

1.3.6.1.4.1.3181.10.6.1.94.3.1.15 (x2gConfigSfpDeltaInterval)

sfp_delta_threshold

This defines how much the optical receive power level can differ between successive reads before a warning trap is generated.

Values

<i>0_5_DB</i>	An event is generated if power level varies more than half a dB
<i>1_DB</i>	An event is generated if power level varies more than 1 dB
<i>1_5_DB</i>	An event is generated if power level varies more than 1.5 dB
<i>2_DB</i>	An event is generated if power level varies more than 2 dB
<i>3_DB</i>	An event is generated if power level varies more than 3 dB
<i>5_DB</i>	An event is generated if power level varies more than 5 dB

OID

1.3.6.1.4.1.3181.10.6.1.94.3.1.16 (x2gConfigSfpDeltaThreshold)

backup_trigger

Defines under which optical signal condition an automated backup is initiated.

Values

<i>DISABLED</i>	Automatic backup function is disabled. Manual switching is possible
<i>SIGNAL_LOSS</i>	Backup is controlled by loss of optical signal as indicated by SFP
<i>CLOCK_LOSS</i>	Backup is controlled by loss of clock synchronization of retimer

OID

1.3.6.1.4.1.3181.10.6.1.94.3.1.17 (x2gConfigBackupTrigger)

stay_with_last_link

When set the backup switch remains in last position even when signal returns. Still the backup warning turns off after the delay set under backup_end parameter expires.

Values

enabled, disabled

OID

1.3.6.1.4.1.3181.10.6.1.94.3.1.18 (x2gConfigStayWithLastLink)

backup_end	<p>Defines how long the signal must remain steady before proper operation is assumed and the backup is terminated.</p> <p>Values</p> <p><i>NO_DELAY</i> Immediately switch off backup when missing signal returns</p> <p><i>15_SECONDS</i> When missing signal returns wait for 15 seconds during which no further signal loss must occur. Only then switch off the backup path</p> <p><i>15_MINUTES</i> When missing signal returns wait for 15 minutes during which no further signal loss must occur. Only then switch off the backup path</p> <p><i>MANUALLY</i> Do not switchback automatically. Use action command to switch off backup</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.3.1.19 (x2gConfigBackupEnd)</p>
permit_link_override	<p>Permits the manual selection of a failed link using the link selection. Defaults to false to safeguard against accidental link selection which would result in loss of connection.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.3.1.20 (x2gConfigPermitLinkOverride)</p>
<p>Group</p> <p>Path</p> <p>Description</p>	<p>txg_config, for all module slots[0..11]</p> <p>Device.MSP1000.txg_config[slot]</p> <p>This table is used to define any TXG or XCM-2 modules in the system.</p>
txg_datarate	<p>This parameter defines the data rate used to setup the internal retimer to provide 3R regeneration. Note that internally interconnected ports must be set to the same rate.</p> <p>Values</p> <p><i>OC_192</i> Port speed 9953 Mbps (OC-192 / STM-64)</p> <p><i>OC_192_FEC</i> Port speed 10660 Mbps (OC192 plus FEC)</p> <p><i>10G_ETH</i> Port speed 10300 Mbps (10G Ethernet)</p> <p><i>10X_FC</i> Port speed 10530 Mbps (10G Fibre Channel)</p> <p><i>OTU2</i> Port speed 10709 MB, FEC RS 255/237, STS-192/STM-64</p> <p><i>OTU_1F</i> Port speed 11270 MB, FEC RS 255/238, 10G FC over OTN</p> <p><i>OTU_2E</i> Port speed 11096 MB, FEC RS 255/237, 10G Eth over OTN</p> <p><i>OTU_2F</i> Port speed 11318 MB, FEC RS 255/237, 10G FC over OTN</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.4.1.2 (txgConfigTxgDatarate)</p>

txg_operation_mode	This parameter defines the data path through the module when an internal cross connect is available. It is also used to setup a permanent bit error rate test. (most settings apply to X2G, TXG, OFX-3, XCM-2 only)	
Values	<i>DISABLED</i>	Both XFP ports are disabled
	<i>TRANSPONDER</i>	Received clock is recovered and then used for transmitter
	<i>REPEATER</i>	Received clock is recovered and specially cleaned and then used for transmitter
	<i>BERT_PORT_1</i>	BERT is operational port 1. Port 2 is unused
	<i>BERT_PORT_2</i>	BERT is operational port 2. Port 1 is unused
OID	1.3.6.1.4.1.3181.10.6.1.94.4.1.3 (txgConfigTxgOperationMode)	

port_1_itu_channel

Tunable laser are supported. Select the wavelength from the supplied 100GHZ ITU-T grid. If the wavelength is not supported by the XFP, a warning event will be received.

Values	<i>FIXED</i>	Fixed wavelength defined by installed optic
	<i>CH11</i>	ITU channel 11
	<i>CH12</i>	ITU channel 12
	<i>CH13</i>	ITU channel 13
	<i>CH14</i>	ITU channel 14
	<i>CH15</i>	ITU channel 15
	<i>CH16</i>	ITU channel 16
	<i>CH17</i>	ITU channel 17
	<i>CH18</i>	ITU channel 18
	<i>CH19</i>	ITU channel 19
	<i>CH20</i>	ITU channel 20
	<i>CH21</i>	ITU channel 21
	<i>CH22</i>	ITU channel 22
	<i>CH23</i>	ITU channel 23
	<i>CH24</i>	ITU channel 24
	<i>CH25</i>	ITU channel 25
	<i>CH26</i>	ITU channel 26
	<i>CH27</i>	ITU channel 27
	<i>CH28</i>	ITU channel 28
	<i>CH29</i>	ITU channel 29
	<i>CH30</i>	ITU channel 30
	<i>CH31</i>	ITU channel 31
	<i>CH32</i>	ITU channel 32
	<i>CH33</i>	ITU channel 33
	<i>CH34</i>	ITU channel 34
	<i>CH35</i>	ITU channel 35
	<i>CH36</i>	ITU channel 36
	<i>CH37</i>	ITU channel 37
	<i>CH38</i>	ITU channel 38
	<i>CH39</i>	ITU channel 39
	<i>CH40</i>	ITU channel 40
	<i>CH41</i>	ITU channel 41
	<i>CH42</i>	ITU channel 42
	<i>CH43</i>	ITU channel 43
	<i>CH44</i>	ITU channel 44
	<i>CH45</i>	ITU channel 45
	<i>CH46</i>	ITU channel 46
	<i>CH47</i>	ITU channel 47
	<i>CH48</i>	ITU channel 48
	<i>CH49</i>	ITU channel 49
	<i>CH50</i>	ITU channel 50
	<i>CH51</i>	ITU channel 51
	<i>CH52</i>	ITU channel 52
	<i>CH53</i>	ITU channel 53
	<i>CH54</i>	ITU channel 54
	<i>CH55</i>	ITU channel 55
	<i>CH56</i>	ITU channel 56

CH57 ITU channel 57

CH58 ITU channel 58

CH59 ITU channel 59

CH60 ITU channel 60

CH61 ITU channel 61

CH62 ITU channel 62

CH63 ITU channel 63

OID

1.3.6.1.4.1.3181.10.6.1.94.4.1.4 (txgConfigPort1ItuChannel)

port_2_itu_channel

Tunable laser are supported. Select the wavelength from the supplied 100GHZ ITU-T grid. If the wavelength is not supported by the XFP, a warning event will be received.

Values	<i>FIXED</i>	Fixed wavelength defined by installed optic
	<i>CH11</i>	ITU channel 11
	<i>CH12</i>	ITU channel 12
	<i>CH13</i>	ITU channel 13
	<i>CH14</i>	ITU channel 14
	<i>CH15</i>	ITU channel 15
	<i>CH16</i>	ITU channel 16
	<i>CH17</i>	ITU channel 17
	<i>CH18</i>	ITU channel 18
	<i>CH19</i>	ITU channel 19
	<i>CH20</i>	ITU channel 20
	<i>CH21</i>	ITU channel 21
	<i>CH22</i>	ITU channel 22
	<i>CH23</i>	ITU channel 23
	<i>CH24</i>	ITU channel 24
	<i>CH25</i>	ITU channel 25
	<i>CH26</i>	ITU channel 26
	<i>CH27</i>	ITU channel 27
	<i>CH28</i>	ITU channel 28
	<i>CH29</i>	ITU channel 29
	<i>CH30</i>	ITU channel 30
	<i>CH31</i>	ITU channel 31
	<i>CH32</i>	ITU channel 32
	<i>CH33</i>	ITU channel 33
	<i>CH34</i>	ITU channel 34
	<i>CH35</i>	ITU channel 35
	<i>CH36</i>	ITU channel 36
	<i>CH37</i>	ITU channel 37
	<i>CH38</i>	ITU channel 38
	<i>CH39</i>	ITU channel 39
	<i>CH40</i>	ITU channel 40
	<i>CH41</i>	ITU channel 41
	<i>CH42</i>	ITU channel 42
	<i>CH43</i>	ITU channel 43
	<i>CH44</i>	ITU channel 44
	<i>CH45</i>	ITU channel 45
	<i>CH46</i>	ITU channel 46
	<i>CH47</i>	ITU channel 47
	<i>CH48</i>	ITU channel 48
	<i>CH49</i>	ITU channel 49
	<i>CH50</i>	ITU channel 50
	<i>CH51</i>	ITU channel 51
	<i>CH52</i>	ITU channel 52
	<i>CH53</i>	ITU channel 53
	<i>CH54</i>	ITU channel 54
	<i>CH55</i>	ITU channel 55
	<i>CH56</i>	ITU channel 56

		<i>CH57</i>	ITU channel 57
		<i>CH58</i>	ITU channel 58
		<i>CH59</i>	ITU channel 59
		<i>CH60</i>	ITU channel 60
		<i>CH61</i>	ITU channel 61
		<i>CH62</i>	ITU channel 62
		<i>CH63</i>	ITU channel 63
	OID	1.3.6.1.4.1.3181.10.6.1.94.4.1.5 (txgConfigPort2ItuChannel)	
<hr/>			
deactivate_port_1	When enabled, the optical interface is disabled and communication is cut.		
	Values	enabled, disabled	
	OID	1.3.6.1.4.1.3181.10.6.1.94.4.1.6 (txgConfigDeactivatePort1)	
<hr/>			
deactivate_port_2	When enabled, the optical interface is disabled and communication is cut.		
	Values	enabled, disabled	
	OID	1.3.6.1.4.1.3181.10.6.1.94.4.1.7 (txgConfigDeactivatePort2)	
<hr/>			
front_panel_mode	Determines what is displayed on the front panel, when available. Also controls the modules local buttons.		
	Values	<i>NORMAL</i>	Displays module name and error conditions
		<i>EXTENDED</i>	Cyclical shows various system information and error conditions
		<i>NORMAL_LOCKED</i>	Like NORMAL but the module buttons are disabled
		<i>EXTENDED_LOCKED</i>	Like EXTENDED but the module buttons are disabled
		<i>REMOTE</i>	Display is not updated and can be controlled from remote management system
	OID	1.3.6.1.4.1.3181.10.6.1.94.4.1.8 (txgConfigFrontPanelMode)	
<hr/>			
loss_of_signal_handling	When set to LOCAL a loss of input signal will not affect another port. When set to PERCOLATE, a loss of signal will turn off the transmitter of the other port.		
	Values	<i>LOCAL</i>	Laser is always turned on when port is enabled
		<i>PERCOLATE</i>	Laser is turned off when receiver of associated port is down
	OID	1.3.6.1.4.1.3181.10.6.1.94.4.1.9 (txgConfigLossOfSignalHandling)	

bert_pattern	Defines the bit pattern with which the build-in bit error rate tester (BERT) operates when cross connect is set to BERT.	
Values	<i>2_7</i>	BERT pattern which repeats every 2 ⁷ bits is used
	<i>2_23</i>	BERT pattern which repeats every 2 ²³ bits is used
	<i>2_31</i>	BERT pattern which repeats every 2 ³¹ bits is used
	<i>CJ_PAT</i>	BERT pattern for 8B10 code testing (X2G, OFX-3 only)
	<i>CR_PAT</i>	BERT pattern for 8B10 code testing (X2G, OFX-3 only)
	<i>8B_10B_CNT</i>	BERT pattern for 8B10 code testing (X2G, OFX-3 only)
OID	1.3.6.1.4.1.3181.10.6.1.94.4.1.10 (txgConfigBertPattern)	
sfp_delta_interval	This enables and defines the interval in which the optical receive power level of each SFP/XFP is read and compared to previous value.	
Values	<i>DISABLED</i>	Optical receiver power delta detection is disabled
	<i>1_SEC</i>	Optical receive power is compared every second
	<i>5_SEC</i>	Optical receive power is compared every 5 seconds
	<i>10_SEC</i>	Optical receive power is compared every 10 seconds
	<i>30_SEC</i>	Optical receive power is compared every 30 seconds
	<i>60_SEC</i>	Optical receive power is compared every minute
	<i>240_SEC</i>	Optical receive power is compared every 4 minutes
OID	1.3.6.1.4.1.3181.10.6.1.94.4.1.11 (txgConfigSfpDeltaInterval)	
sfp_delta_threshold	This defines how much the optical receive power level can differ between successive reads before a warning trap is generated.	
Values	<i>0_5_DB</i>	An event is generated if power level varies more than half a dB
	<i>1_DB</i>	An event is generated if power level varies more than 1 dB
	<i>1_5_DB</i>	An event is generated if power level varies more than 1.5 dB
	<i>2_DB</i>	An event is generated if power level varies more than 2 dB
	<i>3_DB</i>	An event is generated if power level varies more than 3 dB
	<i>5_DB</i>	An event is generated if power level varies more than 5 dB
OID	1.3.6.1.4.1.3181.10.6.1.94.4.1.12 (txgConfigSfpDeltaThreshold)	

Group	cxg_plus_config , for all module slots[0..11]	
Path	Device.MSP1000.cxg_plus_config[slot]	
Description	This table is used to define any CXG+ or OFC-10 modules in the system.	

cxg_port_1_2_datarate	The CXG relies on the features of the XFP to define its data rate. Since various XFP offer different rates with the same settings, only a general setting is provided. Both ports must operate at the same rate.	
Values	<i>TRANSPARENT</i>	No clock recovery is used. May result in bit errors when there is too little optical budget available
	<i>8X_FC</i>	Lower speed SFP+/XFP setting. Usually 8xFC when matching SFP+/XFP are inserted
	<i>10G_ETH</i>	High speed SFP+/XFP setting. Usually 10G when 8G/10G SFP+/XFP are inserted
	<i>10X_FC_16X_FC</i>	Both SFP+XFP control bits are set. Results depend on plugged-in module. May be 10x FibreChannel, 16x FibreChannel or undetermined.
OID	1.3.6.1.4.1.3181.10.6.1.94.5.1.2 (cxgPlusConfigCxgPort12Datarate)	

cxg_port_3_4_datarate	The CXG relies on the features of the XFP to define its data rate. Since various XFP offer different rates with the same settings, only a general setting is provided. Both ports must operate at the same rate.	
Values	<i>TRANSPARENT</i>	No clock recovery is used. May result in bit errors when there is too little optical budget available
	<i>8X_FC</i>	Lower speed SFP+/XFP setting. Usually 8xFC when matching SFP+/XFP are inserted
	<i>10G_ETH</i>	High speed SFP+/XFP setting. Usually 10G when 8G/10G SFP+/XFP are inserted
	<i>10X_FC_16X_FC</i>	Both SFP+XFP control bits are set. Results depend on plugged-in module. May be 10x FibreChannel, 16x FibreChannel or undetermined.
OID	1.3.6.1.4.1.3181.10.6.1.94.5.1.3 (cxgPlusConfigCxgPort34Datarate)	

port_1_itu_channel	Tunable laser are supported. Select the wavelength from the supplied 100GHZ ITU-T grid. If the wavelength is not supported by the XFP, a warning event will be received.
--------------------	--

Values	<i>FIXED</i>	Fixed wavelength defined by installed optic
	<i>CH11</i>	ITU channel 11
	<i>CH12</i>	ITU channel 12
	<i>CH13</i>	ITU channel 13
	<i>CH14</i>	ITU channel 14
	<i>CH15</i>	ITU channel 15
	<i>CH16</i>	ITU channel 16
	<i>CH17</i>	ITU channel 17
	<i>CH18</i>	ITU channel 18
	<i>CH19</i>	ITU channel 19
	<i>CH20</i>	ITU channel 20
	<i>CH21</i>	ITU channel 21
	<i>CH22</i>	ITU channel 22
	<i>CH23</i>	ITU channel 23
	<i>CH24</i>	ITU channel 24
	<i>CH25</i>	ITU channel 25
	<i>CH26</i>	ITU channel 26
	<i>CH27</i>	ITU channel 27
	<i>CH28</i>	ITU channel 28
	<i>CH29</i>	ITU channel 29
	<i>CH30</i>	ITU channel 30
	<i>CH31</i>	ITU channel 31
	<i>CH32</i>	ITU channel 32
	<i>CH33</i>	ITU channel 33
	<i>CH34</i>	ITU channel 34
	<i>CH35</i>	ITU channel 35
	<i>CH36</i>	ITU channel 36
	<i>CH37</i>	ITU channel 37
	<i>CH38</i>	ITU channel 38
	<i>CH39</i>	ITU channel 39
	<i>CH40</i>	ITU channel 40
	<i>CH41</i>	ITU channel 41
	<i>CH42</i>	ITU channel 42
	<i>CH43</i>	ITU channel 43
	<i>CH44</i>	ITU channel 44
	<i>CH45</i>	ITU channel 45
	<i>CH46</i>	ITU channel 46
	<i>CH47</i>	ITU channel 47
	<i>CH48</i>	ITU channel 48
	<i>CH49</i>	ITU channel 49
	<i>CH50</i>	ITU channel 50
	<i>CH51</i>	ITU channel 51
	<i>CH52</i>	ITU channel 52
	<i>CH53</i>	ITU channel 53
	<i>CH54</i>	ITU channel 54
	<i>CH55</i>	ITU channel 55
	<i>CH56</i>	ITU channel 56

CH57 ITU channel 57

CH58 ITU channel 58

CH59 ITU channel 59

CH60 ITU channel 60

CH61 ITU channel 61

CH62 ITU channel 62

CH63 ITU channel 63

OID

1.3.6.1.4.1.3181.10.6.1.94.5.1.4
(cxgPlusConfigPort1ItuChannel)

port_2_itu_channel

Tunable laser are supported. Select the wavelength from the supplied 100GHZ ITU-T grid. If the wavelength is not supported by the XFP, a warning event will be received.

Values	FIXED	Fixed wavelength defined by installed optic
<i>CH11</i>	ITU channel 11	
<i>CH12</i>	ITU channel 12	
<i>CH13</i>	ITU channel 13	
<i>CH14</i>	ITU channel 14	
<i>CH15</i>	ITU channel 15	
<i>CH16</i>	ITU channel 16	
<i>CH17</i>	ITU channel 17	
<i>CH18</i>	ITU channel 18	
<i>CH19</i>	ITU channel 19	
<i>CH20</i>	ITU channel 20	
<i>CH21</i>	ITU channel 21	
<i>CH22</i>	ITU channel 22	
<i>CH23</i>	ITU channel 23	
<i>CH24</i>	ITU channel 24	
<i>CH25</i>	ITU channel 25	
<i>CH26</i>	ITU channel 26	
<i>CH27</i>	ITU channel 27	
<i>CH28</i>	ITU channel 28	
<i>CH29</i>	ITU channel 29	
<i>CH30</i>	ITU channel 30	
<i>CH31</i>	ITU channel 31	
<i>CH32</i>	ITU channel 32	
<i>CH33</i>	ITU channel 33	
<i>CH34</i>	ITU channel 34	
<i>CH35</i>	ITU channel 35	
<i>CH36</i>	ITU channel 36	
<i>CH37</i>	ITU channel 37	
<i>CH38</i>	ITU channel 38	
<i>CH39</i>	ITU channel 39	
<i>CH40</i>	ITU channel 40	
<i>CH41</i>	ITU channel 41	
<i>CH42</i>	ITU channel 42	
<i>CH43</i>	ITU channel 43	
<i>CH44</i>	ITU channel 44	
<i>CH45</i>	ITU channel 45	
<i>CH46</i>	ITU channel 46	
<i>CH47</i>	ITU channel 47	
<i>CH48</i>	ITU channel 48	
<i>CH49</i>	ITU channel 49	
<i>CH50</i>	ITU channel 50	
<i>CH51</i>	ITU channel 51	
<i>CH52</i>	ITU channel 52	
<i>CH53</i>	ITU channel 53	
<i>CH54</i>	ITU channel 54	
<i>CH55</i>	ITU channel 55	
<i>CH56</i>	ITU channel 56	

	<i>CH57</i>	ITU channel 57
	<i>CH58</i>	ITU channel 58
	<i>CH59</i>	ITU channel 59
	<i>CH60</i>	ITU channel 60
	<i>CH61</i>	ITU channel 61
	<i>CH62</i>	ITU channel 62
	<i>CH63</i>	ITU channel 63
OID	1.3.6.1.4.1.3181.10.6.1.94.5.1.5 (cxgPlusConfigPort2ItuChannel)	

port_3_itu_channel

Tunable laser are supported. Select the wavelength from the supplied 100GHZ ITU-T grid. If the wavelength is not supported by the XFP, a warning event will be received.

Values	<i>FIXED</i>	Fixed wavelength defined by installed optic
	<i>CH11</i>	ITU channel 11
	<i>CH12</i>	ITU channel 12
	<i>CH13</i>	ITU channel 13
	<i>CH14</i>	ITU channel 14
	<i>CH15</i>	ITU channel 15
	<i>CH16</i>	ITU channel 16
	<i>CH17</i>	ITU channel 17
	<i>CH18</i>	ITU channel 18
	<i>CH19</i>	ITU channel 19
	<i>CH20</i>	ITU channel 20
	<i>CH21</i>	ITU channel 21
	<i>CH22</i>	ITU channel 22
	<i>CH23</i>	ITU channel 23
	<i>CH24</i>	ITU channel 24
	<i>CH25</i>	ITU channel 25
	<i>CH26</i>	ITU channel 26
	<i>CH27</i>	ITU channel 27
	<i>CH28</i>	ITU channel 28
	<i>CH29</i>	ITU channel 29
	<i>CH30</i>	ITU channel 30
	<i>CH31</i>	ITU channel 31
	<i>CH32</i>	ITU channel 32
	<i>CH33</i>	ITU channel 33
	<i>CH34</i>	ITU channel 34
	<i>CH35</i>	ITU channel 35
	<i>CH36</i>	ITU channel 36
	<i>CH37</i>	ITU channel 37
	<i>CH38</i>	ITU channel 38
	<i>CH39</i>	ITU channel 39
	<i>CH40</i>	ITU channel 40
	<i>CH41</i>	ITU channel 41
	<i>CH42</i>	ITU channel 42
	<i>CH43</i>	ITU channel 43
	<i>CH44</i>	ITU channel 44
	<i>CH45</i>	ITU channel 45
	<i>CH46</i>	ITU channel 46
	<i>CH47</i>	ITU channel 47
	<i>CH48</i>	ITU channel 48
	<i>CH49</i>	ITU channel 49
	<i>CH50</i>	ITU channel 50
	<i>CH51</i>	ITU channel 51
	<i>CH52</i>	ITU channel 52
	<i>CH53</i>	ITU channel 53
	<i>CH54</i>	ITU channel 54
	<i>CH55</i>	ITU channel 55
	<i>CH56</i>	ITU channel 56

CH57 ITU channel 57

CH58 ITU channel 58

CH59 ITU channel 59

CH60 ITU channel 60

CH61 ITU channel 61

CH62 ITU channel 62

CH63 ITU channel 63

OID

1.3.6.1.4.1.3181.10.6.1.94.5.1.6
(cxgPlusConfigPort3ItuChannel)

port_4_itu_channel

Tunable laser are supported. Select the wavelength from the supplied 100GHZ ITU-T grid. If the wavelength is not supported by the XFP, a warning event will be received.

Values	<i>FIXED</i>	Fixed wavelength defined by installed optic
	<i>CH11</i>	ITU channel 11
	<i>CH12</i>	ITU channel 12
	<i>CH13</i>	ITU channel 13
	<i>CH14</i>	ITU channel 14
	<i>CH15</i>	ITU channel 15
	<i>CH16</i>	ITU channel 16
	<i>CH17</i>	ITU channel 17
	<i>CH18</i>	ITU channel 18
	<i>CH19</i>	ITU channel 19
	<i>CH20</i>	ITU channel 20
	<i>CH21</i>	ITU channel 21
	<i>CH22</i>	ITU channel 22
	<i>CH23</i>	ITU channel 23
	<i>CH24</i>	ITU channel 24
	<i>CH25</i>	ITU channel 25
	<i>CH26</i>	ITU channel 26
	<i>CH27</i>	ITU channel 27
	<i>CH28</i>	ITU channel 28
	<i>CH29</i>	ITU channel 29
	<i>CH30</i>	ITU channel 30
	<i>CH31</i>	ITU channel 31
	<i>CH32</i>	ITU channel 32
	<i>CH33</i>	ITU channel 33
	<i>CH34</i>	ITU channel 34
	<i>CH35</i>	ITU channel 35
	<i>CH36</i>	ITU channel 36
	<i>CH37</i>	ITU channel 37
	<i>CH38</i>	ITU channel 38
	<i>CH39</i>	ITU channel 39
	<i>CH40</i>	ITU channel 40
	<i>CH41</i>	ITU channel 41
	<i>CH42</i>	ITU channel 42
	<i>CH43</i>	ITU channel 43
	<i>CH44</i>	ITU channel 44
	<i>CH45</i>	ITU channel 45
	<i>CH46</i>	ITU channel 46
	<i>CH47</i>	ITU channel 47
	<i>CH48</i>	ITU channel 48
	<i>CH49</i>	ITU channel 49
	<i>CH50</i>	ITU channel 50
	<i>CH51</i>	ITU channel 51
	<i>CH52</i>	ITU channel 52
	<i>CH53</i>	ITU channel 53
	<i>CH54</i>	ITU channel 54
	<i>CH55</i>	ITU channel 55
	<i>CH56</i>	ITU channel 56

		<i>CH57</i> ITU channel 57 <i>CH58</i> ITU channel 58 <i>CH59</i> ITU channel 59 <i>CH60</i> ITU channel 60 <i>CH61</i> ITU channel 61 <i>CH62</i> ITU channel 62 <i>CH63</i> ITU channel 63
	OID	1.3.6.1.4.1.3181.10.6.1.94.5.1.7 (cxgPlusConfigPort4ItuChannel)
<hr/>		
deactivate_port_1	When enabled, the optical interface is disabled and communication is cut.	
	Values	enabled, disabled
	OID	1.3.6.1.4.1.3181.10.6.1.94.5.1.8 (cxgPlusConfigDeactivatePort1)
<hr/>		
deactivate_port_2	When enabled, the optical interface is disabled and communication is cut.	
	Values	enabled, disabled
	OID	1.3.6.1.4.1.3181.10.6.1.94.5.1.9 (cxgPlusConfigDeactivatePort2)
<hr/>		
deactivate_port_3	When enabled, the optical interface is disabled and communication is cut.	
	Values	enabled, disabled
	OID	1.3.6.1.4.1.3181.10.6.1.94.5.1.10 (cxgPlusConfigDeactivatePort3)
<hr/>		
deactivate_port_4	When enabled, the optical interface is disabled and communication is cut.	
	Values	enabled, disabled
	OID	1.3.6.1.4.1.3181.10.6.1.94.5.1.11 (cxgPlusConfigDeactivatePort4)
<hr/>		
front_panel_mode	Determines what is displayed on the front panel, when available. Also controls the modules local buttons.	
	Values	<i>NORMAL</i> Displays module name and error conditions <i>EXTENDED</i> Cyclical shows various system information and error conditions <i>NORMAL_LOCKED</i> Like <i>NORMAL</i> but the module buttons are disabled <i>EXTENDED_LOCKED</i> Like <i>EXTENDED</i> but the module buttons are disabled <i>REMOTE</i> Display is not updated and can be controlled from remote management system
	OID	1.3.6.1.4.1.3181.10.6.1.94.5.1.12 (cxgPlusConfigFrontPanelMode)
<hr/>		

loss_of_signal_handling	When set to LOCAL a loss of input signal will not affect another port. When set to PERCOLATE, a loss of signal will turn off the transmitter of the other port.
Values	<p><i>LOCAL</i> Laser is always turned on when port is enabled</p> <p><i>PERCOLATE</i> Laser is turned off when receiver of associated port is down</p>
OID	1.3.6.1.4.1.3181.10.6.1.94.5.1.13 (cxgPlusConfigLossOfSignalHandling)
sfp_delta_interval	This enables and defines the interval in which the optical receive power level of each SFP/XFP is read and compared to previous value.
Values	<p><i>DISABLED</i> Optical receiver power delta detection is disabled</p> <p><i>1_SEC</i> Optical receive power is compared every second</p> <p><i>5_SEC</i> Optical receive power is compared every 5 seconds</p> <p><i>10_SEC</i> Optical receive power is compared every 10 seconds</p> <p><i>30_SEC</i> Optical receive power is compared every 30 seconds</p> <p><i>60_SEC</i> Optical receive power is compared every minute</p> <p><i>240_SEC</i> Optical receive power is compared every 4 minutes</p>
OID	1.3.6.1.4.1.3181.10.6.1.94.5.1.14 (cxgPlusConfigSfpDeltaInterval)
sfp_delta_threshold	This defines how much the optical receive power level can differ between successive reads before a warning trap is generated.
Values	<p><i>0_5_DB</i> An event is generated if power level varies more than half a dB</p> <p><i>1_DB</i> An event is generated if power level varies more than 1 dB</p> <p><i>1_5_DB</i> An event is generated if power level varies more than 1.5 dB</p> <p><i>2_DB</i> An event is generated if power level varies more than 2 dB</p> <p><i>3_DB</i> An event is generated if power level varies more than 3 dB</p> <p><i>5_DB</i> An event is generated if power level varies more than 5 dB</p>
OID	1.3.6.1.4.1.3181.10.6.1.94.5.1.15 (cxgPlusConfigSfpDeltaThreshold)

Group	cxg_config , for all module slots[0..11]
Path	Device.MSP1000.cxg_config[slot]
Description	This table is used to define any CXG or XCM-3 modules in the system.

cxg_port_1_2_datarate	The CXG relies on the features of the XFP to define its data rate. Since various XFP offer different rates with the same settings, only a general setting is provided. Both ports must operate at the same rate.	
Values	<i>TRANSPARENT</i>	No clock recovery is used. May result in bit errors when there is too little optical budget available
	<i>8X_FC</i>	Lower speed SFP+/XFP setting. Usually 8xFC when matching SFP+/XFP are inserted
	<i>10G_ETH</i>	High speed SFP+/XFP setting. Usually 10G when 8G/10G SFP+/XFP are inserted
	<i>10X_FC_16X_FC</i>	Both SFP+XFP control bits are set. Results depend on plugged-in module. May be 10x FibreChannel, 16x FibreChannel or undetermined.
OID	1.3.6.1.4.1.3181.10.6.1.94.6.1.2 (cxgConfigCxgPort12Datarate)	

port_1_itu_channel	Tunable laser are supported. Select the wavelength from the supplied 100GHZ ITU-T grid. If the wavelength is not supported by the XFP, a warning event will be received.
--------------------	--

Values	<i>FIXED</i>	Fixed wavelength defined by installed optic
	<i>CH11</i>	ITU channel 11
	<i>CH12</i>	ITU channel 12
	<i>CH13</i>	ITU channel 13
	<i>CH14</i>	ITU channel 14
	<i>CH15</i>	ITU channel 15
	<i>CH16</i>	ITU channel 16
	<i>CH17</i>	ITU channel 17
	<i>CH18</i>	ITU channel 18
	<i>CH19</i>	ITU channel 19
	<i>CH20</i>	ITU channel 20
	<i>CH21</i>	ITU channel 21
	<i>CH22</i>	ITU channel 22
	<i>CH23</i>	ITU channel 23
	<i>CH24</i>	ITU channel 24
	<i>CH25</i>	ITU channel 25
	<i>CH26</i>	ITU channel 26
	<i>CH27</i>	ITU channel 27
	<i>CH28</i>	ITU channel 28
	<i>CH29</i>	ITU channel 29
	<i>CH30</i>	ITU channel 30
	<i>CH31</i>	ITU channel 31
	<i>CH32</i>	ITU channel 32
	<i>CH33</i>	ITU channel 33
	<i>CH34</i>	ITU channel 34
	<i>CH35</i>	ITU channel 35
	<i>CH36</i>	ITU channel 36
	<i>CH37</i>	ITU channel 37
	<i>CH38</i>	ITU channel 38
	<i>CH39</i>	ITU channel 39
	<i>CH40</i>	ITU channel 40
	<i>CH41</i>	ITU channel 41
	<i>CH42</i>	ITU channel 42
	<i>CH43</i>	ITU channel 43
	<i>CH44</i>	ITU channel 44
	<i>CH45</i>	ITU channel 45
	<i>CH46</i>	ITU channel 46
	<i>CH47</i>	ITU channel 47
	<i>CH48</i>	ITU channel 48
	<i>CH49</i>	ITU channel 49
	<i>CH50</i>	ITU channel 50
	<i>CH51</i>	ITU channel 51
	<i>CH52</i>	ITU channel 52
	<i>CH53</i>	ITU channel 53
	<i>CH54</i>	ITU channel 54
	<i>CH55</i>	ITU channel 55
	<i>CH56</i>	ITU channel 56

CH57 ITU channel 57

CH58 ITU channel 58

CH59 ITU channel 59

CH60 ITU channel 60

CH61 ITU channel 61

CH62 ITU channel 62

CH63 ITU channel 63

OID

1.3.6.1.4.1.3181.10.6.1.94.6.1.3 (cxgConfigPort1ItuChannel)

port_2_itu_channel

Tunable laser are supported. Select the wavelength from the supplied 100GHZ ITU-T grid. If the wavelength is not supported by the XFP, a warning event will be received.

Values	FIXED	Fixed wavelength defined by installed optic
<i>CH11</i>	ITU channel 11	
<i>CH12</i>	ITU channel 12	
<i>CH13</i>	ITU channel 13	
<i>CH14</i>	ITU channel 14	
<i>CH15</i>	ITU channel 15	
<i>CH16</i>	ITU channel 16	
<i>CH17</i>	ITU channel 17	
<i>CH18</i>	ITU channel 18	
<i>CH19</i>	ITU channel 19	
<i>CH20</i>	ITU channel 20	
<i>CH21</i>	ITU channel 21	
<i>CH22</i>	ITU channel 22	
<i>CH23</i>	ITU channel 23	
<i>CH24</i>	ITU channel 24	
<i>CH25</i>	ITU channel 25	
<i>CH26</i>	ITU channel 26	
<i>CH27</i>	ITU channel 27	
<i>CH28</i>	ITU channel 28	
<i>CH29</i>	ITU channel 29	
<i>CH30</i>	ITU channel 30	
<i>CH31</i>	ITU channel 31	
<i>CH32</i>	ITU channel 32	
<i>CH33</i>	ITU channel 33	
<i>CH34</i>	ITU channel 34	
<i>CH35</i>	ITU channel 35	
<i>CH36</i>	ITU channel 36	
<i>CH37</i>	ITU channel 37	
<i>CH38</i>	ITU channel 38	
<i>CH39</i>	ITU channel 39	
<i>CH40</i>	ITU channel 40	
<i>CH41</i>	ITU channel 41	
<i>CH42</i>	ITU channel 42	
<i>CH43</i>	ITU channel 43	
<i>CH44</i>	ITU channel 44	
<i>CH45</i>	ITU channel 45	
<i>CH46</i>	ITU channel 46	
<i>CH47</i>	ITU channel 47	
<i>CH48</i>	ITU channel 48	
<i>CH49</i>	ITU channel 49	
<i>CH50</i>	ITU channel 50	
<i>CH51</i>	ITU channel 51	
<i>CH52</i>	ITU channel 52	
<i>CH53</i>	ITU channel 53	
<i>CH54</i>	ITU channel 54	
<i>CH55</i>	ITU channel 55	
<i>CH56</i>	ITU channel 56	

		<i>CH57</i>	ITU channel 57
		<i>CH58</i>	ITU channel 58
		<i>CH59</i>	ITU channel 59
		<i>CH60</i>	ITU channel 60
		<i>CH61</i>	ITU channel 61
		<i>CH62</i>	ITU channel 62
		<i>CH63</i>	ITU channel 63
	OID	1.3.6.1.4.1.3181.10.6.1.94.6.1.4 (cxgConfigPort2ItuChannel)	
<hr/>			
deactivate_port_1	When enabled, the optical interface is disabled and communication is cut.		
	Values	enabled, disabled	
	OID	1.3.6.1.4.1.3181.10.6.1.94.6.1.5 (cxgConfigDeactivatePort1)	
<hr/>			
deactivate_port_2	When enabled, the optical interface is disabled and communication is cut.		
	Values	enabled, disabled	
	OID	1.3.6.1.4.1.3181.10.6.1.94.6.1.6 (cxgConfigDeactivatePort2)	
<hr/>			
front_panel_mode	Determines what is displayed on the front panel, when available. Also controls the modules local buttons.		
	Values	<i>NORMAL</i>	Displays module name and error conditions
		<i>EXTENDED</i>	Cyclical shows various system information and error conditions
		<i>NORMAL_LOCKED</i>	Like NORMAL but the module buttons are disabled
		<i>EXTENDED_LOCKED</i>	Like EXTENDED but the module buttons are disabled
		<i>REMOTE</i>	Display is not updated and can be controlled from remote management system
	OID	1.3.6.1.4.1.3181.10.6.1.94.6.1.7 (cxgConfigFrontPanelMode)	
<hr/>			
loss_of_signal_handling	When set to LOCAL a loss of input signal will not affect another port. When set to PERCOLATE, a loss of signal will turn off the transmitter of the other port.		
	Values	<i>LOCAL</i>	Laser is always turned on when port is enabled
		<i>PERCOLATE</i>	Laser is turned off when receiver of associated port is down
	OID	1.3.6.1.4.1.3181.10.6.1.94.6.1.8 (cxgConfigLossOfSignalHandling)	

sfp_delta_interval	This enables and defines the interval in which the optical receive power level of each SFP/XFP is read and compared to previous value.
Values	<p><i>DISABLED</i> Optical receiver power delta detection is disabled</p> <p><i>1_SEC</i> Optical receive power is compared every second</p> <p><i>5_SEC</i> Optical receive power is compared every 5 seconds</p> <p><i>10_SEC</i> Optical receive power is compared every 10 seconds</p> <p><i>30_SEC</i> Optical receive power is compared every 30 seconds</p> <p><i>60_SEC</i> Optical receive power is compared every minute</p> <p><i>240_SEC</i> Optical receive power is compared every 4 minutes</p>
OID	1.3.6.1.4.1.3181.10.6.1.94.6.1.9 (cxgConfigSfpDeltaInterval)
sfp_delta_threshold	This defines how much the optical receive power level can differ between successive reads before a warning trap is generated.
Values	<p><i>0_5_DB</i> An event is generated if power level varies more than half a dB</p> <p><i>1_DB</i> An event is generated if power level varies more than 1 dB</p> <p><i>1_5_DB</i> An event is generated if power level varies more than 1.5 dB</p> <p><i>2_DB</i> An event is generated if power level varies more than 2 dB</p> <p><i>3_DB</i> An event is generated if power level varies more than 3 dB</p> <p><i>5_DB</i> An event is generated if power level varies more than 5 dB</p>
OID	1.3.6.1.4.1.3181.10.6.1.94.6.1.10 (cxgConfigSfpDeltaThreshold)

Group	t4g_config , for all module slots[0..11]
Path	Device.MSP1000.t4g_config[slot]
Description	This table is used to define any T4G or OFC-4 modules in the system.

t4g_port_1_2_datarate The CXG relies on the features of the XFP to define its data rate. Since various XFP offer different rates with the same settings, only a general setting is provided. Both ports must operate at the same rate.

Values	<i>TRANSPARENT</i>	Transparent. No clock recovery is used
	<i>100M_ETH</i>	Port speed 125 Mbps (Fast Ethernet)
	<i>1G_ETH</i>	Port speed 1250 Mbps (Gigabit Ethernet)
	<i>ESCON</i>	Port speed 200M, (X2G, OFX-3 only)
	<i>1X_FC</i>	Port speed 1062 Mbps (1G Fibre Channel)
	<i>2X_FC</i>	Port speed 2125 Mbps (2G Fibre Channel)
	<i>4X_FC</i>	Port speed 4250 Mbps (4G Fibre Channel)
	<i>INFINIBAND</i>	Port speed 2500 Mbps (Infiniband)
	<i>OC_3</i>	Port speed 155 Mbps (OC-3 / STM-1)
	<i>OC_12</i>	Port speed 622 Mbps (OC-12 / STM-4)
	<i>OC_48</i>	Port speed 2048 Mbps (OC-48 / STM-16)
OID	1.3.6.1.4.1.3181.10.6.1.94.7.1.2 (t4gConfigT4gPort12Datarate)	

t4g_port_3_4_datarate Tunable laser are supported. Select the wavelength from the supplied 100GHZ ITU-T grid. If the wavelength is not supported by the XFP, a warning event will be received.

Values	<i>TRANSPARENT</i>	Transparent. No clock recovery is used
	<i>100M_ETH</i>	Port speed 125 Mbps (Fast Ethernet)
	<i>1G_ETH</i>	Port speed 1250 Mbps (Gigabit Ethernet)
	<i>ESCON</i>	Port speed 200M, (X2G, OFX-3 only)
	<i>1X_FC</i>	Port speed 1062 Mbps (1G Fibre Channel)
	<i>2X_FC</i>	Port speed 2125 Mbps (2G Fibre Channel)
	<i>4X_FC</i>	Port speed 4250 Mbps (4G Fibre Channel)
	<i>INFINIBAND</i>	Port speed 2500 Mbps (Infiniband)
	<i>OC_3</i>	Port speed 155 Mbps (OC-3 / STM-1)
	<i>OC_12</i>	Port speed 622 Mbps (OC-12 / STM-4)
	<i>OC_48</i>	Port speed 2048 Mbps (OC-48 / STM-16)
OID	1.3.6.1.4.1.3181.10.6.1.94.7.1.3 (t4gConfigT4gPort34Datarate)	

t4g_operation_mode This parameter defines the data path through the module when an internal cross connect is available. It is also used to setup a permanent bit error rate test. (most settings apply to X2G, TXG, OFX-3, XCM-2 only)

Values	<i>DISABLED</i>	All ports are disabled
	<i>TRANSPONDER</i>	Received clock is recovered and then used for transmitter. P1 connects to P2, P3 connects to P4
	<i>BERT_PORT_4</i>	Port 4 is used as bit error rate tester (BERT). All other ports are unused.
OID	1.3.6.1.4.1.3181.10.6.1.94.7.1.4 (t4gConfigT4gOperationMode)	

deactivate_port_1 When enabled, the optical interface is disabled and communication is cut.

Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.1.94.7.1.5 (t4gConfigDeactivatePort1)

deactivate_port_2	When enabled, the optical interface is disabled and communication is cut.											
Values	enabled, disabled											
OID	1.3.6.1.4.1.3181.10.6.1.94.7.1.6 (t4gConfigDeactivatePort2)											
deactivate_port_3	When enabled, the optical interface is disabled and communication is cut.											
Values	enabled, disabled											
OID	1.3.6.1.4.1.3181.10.6.1.94.7.1.7 (t4gConfigDeactivatePort3)											
deactivate_port_4	When enabled, the optical interface is disabled and communication is cut.											
Values	enabled, disabled											
OID	1.3.6.1.4.1.3181.10.6.1.94.7.1.8 (t4gConfigDeactivatePort4)											
front_panel_mode	Determines what is displayed on the front panel, when available. Also controls the modules local buttons.											
Values	<table><tr><td><i>NORMAL</i></td><td>Displays module name and error conditions</td></tr><tr><td><i>EXTENDED</i></td><td>Cyclical shows various system information and error conditions</td></tr><tr><td><i>NORMAL_LOCKED</i></td><td>Like NORMAL but the module buttons are disabled</td></tr><tr><td><i>EXTENDED_LOCKED</i></td><td>Like EXTENDED but the module buttons are disabled</td></tr><tr><td><i>REMOTE</i></td><td>Display is not updated and can be controlled from remote management system</td></tr></table>		<i>NORMAL</i>	Displays module name and error conditions	<i>EXTENDED</i>	Cyclical shows various system information and error conditions	<i>NORMAL_LOCKED</i>	Like NORMAL but the module buttons are disabled	<i>EXTENDED_LOCKED</i>	Like EXTENDED but the module buttons are disabled	<i>REMOTE</i>	Display is not updated and can be controlled from remote management system
<i>NORMAL</i>	Displays module name and error conditions											
<i>EXTENDED</i>	Cyclical shows various system information and error conditions											
<i>NORMAL_LOCKED</i>	Like NORMAL but the module buttons are disabled											
<i>EXTENDED_LOCKED</i>	Like EXTENDED but the module buttons are disabled											
<i>REMOTE</i>	Display is not updated and can be controlled from remote management system											
OID	1.3.6.1.4.1.3181.10.6.1.94.7.1.9 (t4gConfigFrontPanelMode)											
loss_of_signal_handling	When set to LOCAL a loss of input signal will not affect another port. When set to PERCOLATE, a loss of signal will turn off the transmitter of the other port.											
Values	<table><tr><td><i>LOCAL</i></td><td>Laser is always turned on when port is enabled</td></tr><tr><td><i>PERCOLATE</i></td><td>Laser is turned off when receiver of associated port is down</td></tr></table>		<i>LOCAL</i>	Laser is always turned on when port is enabled	<i>PERCOLATE</i>	Laser is turned off when receiver of associated port is down						
<i>LOCAL</i>	Laser is always turned on when port is enabled											
<i>PERCOLATE</i>	Laser is turned off when receiver of associated port is down											
OID	1.3.6.1.4.1.3181.10.6.1.94.7.1.10 (t4gConfigLossOfSignalHandling)											

bert_pattern

Defines the bit pattern with which the build-in bit error rate tester (BERT) operates when cross connect is set to BERT.

Values	2_7	BERT pattern which repeats every 2 ⁷ bits is used
	2_23	BERT pattern which repeats every 2 ²³ bits is used
	2_31	BERT pattern which repeats every 2 ³¹ bits is used
	CJ_PAT	BERT pattern for 8B10 code testing (X2G, OFX-3 only)
	CR_PAT	BERT pattern for 8B10 code testing (X2G, OFX-3 only)
	8B_10B_CNT	BERT pattern for 8B10 code testing (X2G, OFX-3 only)
OID	1.3.6.1.4.1.3181.10.6.1.94.7.1.11 (t4gConfigBertPattern)	

sfp_delta_interval

This enables and defines the interval in which the optical receive power level of each SFP/XFP is read and compared to previous value.

Values	DISABLED	Optical receiver power delta detection is disabled
	1_SEC	Optical receive power is compared every second
	5_SEC	Optical receive power is compared every 5 seconds
	10_SEC	Optical receive power is compared every 10 seconds
	30_SEC	Optical receive power is compared every 30 seconds
	60_SEC	Optical receive power is compared every minute
	240_SEC	Optical receive power is compared every 4 minutes
OID	1.3.6.1.4.1.3181.10.6.1.94.7.1.12 (t4gConfigSfpDeltaInterval)	

sfp_delta_threshold

This defines how much the optical receive power level can differ between successive reads before a warning trap is generated.

Values	0_5_DB	An event is generated if power level varies more than half a dB
	1_DB	An event is generated if power level varies more than 1 dB
	1_5_DB	An event is generated if power level varies more than 1.5 dB
	2_DB	An event is generated if power level varies more than 2 dB
	3_DB	An event is generated if power level varies more than 3 dB
	5_DB	An event is generated if power level varies more than 5 dB
OID	1.3.6.1.4.1.3181.10.6.1.94.7.1.13 (t4gConfigSfpDeltaThreshold)	

Group Path Description	m2g_config , for all module slots[0..11] Device.MSP1000.m2g_config[slot] This table is used to define any M2G or TDM-2 modules in the system.	
channel_1_datarate	Devices the data rate of the first TDM channel (port 1)	Values <i>DISABLED</i> Local port is disabled <i>1G_ETH</i> Gigabit Ethernet <i>1X_FC</i> FibreChannel OID 1.3.6.1.4.1.3181.10.6.1.94.8.1.2 (m2gConfigChannel1Datarate)
channel_2_datarate	Devices the data rate of the second TDM channel (port 2)	Values <i>DISABLED</i> Local port is disabled <i>1G_ETH</i> Gigabit Ethernet <i>1X_FC</i> FibreChannel OID 1.3.6.1.4.1.3181.10.6.1.94.8.1.3 (m2gConfigChannel2Datarate)
port_1_copper_sfp	Set when local copper RJ45 SFP is used and connection cannot be established.	Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.1.94.8.1.4 (m2gConfigPort1CopperSfp)
port_2_copper_sfp	Set when local copper RJ45 SFP is used and connection cannot be established.	Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.1.94.8.1.5 (m2gConfigPort2CopperSfp)
sfp_delta_interval	This enables and defines the interval in which the optical receive power level of each SFP/XFP is read and compared to previous value.	Values <i>DISABLED</i> Optical receiver power delta detection is disabled <i>1_SEC</i> Optical receive power is compared every second <i>5_SEC</i> Optical receive power is compared every 5 seconds <i>10_SEC</i> Optical receive power is compared every 10 seconds <i>30_SEC</i> Optical receive power is compared every 30 seconds <i>60_SEC</i> Optical receive power is compared every minute <i>240_SEC</i> Optical receive power is compared every 4 minutes OID 1.3.6.1.4.1.3181.10.6.1.94.8.1.6 (m2gConfigSfpDeltaInterval)

sfp_delta_threshold	This defines how much the optical receive power level can differ between successive reads before a warning trap is generated.	
Values	<i>0_5_DB</i>	An event is generated if power level varies more than half a dB
	<i>1_DB</i>	An event is generated if power level varies more than 1 dB
	<i>1_5_DB</i>	An event is generated if power level varies more than 1.5 dB
	<i>2_DB</i>	An event is generated if power level varies more than 2 dB
	<i>3_DB</i>	An event is generated if power level varies more than 3 dB
	<i>5_DB</i>	An event is generated if power level varies more than 5 dB
OID	1.3.6.1.4.1.3181.10.6.1.94.8.1.7 (m2gConfigSfpDeltaThreshold)	
link_backup_trigger	Defines under which optical signal condition an automated backup is initiated.	
Values	<i>DISABLED</i>	No automatic link backup
	<i>SIGNAL_LOSS</i>	Switch backup on link signal loss
	<i>ERROR_BURST</i>	Switch backup when a high error rate on the link is detected or on loss of signal
OID	1.3.6.1.4.1.3181.10.6.1.94.8.1.8 (m2gConfigLinkBackupTrigger)	
stay_with_last_link	When set the backup switch remains in last position even when signal returns. Still the backup warning turns off after the delay set under backup_end parameter expires.	
Values	enabled, disabled	
OID	1.3.6.1.4.1.3181.10.6.1.94.8.1.9 (m2gConfigStayWithLastLink)	
backup_end	Defines how long the signal must remain steady before proper operation is assumed and the backup is terminated.	
Values	<i>NO_DELAY</i>	Immediately switch off backup when missing signal returns
	<i>15_SECONDS</i>	When missing signal returns wait for 15 seconds during which no further signal loss must occur. Only then switch off the backup path
	<i>15_MINUTES</i>	When missing signal returns wait for 15 minutes during which no further signal loss must occur. Only then switch off the backup path
	<i>MANUALLY</i>	Do not switchback automatically. Use action command to switch off backup
OID	1.3.6.1.4.1.3181.10.6.1.94.8.1.10 (m2gConfigBackupEnd)	

permit_link_override	Permits the manual selection of a failed link using the link selection. Defaults to false to safeguard against accidental link selection which would result in loss of connection.
Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.1.94.8.1.11 (m2gConfigPermitLinkOverride)

Group	om1_config , for all module slots[0..11]
Path	Device.MSP1000.om1_config[slot]
Description	

wavelength_port_a	Defines which wavelength band is measured. Use 1550 setting when a WDM link is measured.
Values	<i>1550NM</i> Use 1550nm window. Use when DWDM is used <i>1310NM</i> Use with 1310ns window <i>DISABLED</i> Do not measure this port at all
OID	1.3.6.1.4.1.3181.10.6.1.94.9.1.2 (om1ConfigWavelengthPortA)

low_threshold_port_a	Defines the lower optical signal level in dBm. A signal level below this threshold will trigger an event.
Value	String, max. 16 characters.
OID	1.3.6.1.4.1.3181.10.6.1.94.9.1.3 (om1ConfigLowThresholdPortA)

high_threshold_port_a	Defines the upper optical signal level in dBm. A signal level above this threshold will trigger an event.
Value	String, max. 16 characters.
OID	1.3.6.1.4.1.3181.10.6.1.94.9.1.4 (om1ConfigHighThresholdPortA)

wavelength_port_b	Defines which wavelength band is measured. Use 1550 setting when a WDM link is measured.
Values	<i>1550NM</i> Use 1550nm window. Use when DWDM is used <i>1310NM</i> Use with 1310ns window <i>DISABLED</i> Do not measure this port at all
OID	1.3.6.1.4.1.3181.10.6.1.94.9.1.5 (om1ConfigWavelengthPortB)

low_threshold_port_b	Defines the lower optical signal level in dBm. A signal level below this threshold will trigger an event.
Value	String, max. 16 characters.
OID	1.3.6.1.4.1.3181.10.6.1.94.9.1.6 (om1ConfigLowThresholdPortB)

high_threshold_port_b Defines the upper optical signal level in dBm. A signal level above this threshold will trigger an event.

Value String, max. 16 characters.

OID 1.3.6.1.4.1.3181.10.6.1.94.9.1.7
(om1ConfigHighThresholdPortB)

front_panel_mode Determines what is displayed on the front panel, when available. Also controls the modules local buttons.

Values

<i>NORMAL</i>	Displays module name and error conditions
<i>EXTENDED</i>	Cyclical shows various system information and error conditions
<i>NORMAL_LOCKED</i>	Like NORMAL but the module buttons are disabled
<i>EXTENDED_LOCKED</i>	Like EXTENDED but the module buttons are disabled
<i>REMOTE</i>	Display is not updated and can be controlled from remote management system

OID 1.3.6.1.4.1.3181.10.6.1.94.9.1.8 (om1ConfigFrontPanelMode)

Group
Path
Description

lp1_config, for all module slots[0..11]
Device.MSP1000.lp1_config[slot]

wavelength_port_a Defines which wavelength band is measured. Use 1550 setting when a WDM link is measured.

Values

<i>1550NM</i>	Use 1550nm window. Use when DWDM is used
<i>1310NM</i>	Use with 1310nm window
<i>DISABLED</i>	Do not measure this port at all

OID 1.3.6.1.4.1.3181.10.6.1.94.10.1.2 (lp1ConfigWavelengthPortA)

low_threshold_port_a Defines the lower optical signal level in dBm. A signal level below this threshold will trigger an event and a backup when configured.

Value String, max. 16 characters.

OID 1.3.6.1.4.1.3181.10.6.1.94.10.1.3
(lp1ConfigLowThresholdPortA)

high_threshold_port_a Defines the upper optical signal level in dBm. A signal level above this threshold will trigger an event and a backup when configured.

Value String, max. 16 characters.

OID 1.3.6.1.4.1.3181.10.6.1.94.10.1.4
(lp1ConfigHighThresholdPortA)

wavelength_port_b	Defines which wavelength band is measured. Use 1550 setting when a WDM link is measured.
Values	<i>1550NM</i> Use 1550nm window. Use when DWDM is used <i>1310NM</i> Use with 1310ns window <i>DISABLED</i> Do not measure this port at all
OID	1.3.6.1.4.1.3181.10.6.1.94.10.1.5 (Ip1ConfigWavelengthPortB)
low_threshold_port_b	Defines the lower optical signal level in dBm. A signal level below this threshold will trigger an event and a backup when configured.
Value	String, max. 16 characters.
OID	1.3.6.1.4.1.3181.10.6.1.94.10.1.6 (Ip1ConfigLowThresholdPortB)
high_threshold_port_b	Defines the upper optical signal level in dBm. A signal level above this threshold will trigger an event and a backup when configured.
Value	String, max. 16 characters.
OID	1.3.6.1.4.1.3181.10.6.1.94.10.1.7 (Ip1ConfigHighThresholdPortB)
backup_criteria	Defines under which optical signal condition an automated backup is initiated.
Values	<i>SIGNAL_LOW</i> Loss of signal or below threshold triggers backup switching <i>SIGNAL_HIGH</i> Signal above or below threshold triggers backup switching <i>MANUALLY</i> No automatic backup switching. Switching is controlled by ..control.switch_backup actions
OID	1.3.6.1.4.1.3181.10.6.1.94.10.1.8 (Ip1ConfigBackupCriteria)
stay_with_last_link	When set the backup switch remains in last position even when signal return. Still the backup warning turns off after the delay set under backup_end parameter expires.
Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.1.94.10.1.9 (Ip1ConfigStayWithLastLink)
backup_end	Defines how long the signal must remain steady before proper operation is assumed and the backup is terminated.
Values	<i>NO_DELAY</i> Immediately switch off backup when missing signal returns <i>15_SECONDS</i> When missing signal returns wait for 15 seconds during which no further signal loss must occur. Only then switch off the backup path <i>15_MINUTES</i> When missing signal returns wait for 15 minutes during which no further signal loss must occur. Only then switch off the backup path <i>MANUALLY</i> Do not switchback automatically. Use action command to switch off backup
OID	1.3.6.1.4.1.3181.10.6.1.94.10.1.10 (Ip1ConfigBackupEnd)

front_panel_mode	Determines what is displayed on the front panel, when available. Also controls the modules local buttons.		
	Values	NORMAL	Displays module name and error conditions
		EXTENDED	Cyclical shows various system information and error conditions
		NORMAL_LOCKED	Like NORMAL but the module buttons are disabled
		EXTENDED_LOCKED	Like EXTENDED but the module buttons are disabled
		REMOTE	Display is not updated and can be controlled from remote management system
	OID	1.3.6.1.4.1.3181.10.6.1.94.10.1.11 (lp1ConfigFrontPanelMode)	

Group	em_config, for all module slots[0..11]
Path	Device.MSP1000.em_config[slot]
Description	Configuration for EDFA amplifier modules EM2 and EM3.

edfa_operation_mode	Defines which wavelength band is measured. Use 1550 setting when a WDM link is measured.		
	Values	PUMP_DISABLED	Use 1550nm window. Use when DWDM is used
		PRE_AMP	Use with 1310ns window
		BOOSTER	Do not measure this port at all
	OID	1.3.6.1.4.1.3181.10.6.1.94.11.1.2 (emConfigEdfaOperationMode)	

loss_of_signal_handling	Defines if loss of input signal turns off the EDFA pump (PERCOLATE) or not (LOCAL)		
	Values	LOCAL	Laser is always turned on when port is enabled
		PERCOLATE	Laser is turned off when receiver of associated port is down
	OID	1.3.6.1.4.1.3181.10.6.1.94.11.1.3 (emConfigLossOfSignalHandling)	

signal_gain	Desired signal gain in dB.		
	Value	String, max. 16 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.94.11.1.4 (emConfigSignalGain)	

max_output_power	Maximum output power permitted to exit the module.		
	Value	String, max. 16 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.94.11.1.5 (emConfigMaxOutputPower)	

low_threshold_edfa_in	This corresponds to the unamplified input signal before entering the EDFA section. Defines the lower optical signal level in dBm. A signal level below this threshold will trigger an event.										
Value	String, max. 16 characters.										
OID	1.3.6.1.4.1.3181.10.6.1.94.11.1.6 (emConfigLowThresholdEdfaIn)										
high_threshold_edfa_in	This corresponds to the unamplified input signal before entering the EDFA section. Defines the upper optical signal level in dBm. A signal level above this threshold will trigger an event.										
Value	String, max. 16 characters.										
OID	1.3.6.1.4.1.3181.10.6.1.94.11.1.7 (emConfigHighThresholdEdfaIn)										
low_threshold_port_b	Port B is the unamplified return path through the module. Defines the lower optical signal level in dBm. A signal level below this threshold will trigger an event.										
Value	String, max. 16 characters.										
OID	1.3.6.1.4.1.3181.10.6.1.94.11.1.8 (emConfigLowThresholdPortB)										
high_threshold_port_b	Port B is the unamplified return path through the module. Defines the upper optical signal level in dBm. A signal level above this threshold will trigger an event.										
Value	String, max. 16 characters.										
OID	1.3.6.1.4.1.3181.10.6.1.94.11.1.9 (emConfigHighThresholdPortB)										
front_panel_mode	Determines what is displayed on the front panel, when available. Also controls the modules local buttons.										
Values	<table> <tr> <td data-bbox="655 1319 751 1346"><i>NORMAL</i></td><td data-bbox="900 1319 1254 1373">Displays module name and error conditions</td></tr> <tr> <td data-bbox="655 1379 775 1406"><i>EXTENDED</i></td><td data-bbox="900 1379 1246 1433">Cyclical shows various system information and error conditions</td></tr> <tr> <td data-bbox="655 1440 855 1467"><i>NORMAL_LOCKED</i></td><td data-bbox="900 1440 1302 1494">Like NORMAL but the module buttons are disabled</td></tr> <tr> <td data-bbox="655 1500 879 1527"><i>EXTENDED_LOCKED</i></td><td data-bbox="900 1500 1326 1554">Like EXTENDED but the module buttons are disabled</td></tr> <tr> <td data-bbox="655 1561 751 1588"><i>REMOTE</i></td><td data-bbox="900 1561 1302 1648">Display is not updated and can be controlled from remote management system</td></tr> </table>	<i>NORMAL</i>	Displays module name and error conditions	<i>EXTENDED</i>	Cyclical shows various system information and error conditions	<i>NORMAL_LOCKED</i>	Like NORMAL but the module buttons are disabled	<i>EXTENDED_LOCKED</i>	Like EXTENDED but the module buttons are disabled	<i>REMOTE</i>	Display is not updated and can be controlled from remote management system
<i>NORMAL</i>	Displays module name and error conditions										
<i>EXTENDED</i>	Cyclical shows various system information and error conditions										
<i>NORMAL_LOCKED</i>	Like NORMAL but the module buttons are disabled										
<i>EXTENDED_LOCKED</i>	Like EXTENDED but the module buttons are disabled										
<i>REMOTE</i>	Display is not updated and can be controlled from remote management system										
OID	1.3.6.1.4.1.3181.10.6.1.94.11.1.10 (emConfigFrontPanelMode)										

Group	module_control , for all module slots[0..11]
Path	Device.MSP1000.module_control[slot]
Description	

enter_password	<p>This command will set the module password. Only required when the nms_operation_mode is set to passive mode. Enter the password before configuration or actions can be accepted by the module.</p> <p>Action Execute command with parameter string max. 16 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.12.1.2 (moduleControlEnterPassword)</p>
reboot_module	<p>This command will restart the module. All communication will be disrupted! Syntax: reboot_module = CONFIRM.</p> <p>Action Execute command with parameter string max. 16 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.12.1.3 (moduleControlRebootModule)</p>
warm_start	<p>This command will warm start the module. Communication shall not be disrupted. (Firmware dependent) Syntax: warm_start = CONFIRM.</p> <p>Action Execute command with parameter string max. 16 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.12.1.4 (moduleControlWarmStart)</p>
clear_counter	<p>This command will clear all module and port related statistics counter.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.12.1.5 (moduleControlClearCounter)</p>
switch_off_backup	<p>For a module that supports backup and which currently is in backup condition this command will revert to normal operation. If this would disrupt traffic a warning is returned and nothing is executed. To override this warning and switch back nonetheless type switch_off_backup = CONFIRM</p> <p>Action Execute command with parameter string max. 16 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.12.1.6 (moduleControlSwitchOffBackup)</p>
switch_to_backup	<p>For a module that supports backup this command will switch to the backup link. If this would disrupt traffic because backup link is not available a warning is returned and nothing is executed. To override this warning and switch over nonetheless type switch_to_backup = CONFIRM</p> <p>Action Execute command with parameter string max. 16 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.12.1.7 (moduleControlSwitchToBackup)</p>
automatic_backup	<p>This command returns a manually overridden backup module to normal automatic mode. No parameter are required.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.12.1.8 (moduleControlAutomaticBackup)</p>
write_display	<p>Writes to the front panel display of the module. Only for modules that offer a front panel display.</p> <p>Action Execute command with parameter string max. 64 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.12.1.9 (moduleControlWriteDisplay)</p>

led_test	<p>This will start the modules LED test and will return the LED back up automatic mode after a few seconds. May be also be used to identify a certain module.</p> <p>Action Excecute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.12.1.10 (moduleControlLedTest)</p>
loop_off	<p>Turns all loops off</p> <p>Action Excecute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.12.1.11 (moduleControlLoopOff)</p>
loop_port_1	<p>Tries to engage a loop at port 1. Note not all modules support loops. View port status to check success.</p> <p>Action Excecute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.12.1.12 (moduleControlLoopPort1)</p>
loop_port_2	<p>Tries to engage a loop at port 2. Note not all modules support loops. View port status to check success.</p> <p>Action Excecute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.12.1.13 (moduleControlLoopPort2)</p>
loop_port_3	<p>Tries to engage a loop at port 3. Note not all modules support loops. View port status to check success.</p> <p>Action Excecute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.12.1.14 (moduleControlLoopPort3)</p>
loop_port_4	<p>Tries to engage a loop at port 4. Note not all modules support loops. View port status to check success.</p> <p>Action Excecute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.12.1.15 (moduleControlLoopPort4)</p>
bert_restart	<p>Resynchronizes BERT. Only has an effect if a BERT is available on the module and configured to be active. ATTENTION: Not implemented.</p> <p>Action Excecute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.12.1.16 (moduleControlBertRestart)</p>
bert_insert_error	<p>Inserts an error in the data pattern. This can be used to confirm that a BERT is actually operating. Only has an effect if a BERT is available on the module and configured to be active. ATTENTION: Not implemented.</p> <p>Action Excecute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.12.1.17 (moduleControlBertInsertError)</p>

bert_clear_counter	Clears the BERT counter. Only has an effect if a BERT is available on the module and configured to be active. ATTENTION: Not implemented.
Action	Execute command.
OID	1.3.6.1.4.1.3181.10.6.1.94.12.1.18 (moduleControlBertClearCounter)

Group	system_config
Path	Device.MSP1000.system_config
Description	

nms_operation_mode	Read and learn in PASSIVE mode or ACTIVE mode forcing configuration upon the other modules.
Values	<p><i>PASSIVE</i> The NMS only listens to the bus traffic and reconfigures itself according to the current rack setting. It learns the current installation. It is also possible to write configuration via the NM module.</p> <p><i>ACTIVE</i> In active mode the NMS forces its configuration upon the modules. When a module is exchanged, it is automatically reconfigured to match the defined slot configuration. Otherwise operation is similar to PASSIVE mode.</p>
OID	1.3.6.1.4.1.3181.10.6.1.94.1.1.2 (systemConfigNmsOperationMode)

core_mode	Use V2 unless used with an older system running in V1 mode. Only change when instructed.
Values	<p><i>V1</i> Legacy internal bus protocol version 1</p> <p><i>V2</i> Internal bus protocol version 2. This should be selected for new installations</p>
OID	1.3.6.1.4.1.3181.10.6.1.94.1.1.3 (systemConfigCoreMode)

node_id	Node Id used when NMS is used in combination with SEEmiles V5 management software. When in doubt use default node id 60000.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.1.94.1.1.4 (systemConfigNodeId)

disable_legacy_access	When set network access via SEEmiles is no longer possible.
Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.1.94.1.1.5 (systemConfigDisableLegacyAccess)

22.5 MSP1000 Status Parameters

Group	module_inventory , for all module slots[0..11]	
Path	Device.MSP1000.module_inventory[slot]	
Description		
expected_module	Name of module configured for this slot.	
	Value	String, max. 16 characters.
	OID	1.3.6.1.4.1.3181.10.6.1.94.101.1.2 (moduleInventoryExpectedModule)
module	Name of module actually discovered in this slot. This name should be equal to the above name otherwise configuration may not apply properly.	
	Value	String, max. 16 characters.
	OID	1.3.6.1.4.1.3181.10.6.1.94.101.1.3 (moduleInventoryModule)
type	General functional type of module inserted.	
	Values	<div> <div><i>EMPTY</i></div> <div>No backup active or no backup supported by this module</div> </div> <div> <div><i>UNKNOWN</i></div> <div>Module is not known to the manager</div> </div> <div> <div><i>TRANSPONDER</i></div> <div>Transponder for data transfer</div> </div> <div> <div><i>MEASUREMENT</i></div> <div>Measurement or testing module</div> </div> <div> <div><i>AMPLIFIER</i></div> <div>Optical amplifier (EDFA)</div> </div> <div> <div><i>MANAGEMENT</i></div> <div>Management module</div> </div> <div> <div><i>PASSIVE</i></div> <div>Passive optical filter module</div> </div> <div> <div><i>OCCUPIED</i></div> <div>Slot covered by a double width module</div> </div>
	OID	1.3.6.1.4.1.3181.10.6.1.94.101.1.4 (moduleInventoryType)
board_code	Internal code of actually inserted module.	
	Value	Number in range 0-255
	OID	1.3.6.1.4.1.3181.10.6.1.94.101.1.5 (moduleInventoryBoardCode)
additional_info	Additional information that may be saved in some modules during production.	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.1.94.101.1.6 (moduleInventoryAdditionalInfo)
serial_number	Serial number as stored within the hardware.	
	Value	String, max. 16 characters.
	OID	1.3.6.1.4.1.3181.10.6.1.94.101.1.7 (moduleInventorySerialNumber)

occupied_slots	<p>Number of slots taken by this module. Usually 1.</p> <p>Value Number in range 0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.101.1.8 (moduleInventoryOccupiedSlots)</p>
project_number	<p>Internal hardware project number</p> <p>Value String, max. 8 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.101.1.9 (moduleInventoryProjectNumber)</p>
build_version	<p>Precise build code for hardware version tracking.</p> <p>Value String, max. 16 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.101.1.10 (moduleInventoryBuildVersion)</p>
production_date	<p>Production data of the module</p> <p>Value String, max. 16 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.101.1.11 (moduleInventoryProductionDate)</p>
mfg_test_info	<p>Internal information for quality management. Manufacturing Site / Test Site / Test Person</p> <p>Value String, max. 16 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.101.1.12 (moduleInventoryMfgTestInfo)</p>
number_of_optical_ports	<p>Indicates the number of actively monitored optical ports of this type of module.</p> <p>Value Number in range 0-255</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.101.1.13 (moduleInventoryNumberOfOpticalPorts)</p>
number_of_sfp_ports	<p>Indicates the number of optical SFP or SFP+ ports of this type of module.</p> <p>Value Number in range 0-255</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.101.1.14 (moduleInventoryNumberOfSfpPorts)</p>
number_of_xfp_ports	<p>Indicates the number of optical XFP ports of this type of module.</p> <p>Value Number in range 0-255</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.101.1.15 (moduleInventoryNumberOfXfpPorts)</p>
core_firmware_version	<p>Core operating system software version.</p> <p>Value String, max. 24 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.94.101.1.16 (moduleInventoryCoreFirmwareVersion)</p>

core_firmware_date	Core operating system software creation date. Value String, max. 16 characters. OID 1.3.6.1.4.1.3181.10.6.1.94.101.1.17 (moduleInventoryCoreFirmwareDate)
appl_firmware_version	Application software version. Value String, max. 24 characters. OID 1.3.6.1.4.1.3181.10.6.1.94.101.1.18 (moduleInventoryApplFirmwareVersion)
appl_firmware_date	Application software creation date. Value String, max. 16 characters. OID 1.3.6.1.4.1.3181.10.6.1.94.101.1.19 (moduleInventoryApplFirmwareDate)
Group Path Description	module_status , for all module slots[0..11] Device.MSP1000.module_status[slot] This table holds a record for each module in the system. Note that not all modules deliver every kind of status.
module	Name of module actually discovered in this slot. Value String, max. 16 characters. OID 1.3.6.1.4.1.3181.10.6.1.94.102.1.2 (moduleStatusModule)
system_ok	True when the module has booted and appears ok. Values true, false OID 1.3.6.1.4.1.3181.10.6.1.94.102.1.3 (moduleStatusSystemOk)
error_condition	True when any error condition is currently present. Values true, false OID 1.3.6.1.4.1.3181.10.6.1.94.102.1.4 (moduleStatusErrorCondition)
test_mode	True when module is in loopback test or a backup is engaged. Values true, false OID 1.3.6.1.4.1.3181.10.6.1.94.102.1.5 (moduleStatusTestMode)
spare_part	True when module is marked as spare part. Values true, false OID 1.3.6.1.4.1.3181.10.6.1.94.102.1.6 (moduleStatusSparePart)

uptime	Uptime since last reboot in seconds.
Value	PERIOD0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.1.94.102.1.7 (moduleStatusUptime)
time_since_counter_reset	How long ago have the statistics counter been restarted.
Value	PERIOD0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.1.94.102.1.8 (moduleStatusTimeSinceCounterReset)
temperature	Temperature value in centigrade.
Value	Number in range 0-255
OID	1.3.6.1.4.1.3181.10.6.1.94.102.1.9 (moduleStatusTemperature)
too_hot	True when module is running too hot.
Values	true, false
OID	1.3.6.1.4.1.3181.10.6.1.94.102.1.10 (moduleStatusTooHot)
backup_state	Indicates if a backup is active and in which state.
Values	<div> <div><i>NONE</i></div> <div>No backup active or no backup supported by this module</div> </div> <div> <div><i>DISRUPTED</i></div> <div>Both links are down and communication is disrupted</div> </div> <div> <div><i>BACKUP</i></div> <div>Backup is engaged and working</div> </div> <div> <div><i>AWAIT_SWITCHBACK</i></div> <div>Backup condition is finished but the backup is still active due to hold time</div> </div> <div> <div><i>MANUAL</i></div> <div>Backup was switches manually by operator</div> </div>
OID	1.3.6.1.4.1.3181.10.6.1.94.102.1.11 (moduleStatusBackupState)
backup_counter	Counts the number of times this module has initiated a backup (if backup feature is available for this module type).
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.1.94.102.1.12 (moduleStatusBackupCounter)
backup_duration	How long the backup has been activated in total since last value reset.
Value	PERIOD0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.1.94.102.1.13 (moduleStatusBackupDuration)

Group Path Description	em_status, for all module slots[0..11] Device.MSP1000.em_status[slot] Optical amplifier status		
system_ok	True when no errors are present		
	Values	true, false	
	OID	1.3.6.1.4.1.3181.10.6.1.94.104.1.2 (emStatusSystemOk)	
errors	Indicates various optical error conditions.		
	Values	OK	No other errors present
		LOSS_OF_INPUT	Input signal missing. Nothing to amplify
		LOSS_OF_OUTPUT	Output power dropped due to other error
		TOO_HOT	The pump laser is running too hot
		EYE_SAFETY_SHUTDOWN	Laser pump disabled to protect eyes
		BACK_REFLECTION	Back reflection may be caused by a bad cable on the output side (Port B)
		POWER_LIMIT	Output power limit reached
		OVER_CURRENT	Too much electrical power is consumed
		PUMP_DOWN	The pump laser is disabled due to other error
	OID	1.3.6.1.4.1.3181.10.6.1.94.104.1.3 (emStatusErrors)	
hardware_code	Details codes about the installed hardware components.		
	Value	String, max. 32 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.94.104.1.4 (emStatusHardwareCode)	
time_since_power_error	How long ago since the last time the output power was in error condition.		
	Value	PERIOD0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.1.94.104.1.5 (emStatusTimeSincePowerError)	
time_with_power_loss	Accumulated time the output power has been down.		
	Value	PERIOD0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.1.94.104.1.6 (emStatusTimeWithPowerLoss)	
input_signal_low_counter	Number of times a loss of signal has occurred.		
	Value	Number in range 0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.1.94.104.1.7 (emStatusInputSignalLowCounter)	

input_power	Optical input power of port A. Value String, max. 16 characters. OID 1.3.6.1.4.1.3181.10.6.1.94.104.1.8 (emStatusInputPower)
signal_gain	Indicates how strong the input signal is amplified. Value String, max. 16 characters. OID 1.3.6.1.4.1.3181.10.6.1.94.104.1.9 (emStatusSignalGain)
optimal_flat_gain	Indicates the best gain setting for an even amplification across the wavelength channels Value String, max. 16 characters. OID 1.3.6.1.4.1.3181.10.6.1.94.104.1.10 (emStatusOptimalFlatGain)
back_reflection	The value should be low and indicates cable issues if not. Value String, max. 16 characters. OID 1.3.6.1.4.1.3181.10.6.1.94.104.1.11 (emStatusBackReflection)
signal_output_power	Indicated the actually achieved optical signal output power. Value String, max. 16 characters. OID 1.3.6.1.4.1.3181.10.6.1.94.104.1.12 (emStatusSignalOutputPower)
total_output_power	Indicated the actually achieved optical output power leaving the module (including noise). Value String, max. 16 characters. OID 1.3.6.1.4.1.3181.10.6.1.94.104.1.13 (emStatusTotalOutputPower)
min_output_power	Indicates the minimum optical output level that must be send out Value String, max. 16 characters. OID 1.3.6.1.4.1.3181.10.6.1.94.104.1.14 (emStatusMinOutputPower)
max_output_power	Indicates the maximum optical output level that can be send out Value String, max. 16 characters. OID 1.3.6.1.4.1.3181.10.6.1.94.104.1.15 (emStatusMaxOutputPower)
cfg_output_power	Indicated the desired configured optical output power Value String, max. 16 characters. OID 1.3.6.1.4.1.3181.10.6.1.94.104.1.16 (emStatusCfgOutputPower)

Group	bert_status , for all module slots[0..11]		
Path	Device.MSP1000.bert_status[slot]		
Description	Displays the results of the bit error rate tester (BERT) if it is present and enabled in a slot		
location	Textual description of BERT port location.		
	Value	String, max. 16 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.94.105.1.2 (bertStatusLocation)	
bert_operation	Indicates the general bit error rate tester operational status.		
	Values	<i>UNUSED</i>	BERT is not enabled or not present in this module
		<i>IN_SYNC</i>	BERT has synchronized. Test data can be transferred.
		<i>WAS_OUT_OF_SYNC</i>	BERT is now synchronized, but was out of sync of some time after that last BERT restart or clear error command.
		<i>OUT_OF_SYNC</i>	BERT is out of sync. No data transfer is possible.
	OID	1.3.6.1.4.1.3181.10.6.1.94.105.1.3 (bertStatusBertOperation)	
total_errors	Number of errored bits. Only valid when BERT is synchronized.		
	Value	Number in range 0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.1.94.105.1.4 (bertStatusTotalErrors)	
time_since_last_error	Seconds elapsed since the last error was detected.		
	Value	PERIOD0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.1.94.105.1.5 (bertStatusTimeSinceLastError)	
total_test_time	Accumulated time how long the test was run since last value clear.		
	Value	PERIOD0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.1.94.105.1.6 (bertStatusTotalTestTime)	
errored_time	Accumulated seconds in which at least on errored bit was detected.		
	Value	PERIOD0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.1.94.105.1.7 (bertStatusErroredTime)	
bit_error_rate	Averaged bit error rate during test interval.		
	Value	String, max. 16 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.94.105.1.8 (bertStatusBitErrorRate)	

ber_since_last_error	Bit error rate since last error.
	Value String, max. 16 characters.
	OID 1.3.6.1.4.1.3181.10.6.1.94.105.1.9 (bertStatusBerSinceLastError)
theoretical_ber	Theoretical best possible error rate in the given time frame of the current test interval.
	Value String, max. 16 characters.
	OID 1.3.6.1.4.1.3181.10.6.1.94.105.1.10 (bertStatusTheoreticalBer)
availability	Relation of transmitted vs. Errored bits.
	Value String, max. 16 characters.
	OID 1.3.6.1.4.1.3181.10.6.1.94.105.1.11 (bertStatusAvailability)
Group Path Description	
system_status Device.MSP1000.system_status	
any_error_condition	True when any error condition is currently present in any module.
	Values true, false
	OID 1.3.6.1.4.1.3181.10.6.1.94.100.1.2 (systemStatusAnyErrorCondition)
any_test_mode	True when any module is in loopback test or has a backup engaged.
	Values true, false
	OID 1.3.6.1.4.1.3181.10.6.1.94.100.1.3 (systemStatusAnyTestMode)
any_spare_part	True when any module is marked as spare part.
	Values true, false
	OID 1.3.6.1.4.1.3181.10.6.1.94.100.1.4 (systemStatusAnySparePart)
used_node_id	Actually used node id as discovered from device
	Value Number in range 0-0xFFFFFFFF
	OID 1.3.6.1.4.1.3181.10.6.1.94.100.1.5 (systemStatusUsedNodeId)
local_rack	Indicates in which rack the management module over which this information is retrieved is inserted.
	Value Number in range 0-0xFFFFFFFF
	OID 1.3.6.1.4.1.3181.10.6.1.94.100.1.6 (systemStatusLocalRack)

local_slot	Indicates in which slot the management module over which this information is retrieved is inserted.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.1.94.100.1.7 (systemStatusLocalSlot)

23 SmartOffice

23.1 Key Features

General Features

SmartOffice is complete room automation system designed to measure and control office environment. This includes lighting, temperature, outlets, blinds, air condition and other facilities. Sensor and actors from MICROSENS or various third parties can be combined for a customized decentralized solution. Such rooms can in turn be managed centrally from a Building Management System.

A SmartOffice solution can be introduced room-by-room to upgrade existing installations. Automated rooms conserve energy save costs by turning down when not in use.

PoE based LED Lighting

LED panels replace traditional neon tubes. The MICROSENS SmartLightController acts as an intelligent power supply that converts PoE energy to dimmable LED compatible power.

The LED panels can be dimmed and some panel type offer tunable color of light as well

Room Sensors

The MICROSENS SmartLightController includes sensors to detect ambient temperature, brightness, motion. These sensor data act as inputs to the room automation.

Small, non intrusive sensor at the ceiling.

Automatic Room

A SmartOffice can operate fully automated, based on motion and time. After a programmable idle time the room is shut down. What exactly shuts down, and what not can be configured.

No need to for manual intervention. No one can forget to turn off lights or projector after a meeting is finished.

Configurable Graphical User Interface

A SmartOffice can also be operated very conveniently via a tablet or mobile phone. The graphical user interface (GUI) is fully configurable and customizable to meet any customer requirements.

GUI will autosize and adapt to any display device. When several GUI are used in parallel they will all synchronize.

Scene Based

All actions are grouped in scenes. A scene may affect every as little or as much of the parameter as desired. A scene can be global, room specific or even remotely accessed (if enabled) to be engaged from a third party.

A streamlined logical design eases customization and operation.

Hardware Buttons

A SmartOffice can interface to many types of physical switches. Any switch can be mapped to any scene.

Some people prefer traditional switches to control or override automatic functions.

Scripting Language

A key feature of the SmartOffice solution is the powerful scripting engine. The script incorporates the decision logic as to what to do based on sensor input. Most scripts are preinstalled during installation of the SmartDirector App, but additional custom scripts may be added to perform a wide range of features such as SNMP, HTTP or FTP operations, special office functions, etc.

Scripts may be used to enhance scene functionality beyond the normal scope of room control.

SmartDirector App

The SmartOffice framework offers great flexibility. In fact so much that it is sensible to offer a default functionality and graphical user interface. This interface is created by installing the SmartDirector App. For special applications, other variations of the App can be created, without affecting the general firmware of the underlying switch.

The SmartDirector App creates the visual interface that normal Office users will see. It also comes with a set of configuration parameters to ease initial deployment.

microPLC

SmartOffice comes with software script controlled PLC (programmable Logic controller) function that permits PID regulators and other typical PLC applications. The microPLC does not support IEC programming but instead relies on microScript. PLC and event based operation may coexist to offer the best programming interface for any office and building automation task at hand.

The combination of event and timing controlled program execution offers the optimal platform for any given task in building automation.

Remote Control Interface

SmartOffice comes with a local graphical interface. To operate the system remotely it is possible to simulate operation via an HTTPS REST API interface. When enabled, for each element individually, it is possible to expose a well defined set of functions, which can be controlled. Likewise, it is possible to read information from the system.

A building manager that wants to turn off all lights in the building at the push of a button, could utilize this interface to accomplish the task, without the need to know any details about the individual rooms.

enOcean support

SmartOffice supports wireless automation devices using the enOcean protocol. This includes switches, relays to switch outlets, blinds and some sensors. Energy consumption monitoring is available.

A key feature of enOcean is the fact the physical switches require no battery. Energy is harvested from piezo crystal during mechanical switch movement.

Homematic support

SmartOffice supports wireless automation devices using the Homematic protocol. This includes switches, relays to switch outlets, temperature control and other devices.

These wireless devices combine low cost with good functionality.

Modbus/RTU support

Modbus is a standard automation bus. SmartOffice supports local serial wiring to Modbus enabled devices. Custom scripts are required for integration as there is no standard on how to interpret the data.

Interface to older style automation systems.

Modbus/IP support

Modbus/IP is a standard automation protocol user over IP. Configurable mapping of any Modbus coil, register or memory cell to a named and data typed SmartOffice sensor or actor data point. This way Modbus devices can seamlessly be integrated into a SmartOffice installation.

Seamlessly integrate older style automation systems.

23.2 Functional Description

SmartOffice

SmartOffice setup and status parameters.

23.3 SmartOffice CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Device.	smartoffice.					Smart light and office control
			enable_smart_office		R/W	Generally enable the SmartOffice solution.
	director_config.					General configuration of the director.
			domain_name		R/W	
			general_mode		R/W	
			act_on_ungrouped_sensors		R/W	When set any sensor attributes which are not configured to be part of a sensor group, will also trigger the regular script execution. This may be selected in smaller setups to save the effort of defining groups. Note that no event rate limiting can be applied to ungrouped sensors and thus using this mode can result in overloading the system leading to sluggish response times.
			scan_filter		R/W	The scan filter may be used to limit the displayed output when applying the scan_light_controllers action.
			scan_light_controllers		X	Scan the local network for reachable SmartLightController and display a list. The scan_filter parameter is applied.
	device_config[DYNAMIC].					Defines the configuration of each device under control. A device may contain one or more actor or sensor functions.
			device_name		R/W	Unique group name referenced by the director. Important: For some devices further configuration options are available in the section Device.Controller. The name defined here must be identical to a name defined there to match the configuration options.
			location		R/W	Free text to describe the position of the controller on the premises. This value need NOT be saved within the sensor itself.
			latitude		R/W	A value in degrees such as: 50,123
			longitude		R/W	A value in degrees such as: 50,123
			altitude		R/W	A value in meters.
			placement		R/W	Information where to find the controller

product_type	R/W	The product type is used by the system to select the network protocol required to access the device. Note that for some devices a further configuration section exists under the Device.Controller section. Such additional config exists for type SMARTLIGHT_CONTROLLER and SMART_IO_CONTROLLER.
device_id	R/W	Unique manufacturer dependent identifier of the device. For SmartLightController the MAC address of the controller is entered here.
network_address	R/W	May be an IP or other type of address depending on the given network access method. Can be left blank for a SmartLightController.
additional_parameter	R/W	Comma separated list of any parameter specific for this device. Example: panel=type A,refresh_rate=12
network_failure_action	R/W	Defines what the actor does if the network connection fails or after reboot until communication is established.
identify	X	The actor will blink with its status led to signal its presence and physical location. Supply instance or 0 or nothing for all instances.
restart	X	Restart the device.
calibrate	X	Start calibration process (if available for this actor type).
pair	X	Start pairing process that couples individual device to this director.
unpair	X	Discard existing pairing between an individual device and this director.
update_firmware	X	Update the device firmware. When no file name is supplied, the latest version is automatically selected. Alternatively, a specific file name can be supplied to use another version. Use Management.files.firmware.display_files to view a list of available files under the SLC section. (applies to SmartLight Controllers)
actor_group_config[DYNAMIC].		Defines a group of actors that support the same attribute and which shall be set together to the same value.
group_name	R/W	Unique group name referenced by the director
attribute	R/W	The attribute which is configured. Locally, identical attributes of the associated devices listed below are grouped.
associated_devices	R/W	List of all actors that supply information to a particular group. When an instance is used, here the syntax devicename.instance is used. Alternatively, a colon separator may be used instead of the dot. All records are comma separated. Instance ranges may be used: DEV.(1-4,12) This selects instances 1,2,3,4,12 from device DEV.

additional_parameter	R/W	Comma separated list of any parameter specific for this attribute if needed.
default_value	R/W	Defines the default value which is written to the actors upon system start until another value is written. When empty the value of 0 is used.
value_caching	R/W	When enabled the group target value is saved to local non volatile memory. Should the director restart, the cached values will be restored and send to the devices. This feature is useful to ensure uninterrupted operation even in the event of a system failure or to restore conditions after a power outage.
additional_script_name	R/W	When the actor group is updated, an additional script, defined here, can be executed to run time consuming functions outside of the standard processing loop. Usually, this field is left empty.
manual_set_value	X	This command permits setting of the group value manually bypassing the defined script logic. This is intended for testing only. Important: This manual setting always acts on priority level 8. Important: manual override will continue until manually released by setting ..manual_set_value = (type enter without a value).
sensor_group_config[DYNAMIC].		Defines a group of sensors that support the same attribute and whose data should be interpreted together.
group_name	R/W	Unique group name referenced by the director
attribute	R/W	The attribute which is configured. Locally, identical attributes of the associated devices listed below are grouped.
associated_devices	R/W	List of all sensors that supply information to a particular group. When an instance is used, here the syntax devicename.instance is used. Alternatively, a colon separator may be used instead of the dot. All records are comma separated. Instance ranges may be used: DEV.(1-4,12) This selects instances 1,2,3,4,12 from device DEV.
value_caching	R/W	When enabled the group target value is saved to local non volatile memory. Should the director restart, the cached values will be restored and send to the devices. This feature is useful to ensure uninterrupted operation even in the event of a system failure or to restore conditions after a power outage.

run_script_when	R/W	Defines how much the sensor group status needs to change in order to trigger the run of a script (and the optional additional_script). This also triggers MQTT and MODBUS activity. These protocols trigger at the same condition as the scripts when configured to send out sensor group changes. (The script names may be left empty if only MQTT is required for example). The parameter can be used to limit the number of script runs by not following little changes that lead to no effect. This filter is logically behind the sensor specific limits defined elsewhere in this table. When the sensor filter is setup well, then this filter here can be relaxed.
run_script_delta	R/W	Defines how much the value can deviate before a value change is reported automatically. Depending on the setting of the report_mode an absolute or a percent value is expected.
run_script_idle_time	R/W	When unequal to 0, the script and possible MQTT, MODBUS output are executed after the specified value in seconds. The time is restarted whenever the script is executed for whatever reason. This feature is useful to guarantee that a group update is executed even if the reported data never change.
script_name	R/W	When the group is updated and the required conditions are met, the script specified in this parameter is executed. If the parameter is left blank, the standard MS_SmartOfficeControl.ms script is executed. The specified script should not contain any time consuming functions. Syntax: = appname/ filename:subroutine The appname and subroutine name are optional. Without appname, the script must be located in xml_cli_scripts folder.
additional_script_name	R/W	When the group is updated and the required conditions are met and a script is defined here, this script is executed in the background after the standard processing for this group has taken place. An additional script, defined here, can be used to run time consuming functions outside of the standard processing loop. Usually, this field is left empty.
report_mode	R/W	This and the following six parameters act directly in the sensor device driver with the aim to minimize incoming traffic into the system right at the source. The report_mode acts in combination with the update_delta. Do not confuse these parameters with the run_script_.. parameter which act later in the processing chain after the sensor data are received.

additional_parameter	R/W	Optional, comma separated list of any parameter specific for the sensor (driver) that supports this attribute. Usually empty.
lower_boundary	R/W	When the measured value of any individual sensor is equal or below this value the sensor_list status is set to LOWER_LIMIT. The value is configured with a numerical value optionally followed by a unit. To eliminate superfluous events caused by slight variations of the sensor value, a hysteresis can be specified. The value will then return back to OK, only when the value rises again above the boundary + hysteresis. Syntax: boundary, hysteresis. Example: 12000mW,500mW
upper_boundary	R/W	When the measured value of any individual sensor is equal or above this value the sensor_list status is set to UPPER_LIMIT. The value is configured with a numerical value optionally followed by a unit. To eliminate superfluous events caused by slight variations of the sensor value, a hysteresis can be specified. The value will then return back to OK, only when the value decreases again below the boundary - hysteresis. Syntax: boundary, hysteresis. Example: 19.5C,1.5C
boundary_hysteresis	R/W	How much the value must return within bounds before the alarm condition is cleared. This value is no longer used as the hysteresis is now specified as second value of the boundary parameter.
update_delta	R/W	Defines how much the value can deviate before a value change is reported automatically. Depending on the setting of the report_mode an absolute or a percent value is expected. This value is used by sensor driver and limits inbound sensor traffic.
rate_limit	R/W	Defines how quickly the value is reported. Defined In units of 100ms. 0 means no rate limiting. This value is used by sensor driver and limits inbound sensor traffic.
clear_values	X	Clear status values for minimum_peak_hold and maximum_peak_hold of the associated sensor_group_status.
device_information[64].		Summarizes the most important inventory information of each detected device.
name	R	Unique name for reference. This is name of the base device.
hardware_id	R	A product specific hardware identification. May for example contain the MAC address.

device_type	R	Indicates if this is an actor or sensor device.
operational_state	R	Indicates the operational state of the device. Device (not attribute) specific errors will be indicated here.
actor_attributes	R	Lists which settable actor attributes are provided by this device.
sensor_attributes	R	Lists which readable sensor attributes are provided by this device.
vendor_name	R	Vendor or manufacturer name of the device.
article_number	R	This device article number.
serial_number	R	This device serial number.
hardware_revision	R	This device hardware version.
software_version	R	This device software / firmware version.
additional_info	R	Optional comma separated list of status fields specific for this type of device.
device_status[64].		Summarizes the most important status information of each detected device.
name	R	Unique name for reference. This is name of the base device.
temperature	R	Temperature value in centigrade. When several thermometers exist, the most severe value is shown. When no thermometer exists, 0 is displayed and climate_level indicates UNUSED.
climate_level	R	Annotated temperature level.
power_supply_status	R	Displays state of power supply
fan_status	R	Displays state of cooling fan. Indicates UNUSED in fanless devices.
actor_list[512].		This table lists all currently registered actors with all their attributes.
device	R	This is name of the base device which controls this actor. There may be several actor types (attributes) in the same device and these share the same name but use different attributes. There may also be several similar actor attributes. These are differentiated with the instance parameter.
instance	R	Describes a unique instance when several similar functional attributes are existing in the same device
attribute	R	The kind of function this actor is acting on
associated_groups	R	Indicates in which actor_groups this actor takes part.
value	R	The currently set value as text string followed by the unit such as mA or Lux.
actor_state	R	Indicates whether the indicated value was successfully written to the actual device.
creator	R	Indicates which subsystem created the actor entry.

last_update	R	Indicates the time when this record was last updated.
sensor_list[512].		This table lists all currently registered sensors with all their attributes.
device	R	This is name of the base device which controls this sensor. There may be several different sensor types (attributes) in the same device. These share the same name but use different attributes. There may also be several similar sensors in the device. These are differentiated with the instance parameter.
instance	R	Describes a unique instance when several similar functional attributes are existing in the same device
attribute	R	The kind of measurement this sensor is reporting.
associated_groups	R	Indicates in which sensor_groups this sensor takes part.
value	R	The last reported value as text string followed by the unit such as mA or Lux.
sensor_state	R	Indicates particular sensor states such hitting a boundary.
creator	R	Indicates which subsystem created the sensor entry.
last_update	R	Indicates the time when this record was last updated.
actor_group_status[128].		Calculated status of the defined actor groups. The listed value reflects the value all associated actors should use. The values update when an actor group is set by a script or manually.
group_name	R	This is name mirrors the actor_group_configuration.
attribute	R	The name of the controlled attribute.
num_assigned_actors	R	Number of actors that are configured for this group.
num_failed_actors	R	Number of actors that have not responded as expected.
group_state	R	
value	R	This value is set by the decision logic. May contain simple on,OFF or for example a sound file name
active_priority	R	Indicates which priority level is currently controlling the group value. Lower values have higher priority.
priority_value_chain	R	Displays the priority=value pairs of all currently defined priority levels. Relinquished priorities are not shown.
cache_status	R	Indicates if this group_status is saved even upon system power loss or reboot.
last_update	R	Indicates the time when this group status was last updated.

sensor_group_status[128].		Calculated status for all sensor groups. The sensor values of all contributing sensors are used to calculate min, max and average values. The values update each time a sensor reports changes.
group_name	R	This is name mirrors the sensor_group_configuration.
attribute	R	The name of the attribute measured. E.g. brightness, motion, switch.
num_assigned_sensors	R	Number of sensors that are configured for this group.
num_failed_sensors	R	Number of sensors that have not responded as expected.
group_state	R	Informes when not all sensors operate as expected.
minimum_peak_hold	R	Minimum value ever reported in this group since last value clear.
minimum_value	R	Minimum value out of all sensors that report to this group.
average_value	R	Average value out of all sensors that report to this group. Uses the number of reporting sensors to calculate the average. This field holds the group value when the group contains textual data.
maximum_value	R	Maximum value out of all sensors that report to this group.
maximum_peak_hold	R	Maximum value ever reported in this group since last value clear.
total_value	R	The total sum of all individual sensor values in this group.
lower_boundary_reached	R	Number of sensors that have reached their lower threshold. A value of 0 means no sensor has reached a lower boundary.
upper_boundary_reached	R	Number of sensors that have reached their upper threshold. A value of 0 means no sensor has reached an upper boundary.
updating_sensor_index	R	Indicates the index to the sensor_list which has caused the latest group update.
cache_status	R	Indicates if this attribute is saved even upon system power loss or reboot.
last_update	R	Indicates the time when this group status was last updated.

23.4 SmartOffice Configuration Parameters

Group Path	General Parameters
	Device.SmartOffice
enable_smart_office	<p>Generally enable the SmartOffice solution.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.1 (smartofficeEnableSmartOffice)</p>
Group Path	device_config , dynamical size
Description	<p>Device.SmartOffice.device_config</p> <p>Defines the configuration of each device under control. A device may contain one or more actor or sensor functions.</p>
device_name	<p>Unique group name referenced by the director. Important: For some devices further configuration options are available in the section Device.Controller. The name defined here must be identical to a name defined there to match the configuration options.</p> <p>Value String, max. 31 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.3.1.2 (deviceConfigDeviceName)</p>
location	<p>Free text to describe the position of the controller on the premises. This value need NOT be saved within the sensor itself.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.3.1.3 (deviceConfigLocation)</p>
latitude	<p>A value in degrees such as: 50,123</p> <p>Value String, max. 8 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.3.1.4 (deviceConfigLatitude)</p>
longitude	<p>A value in degrees such as: 50,123</p> <p>Value String, max. 8 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.3.1.5 (deviceConfigLongitude)</p>
altitude	<p>A value in meters.</p> <p>Value String, max. 8 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.3.1.6 (deviceConfigAltitude)</p>

placement	Information where to find the controller	
Values	<i>UNSET</i>	Undefined
	<i>FLOOR</i>	Device is placed on the floor or within a double floor
	<i>WALL</i>	Device is hanging on the wall
	<i>CEILING</i>	Device is placed on the ceiling or hanging from the ceiling
	<i>DUCT</i>	Device is placed in a cable duct
	<i>OUTSIDE</i>	Device is placed outside of the building
	<i>DESK</i>	Device is placed on or under a desk
OID	1.3.6.1.4.1.3181.10.6.1.99.3.1.7 (deviceConfigPlacement)	
product_type	The product type is used by the system to select the network protocol required to access the device. Note that for some devices a further configuration section exists under the Device.Controller section. Such additional config exists for type SMARTLIGHT_CONTROLLER and SMART_IO_CONTROLLER.	
Values	<i>VIRTUAL</i>	Software defined sensor without a physical presence
	<i>SMARTLIGHT_CONTROLLER</i>	SmartLight controller via IP
	<i>SMART_IO_CONTROLLER</i>	SmartIO controller via IP
	<i>HM</i>	HM wireless device via USB or Serial
	<i>FHEM</i>	Attached via internal FHEM server
	<i>IP500</i>	Attached via IP500 server
	<i>ENOCAN</i>	Attached via internal FHEM server
	<i>KNX</i>	Attached via IP500 server
	<i>CSLC_V2</i>	Central SmartLight Controller via IP with 4x 6 light ports (CSLC V2)
	<i>CSLC_24</i>	Central SmartLight Controller via IP with 24 light ports. (CSLC V4)
	<i>DIGITAL_IO_CONTROLLER</i>	Smart Digital IO controller via IP with only digital inputs and outputs
OID	1.3.6.1.4.1.3181.10.6.1.99.3.1.8 (deviceConfigProductType)	
device_id	Unique manufacturer dependent identifier of the device. For SmartLightController the MAC address of the controller is entered here.	
Value	String, max. 32 characters.	
OID	1.3.6.1.4.1.3181.10.6.1.99.3.1.9 (deviceConfigDeviceId)	
network_address	May be an IP or other type of address depending on the given network access method. Can be left blank for a SmartLightController.	
Value	String, max. 50 characters.	
OID	1.3.6.1.4.1.3181.10.6.1.99.3.1.10 (deviceConfigNetworkAddress)	

additional_parameter	Comma separated list of any parameter specific for this device. Example: panel=type A,refresh_rate=12 Value String, max. 512 characters. OID 1.3.6.1.4.1.3181.10.6.1.99.3.1.11 (deviceConfigAdditionalParameter)
network_failure_action	Defines what the actor does if the network connection fails or after reboot until communication is established. Values <i>KEEP_CURRENT</i> Light is kept in the current value <i>OFF</i> Light is switched off <i>ON</i> Light is 100% switched on <i>DIMMED</i> Light is set to the configured dim level OID 1.3.6.1.4.1.3181.10.6.1.99.3.1.12 (deviceConfigNetworkFailureAction)
identify	The actor will blink with its status led to signal its presence and physical location. Supply instance or 0 or nothing for all instances. Action Execute command with parameter string max. 8 characters. OID 1.3.6.1.4.1.3181.10.6.1.99.3.1.13 (deviceConfigIdentify)
restart	Restart the device. Action Execute command. OID 1.3.6.1.4.1.3181.10.6.1.99.3.1.14 (deviceConfigRestart)
calibrate	Start calibration process (if available for this actor type). Action Execute command with parameter string max. 8 characters. OID 1.3.6.1.4.1.3181.10.6.1.99.3.1.15 (deviceConfigCalibrate)
pair	Start pairing process that couples individual device to this director. Action Execute command. OID 1.3.6.1.4.1.3181.10.6.1.99.3.1.16 (deviceConfigPair)
unpair	Discard existing pairing between an individual device and this director. Action Execute command. OID 1.3.6.1.4.1.3181.10.6.1.99.3.1.17 (deviceConfigUnpair)
update_firmware	Update the device firmware. When no file name is supplied, the latest version is automatically selected. Alternatively, a specific file name can be supplied to use another version. Use Management.files.firmware.display_files to view a list of available files under the SLC section. (applies to SmartLight Controllers) Action Execute command with parameter string max. 128 characters. OID 1.3.6.1.4.1.3181.10.6.1.99.3.1.18 (deviceConfigUpdateFirmware)

Group	actor_group_config , dynamical size
Path	Device.SmartOffice.actor_group_config
Description	Defines a group of actors that support the same attribute and which shall be set together to the same value.
group_name	<p>Unique group name referenced by the director</p> <p>Value String, max. 31 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.4.1.2 (actorGroupConfigGroupName)</p>
attribute	<p>The attribute which is configured. Locally, identical attributes of the associated devices listed below are grouped.</p> <p>Value String, max. 31 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.4.1.3 (actorGroupConfigAttribute)</p>
associated_devices	<p>List of all actors that supply information to a particular group. When an instance is used, here the syntax devicename.instance is used. Alternatively, a colon separator may be used instead of the dot. All records are comma separated. Instance ranges may be used: DEV.(1-4,12) This selects instances 1,2,3,4,12 from device DEV.</p> <p>Value String, max. 512 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.4.1.4 (actorGroupConfigAssociatedDevices)</p>
additional_parameter	<p>Comma separated list of any parameter specific for this attribute if needed.</p> <p>Value String, max. 512 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.4.1.5 (actorGroupConfigAdditionalParameter)</p>
default_value	<p>Defines the default value which is written to the actors upon system start until another value is written. When empty the value of 0 is used.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.4.1.6 (actorGroupConfigDefaultValue)</p>
value_caching	<p>When enabled the group target value is saved to local non volatile memory. Should the director restart, the cached values will be restored and send to the devices. This feature is useful to ensure uninterrupted operation even in the event of a system failure or to restore conditions after a power outage. ATTENTION: Not implemented.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.4.1.7 (actorGroupConfigValueCaching)</p>

additional_script_name	<p>When the actor group is updated, an additional script, defined here, can be executed to run time consuming functions outside of the standard processing loop. Usually, this field is left empty.</p> <p>Value String, max. 63 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.4.1.8 (actorGroupConfigAdditionalScriptName)</p>
manual_set_value	<p>This command permits setting of the group value manually bypassing the defined script logic. This is intended for testing only. Important: This manual setting always acts on priority level 8. Important: manual override will continue until manually released by setting ..manual_set_value = (type enter without a value).</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.4.1.9 (actorGroupConfigManualSetValue)</p>
<p>Group</p> <p>Path</p> <p>Description</p>	<p>sensor_group_config, dynamical size</p> <p>Device.SmartOffice.sensor_group_config</p> <p>Defines a group of sensors that support the same attribute and whose data should be interpreted together.</p>
group_name	<p>Unique group name referenced by the director</p> <p>Value String, max. 31 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.5.1.2 (sensorGroupConfigGroupName)</p>
attribute	<p>The attribute which is configured. Locally, identical attributes of the associated devices listed below are grouped.</p> <p>Value String, max. 31 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.5.1.3 (sensorGroupConfigAttribute)</p>
associated_devices	<p>List of all sensors that supply information to a particular group. When an instance is used, here the syntax devicename.instance is used. Alternatively, a colon separator may be used instead of the dot. All records are comma separated. Instance ranges may be used: DEV.(1-4,12) This selects instances 1,2,3,4,12 from device DEV.</p> <p>Value String, max. 512 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.5.1.4 (sensorGroupConfigAssociatedDevices)</p>

value_caching	<p>When enabled the group target value is saved to local non volatile memory. Should the director restart, the cached values will be restored and send to the devices. This feature is useful to ensure uninterrupted operation even in the event of a system failure or to restore conditions after a power outage. ATTENTION: Not implemented.</p>
Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.1.99.5.1.5 (sensorGroupConfigValueCaching)

run_script_when

Defines how much the sensor group status needs to change in order to trigger the run of a script (and the optional additional_script). This also triggers MQTT and MODBUS activity. These protocols trigger at the same condition as the scripts when configured to send out sensor group changes. (The script names may be left empty if only MQTT is required for example). The parameter can be used to limit the number of script runs by not following little changes that lead to no effect. This filter is logically behind the sensor specific limits defined elsewhere in this table. When the sensor filter is setup well, then this filter here can be relaxed.

Values	<i>DISABLED</i>	This group does not request a script run. The group value is still updated and available for read
	<i>ANY_CHANGE</i>	Any change of a group value will trigger a script run. No filter is active. This is useful for digital inputs but usually not recommendable for analog signals with lots of small variations.
	<i>LIMIT_CROSSED</i>	The script will run whenever at least one sensor in the group will reach a limit (LOWER_LIMIT or UPPER_LIMIT) and also when no sensor reports a limit, while the limit was reached before. Refer to lower_boundary parameter for additional details.
	<i>AVG_ABSOLUTE</i>	The script will trigger only on changes of the average value. The value must deviate from the last reported value by the absolute value defined for run_script_delta. Note that some sensors indicate intermediate steps even when a large change of the measured value is expected. In such cases delta between evaluations may be smaller than expected and the trigger may not fire if the run_script_delta value is too large.
	<i>AVG_PERCENT</i>	The script will trigger only on changes of the average value. The value must deviate from the last reported value by the percentage value defined for run_script_delta. Also see comment for AVG_ABSOLUTE.
	<i>TOTAL_ABSOLUTE</i>	The script will trigger only on changes of the total value. The value must deviate from the last reported value by the absolute value defined for run_script_delta. Note that some sensors indicate intermediate steps even when a large change of the measured value is expected. In such cases delta between evaluations may be smaller than expected and the trigger may not fire if the run_script_delta value is too large.
	<i>TOTAL_PERCENT</i>	The script will trigger only on changes of the total value. The value must deviate from the last reported value by the percentage value defined for run_script_delta. Also see comment for TOTAL_ABSOLUTE.
	<i>NEW_PEAK_LEVEL</i>	The script will run when a new peak level is detected. This applies to lower and upper peak level. When the peak level is manually reset, the script will not immediately execute, but will on the next update of the group data.
	<i>ANY_UPDATE</i>	Like ANY_CHANGE but even updates if no values have changed as result of new sensor reports. This setting can cause significant system load depending on the update frequency of the sensor.

	<p><i>ZERO_CROSSING</i> The script will trigger on change from zero to any other value and from any value to zero. It will not trigger when the average value changes between different non zero values.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.5.1.6 (sensorGroupConfigRunScriptWhen)</p>
run_script_delta	<p>Defines how much the value can deviate before a value change is reported automatically. Depending on the setting of the report_mode an absolute or a percent value is expected.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.5.1.7 (sensorGroupConfigRunScriptDelta)</p>
run_script_idle_time	<p>When unequal to 0, the script and possible MQTT, MODBUS output are executed after the specified value in seconds. The time is restarted whenever the script is executed for whatever reason. This feature is useful to guarantee that a group update is executed even if the reported data never change.</p> <p>Value Number in range 0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.5.1.8 (sensorGroupConfigRunScriptIdleTime)</p>
script_name	<p>When the group is updated and the required conditions are met, the script specified in this parameter is executed. If the parameter is left blank, the standard MS_SmartOfficeControl.ms script is executed. The specified script should not contain any time consuming functions. Syntax: = appname/ filename:subroutine The appname and subroutine name are optional. Without appname, the script must be located in xml_cli_scripts folder.</p> <p>Value String, max. 63 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.5.1.9 (sensorGroupConfigScriptName)</p>
additional_script_name	<p>When the group is updated and the required conditions are met and a script is defined here, this script is executed in the background after the standard processing for this group has taken place. An additional script, defined here, can be used to run time consuming functions outside of the standard processing loop. Usually, this field is left empty.</p> <p>Value String, max. 63 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.5.1.10 (sensorGroupConfigAdditionalScriptName)</p>

report_mode	<p>This and the following six parameters act directly in the sensor device driver with the aim to minimize incoming traffic into the system right at the source. The report_mode acts in combination with the update_delta. Do not confuse these parameters with the run_script... parameter which act later in the processing chain after the sensor data are received.</p>												
Values	<table> <tr> <td data-bbox="730 409 845 439"><i>DISABLED</i></td><td data-bbox="954 409 1434 472">This sensor does not transmit any information on its own</td></tr> <tr> <td data-bbox="730 477 829 506"><i>PASSIVE</i></td><td data-bbox="954 477 1434 539">The sensor can be polled but does not generate messages on its own</td></tr> <tr> <td data-bbox="730 544 917 573"><i>DELTA_PERCENT</i></td><td data-bbox="954 544 1434 651">The sensor can be polled and also generates status updates when its value changes for at least the percentage defined for the update_delta value</td></tr> <tr> <td data-bbox="730 656 933 685"><i>DELTA_ABSOLUTE</i></td><td data-bbox="954 656 1434 763">The sensor can be polled and also generates status updates its absolute value changes for more then defined for the update_delta</td></tr> <tr> <td data-bbox="730 768 917 797"><i>ON_THRESHOLD</i></td><td data-bbox="954 768 1434 853">The sensor can be polled and also generates status updates when the lower or upper boundary is crossed</td></tr> <tr> <td data-bbox="730 857 790 887"><i>TEST</i></td><td data-bbox="954 857 1434 943">In test mode the sensor may generate test data output independent of the actual sensor data values</td></tr> </table>	<i>DISABLED</i>	This sensor does not transmit any information on its own	<i>PASSIVE</i>	The sensor can be polled but does not generate messages on its own	<i>DELTA_PERCENT</i>	The sensor can be polled and also generates status updates when its value changes for at least the percentage defined for the update_delta value	<i>DELTA_ABSOLUTE</i>	The sensor can be polled and also generates status updates its absolute value changes for more then defined for the update_delta	<i>ON_THRESHOLD</i>	The sensor can be polled and also generates status updates when the lower or upper boundary is crossed	<i>TEST</i>	In test mode the sensor may generate test data output independent of the actual sensor data values
<i>DISABLED</i>	This sensor does not transmit any information on its own												
<i>PASSIVE</i>	The sensor can be polled but does not generate messages on its own												
<i>DELTA_PERCENT</i>	The sensor can be polled and also generates status updates when its value changes for at least the percentage defined for the update_delta value												
<i>DELTA_ABSOLUTE</i>	The sensor can be polled and also generates status updates its absolute value changes for more then defined for the update_delta												
<i>ON_THRESHOLD</i>	The sensor can be polled and also generates status updates when the lower or upper boundary is crossed												
<i>TEST</i>	In test mode the sensor may generate test data output independent of the actual sensor data values												
OID	1.3.6.1.4.1.3181.10.6.1.99.5.1.11 (sensorGroupConfigReportMode)												
additional_parameter	<p>Optional, comma separated list of any parameter specific for the sensor (driver) that supports this attribute. Usually empty.</p>												
Value	String, max. 512 characters.												
OID	1.3.6.1.4.1.3181.10.6.1.99.5.1.12 (sensorGroupConfigAdditionalParameter)												
lower_boundary	<p>When the measured value of any individual sensor is equal or below this value the sensor_list status is set to LOWER_LIMIT. The value is configured with a numerical value optionally followed by a unit. To eliminate superfluous events caused by slight variations of the sensor value, a hysteresis can be specified. The value will then return back to OK, only when the value rises again above the boundary + hysteresis. Syntax: boundary, hysteresis. Example: 12000mW,500mW</p>												
Value	String, max. 32 characters.												
OID	1.3.6.1.4.1.3181.10.6.1.99.5.1.13 (sensorGroupConfigLowerBoundary)												
upper_boundary	<p>When the measured value of any individual sensor is equal or above this value the sensor_list status is set to UPPER_LIMIT. The value is configured with a numerical value optionally followed by a unit. To eliminate superfluous events caused by slight variations of the sensor value, a hysteresis can be specified. The value will then return back to OK, only when the value decreases again below the boundary - hysteresis. Syntax: boundary, hysteresis. Example: 19.5C,1.5C</p>												
Value	String, max. 32 characters.												
OID	1.3.6.1.4.1.3181.10.6.1.99.5.1.14 (sensorGroupConfigUpperBoundary)												

boundary_hysteresis	<p>How much the value must return within bounds before the alarm condition is cleared. This value is no longer used as the hysteresis is now specified as second value of the boundary parameter.</p>
Values	<p><i>NONE</i> No hysteresis applies</p> <p><i>LOW</i> A low hysteresis applies. The value reacts more quickly but is more prone to oscillating. The actual hysteresis depends on the configured update delta value.</p> <p><i>HIGH</i> A higher hysteresis applies. The value need to change more before they are reported but oscillating is safely prevented. The actual hysteresis depends on the configured update delta value.</p>
OID	<p>1.3.6.1.4.1.3181.10.6.1.99.5.1.15 (sensorGroupConfigBoundaryHysteresis)</p>
update_delta	<p>Defines how much the value can deviate before a value change is reported automatically. Depending on the setting of the report_mode an absolute or a percent value is expected. This value is used by sensor driver and limits inbound sensor traffic.</p>
Value	String, max. 32 characters.
OID	<p>1.3.6.1.4.1.3181.10.6.1.99.5.1.16 (sensorGroupConfigUpdateDelta)</p>
rate_limit	<p>Defines how quickly the value is reported. Defined In units of 100ms. 0 means no rate limiting. This value is used by sensor driver and limits inbound sensor traffic.</p>
Value	Number in range 0-0xFFFFFFFF
OID	<p>1.3.6.1.4.1.3181.10.6.1.99.5.1.17 (sensorGroupConfigRateLimit)</p>
clear_values	<p>Clear status values for minimum_peak_hold and maximum_peak_hold of the associated sensor_group_status.</p>
Action	Execute command.
OID	<p>1.3.6.1.4.1.3181.10.6.1.99.5.1.18 (sensorGroupConfigClearValues)</p>
Group Path Description	
director_config Device.SmartOffice.director_config General configuration of the director.	
domain_name	<p>Value String, max. 16 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.99.2.1.2 (directorConfigDomainName)</p>

general_mode

Values	<i>DISABLED</i>	The director will not perform any SmartOffice operation
	<i>AUTOMATIC</i>	The director will automatically perform according to the configuration and scripts as defined. Normal mode.
	<i>PASSIVE</i>	The director will process sensor information but will not update actor settings regardless of any script definitions.
OID	1.3.6.1.4.1.3181.10.6.1.99.2.1.3 (directorConfigGeneralMode)	

act_on_ungrouped_sensors

When set any sensor attributes which are not configured to be part of a sensor group, will also trigger the regular script execution. This may be selected in smaller setups to save the effort of defining groups. Note that no event rate limiting can be applied to ungrouped sensors and thus using this mode can result in overloading the system leading to sluggish response times.

Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.1.99.2.1.4 (directorConfigActOnUngroupedSensors)

scan_filter

The scan filter may be used to limit the displayed output when applying the scan_light_controllers action.

Values	<i>ALL</i>	Display all detected controllers. The filter is off.
	<i>LOCAL</i>	Display all detected controllers connected to the local device.
	<i>PAIRED</i>	Display all detected controllers paired to any device.
	<i>UNPAIRED</i>	Display all detected controllers not paired to any device.
	<i>SLC</i>	Display all detected smart light controllers
	<i>CSLC</i>	Display all detected central smart light controllers
	<i>SIOC</i>	Display all detected smart i/o controllers
	<i>ZLC</i>	Display all detected zone light controllers
OID	1.3.6.1.4.1.3181.10.6.1.99.2.1.5 (directorConfigScanFilter)	

scan_light_controllers

Scan the local network for reachable SmartLightController and display a list. The scan_filter parameter is applied.

Action	Execute command.
OID	1.3.6.1.4.1.3181.10.6.1.99.2.1.6 (directorConfigScanLightControllers)

23.5 SmartOffice Status Parameters

24 SmartOffice Controller

24.1 Key Features

Smart Light Controller

Above the standard device setup in the SmartOffice section, it is possible to configure more details and features via a specific set of parameters.

Smart IO Controller

The Smart I/O Controller offers a host of digital and analog interfaces which need to be configured. By setting an attribute the I/O channels are linked to SmartOffice sensor and actor groups.

CSLC

The Central SmartLight Controller (CSLC) offers 24 LED ports in a single high density 1U enclosure. The G6 firmware also runs on the CSLC hardware.

The CSLC is a high density LED controller for SmartOffice applications. Standard twisted pair cabling is used to connect up to 24 LED panels.

24.2 Functional Description

Preface

In the Controller section hardware device controller specific configuration options are grouped. These are SmartOffice related controller devices for which a more elaborate configuration is required than that provided under the normal SmartOffice device configuration section. Devices like the SmartLight Controller or the Smart I/O Controller can be configured in this section. Additional similar controllers might be added in future releases.

24.3 Controller CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Device.	controller.		SmartOffice Controller specific parameter			
			smartlight_config[DYNAMIC].			
			name	R/W		Unique name must precisely match the device name specified under Device.SmartOffice.device_config.device_name for a device of product_type = SMARTLIGHT_CONTROLLER.
			type	R/W		Flags if RADIUS or TACACS+ is specified in this entry.
			max_source_power	R/W		Defines the maximum electrical power in W that can be consumed from the attached PoE source.
			max_panel_power	R/W		Defines the maximum electrical power in W that is delivered to the attached light.
			manual_get_input	X		May be used to manually read an input value. Syntax example: manual_get_input = ain2 [R]. Append R or raw for unprocessed value. Otherwise the scaled input is displayed.
			manual_set_output	X		May be used to manually force an output value. Syntax example: manual_set_output = aout1 50 [raw]. Append raw if the value should be treated as a raw, unscaled value.
			read_command	X		May be used to manually read an internal controller value. Syntax: read_command = parameter.
			write_command	X		May be used to manually write an internal controller value. Syntax: write_command = parameter value.
			smart_io_config[DYNAMIC].			
			name	R/W		Unique name must precisely match the device name specified under Device.SmartOffice.device_config.device_name for a device of product_type = SMART_IO_CONTROLLER.
			pt1_attribute	R/W		This defines the attribute with which it will register the PT1 temperature sensor to the system.
			pt1_sensor_type	R/W		Defines the sensor connected to PT1 input.
			pt1_filter_time	R/W		Time in seconds used to average out the value.

pt1_transformation	R/W	May be used to transform the input value to another format. Example C to F: $=(\$*1.8)+32$. Use # to append a unit to the value. May also be used for further linearization of the value. Annotation example: [0=\$# (freezing),]40=\$# (too hot), =\$
pt2_attribute	R/W	This defines the attribute with which it will register the PT2 temperature sensor to the system.
pt2_sensor_type	R/W	Defines the sensor connected to PT2 input.
pt2_filter_time	R/W	Time in seconds used to average out the value.
pt2_transformation	R/W	May be used to transform the input value to another format. Example C to F: $=(\$*1.8)+32$. Use # to append a unit to the value. May also be used for further linearization of the value. Annotation example: [0=\$# (freezing),]40=\$# (too hot), =\$
ain1_attribute	R/W	This defines the attribute with which it will register the analog input 1 to the system.
ain1_sensor_type	R/W	Defines the sensor connected to the analog input 1.
ain1_raw_min	R/W	Defines the lowest raw value data point.
ain1_raw_max	R/W	Defines the highest raw value data point.
ain1_scaled_min	R/W	Defines the lower scaled value at the lower raw value data point.
ain1_scaled_max	R/W	Defines the scaled value at the max raw value data point.
ain1_filter_time	R/W	Time in seconds used to average out the value.
ain1_update_delta	R/W	Defines how much the input value can deviate before a value change is reported. An absolute or a percent value is expected. An optional minimum update period in seconds can be defined as well. Syntax: delta, time. Example: 5%,60s
ain1_transformation	R/W	May be used to transform the input value to another format. Syntax: value=text, value=text,... Or calculations: $=\$*10$ Example C to F: $=(\$*1.8)+32$. Use # to append a unit to the value. Also in combination with calculation like: $\$/1000\#mW$. For more options please refer to separate documentation.
ain2_attribute	R/W	This defines the attribute with which it will register the analog input 2 to the system.
ain2_sensor_type	R/W	Defines the sensor connected to the analog input 2.
ain2_raw_min	R/W	Defines the lowest raw value data point.
ain2_raw_max	R/W	Defines the highest raw value data point.
ain2_scaled_min	R/W	Defines the lower scaled value at the lower raw value data point.
ain2_scaled_max	R/W	Defines the scaled value at the max raw value data point.
ain2_filter_time	R/W	Time in seconds used to average out the value.

ain2_update_delta	R/W	Defines how much the input value can deviate before a value change is reported. An absolute or a percent value is expected. An absolute or a percent value is expected. An optional minimum update period in seconds can be defined as well. Syntax: delta, time. Example: 10,3600 (update at least once an hour)
ain2_transformation	R/W	May be used to transform the input value to another format. Syntax: value=text, value=text,.. Or calculations: =\$*10 Example C to F: =(\$*1.8)+32. Use # to append a unit to the value. Also in combination with calculation like: \$/1000#mW. For more options please refer to separate documentation.
ain3_attribute	R/W	This defines the attribute with which it will register the analog input 3 to the system.
ain3_sensor_type	R/W	Defines the sensor connected to the analog input 3.
ain3_raw_min	R/W	Defines the lowest raw value data point.
ain3_raw_max	R/W	Defines the highest raw value data point.
ain3_scaled_min	R/W	Defines the lower scaled value at the lower raw value data point.
ain3_scaled_max	R/W	Defines the scaled value at the max raw value data point.
ain3_filter_time	R/W	Time in seconds used to average out the value.
ain3_update_delta	R/W	Defines how much the input value can deviate before a value change is reported. An absolute or a percent value is expected. An absolute or a percent value is expected. An optional minimum update period in seconds can be defined as well. Syntax: delta, time. Example: 5%,60s
ain3_transformation	R/W	May be used to transform the input value to another format. Syntax: value=text, value=text,.. Or calculations: =\$*10 Example C to F: =(\$*1.8)+32. Use # to append a unit to the value. Also in combination with calculation like: \$/1000#mW. For more options please refer to separate documentation.
ain4_attribute	R/W	This defines the attribute with which it will register the analog input 4 to the system.
ain4_sensor_type	R/W	Defines the sensor connected to the analog input 4.
ain4_raw_min	R/W	Defines the lowest raw value data point.
ain4_raw_max	R/W	Defines the highest raw value data point.
ain4_scaled_min	R/W	Defines the lower scaled value at the lower raw value data point.
ain4_scaled_max	R/W	Defines the scaled value at the max raw value data point.
ain4_filter_time	R/W	Time in seconds used to average out the value.

ain4_update_delta	R/W	Defines how much the input value can deviate before a value change is reported. An absolute or a percent value is expected. An absolute or a percent value is expected. An optional minimum update period in seconds can be defined as well. Syntax: delta, time. Example: 15%,5s
ain4_transformation	R/W	May be used to transform the input value to another format. Syntax: value=text, value=text,.. Or calculations: =\$*10 Example C to F: =(\$*1.8)+32. Use # to append a unit to the value. Also in combination with calculation like: \$/1000#mW. For more options please refer to separate documentation.
din_idle_time	R/W	When unequal to 0, the value of the digital inputs is reported after the specified value in seconds. The time is restarted whenever a digital value is otherwise reported. This feature is useful to guarantee that a group update is executed even if the reported data never change.
din1_mode	R/W	Used to enable the digital input 1.
din1_attribute	R/W	This defines the attribute with which it will register the digital input 1 to the system. If left blank, the digital input is not reported (disabled).
din1_transformation	R/W	May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.
din2_mode	R/W	Used to enable the digital input 2.
din2_attribute	R/W	This defines the attribute with which it will register the digital input 2 to the system. If left blank, the digital input is not reported (disabled).
din2_transformation	R/W	May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.
din3_mode	R/W	Used to enable the digital input 3.
din3_attribute	R/W	This defines the attribute with which it will register the digital input 3 to the system. If left blank, the digital input is not reported (disabled).
din3_transformation	R/W	May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.
din4_mode	R/W	Used to enable the digital input 4.
din4_attribute	R/W	This defines the attribute with which it will register the digital input 4 to the system. If left blank, the digital input is not reported (disabled).
din4_transformation	R/W	May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.

about1_attribute	R/W	This defines the attribute with which it will register the analog output 1 to the system. If left blank, this analog output cannot not be used.
about1_mode	R/W	Defines the output mode of digital output 1.
about1_transformation	R/W	May be used to transform a possible non compliant output value (of the actor group) into a compliant value. Note this transformation takes place before the scaling parameter are applied. Syntax: text=value, text=value,.. Or calculations like: =\$/1000 For more options please refer to separate documentation.
about1_raw_min	R/W	Defines the lowest raw value data point.
about1_raw_max	R/W	Defines the highest raw value data point.
about1_scaled_min	R/W	Defines the lower scaled value at the lower raw value data point.
about1_scaled_max	R/W	Defines the scaled value at the max raw value data point.
about2_attribute	R/W	This defines the attribute with which it will register the analog output 2 to the system. If left blank, this analog output cannot not be used.
about2_mode	R/W	Defines the output mode of digital output 1.
about2_transformation	R/W	May be used to transform a possible non compliant output value (of the actor group) into a compliant value. Note this transformation takes place before the scaling parameter are applied. Syntax: text=value, text=value,.. Or calculations like: =\$/1000 For more options please refer to separate documentation.
about2_raw_min	R/W	Defines the lowest raw value data point.
about2_raw_max	R/W	Defines the highest raw value data point.
about2_scaled_min	R/W	Defines the lower scaled value at the lower raw value data point.
about2_scaled_max	R/W	Defines the scaled value at the max raw value data point.
dout1_attribute	R/W	This defines the attribute with which it will register the digital output 1 to the system. If left blank, the digital input cannot not be used.
dout1_mode	R/W	Defines the output mode of digital output 1.
dout1_pwm_frequency	R/W	When PWM mode is selected, this parameter defines the PWM frequency in Hz.
dout1_transformation	R/W	May be used to transform a textual input to acceptable digital values. Example: OFF=0, ON=1. Or to accept other numeric ranges: 0=0,100=1.
dout2_attribute	R/W	This defines the attribute with which it will register the digital output 2 to the system. If left blank, the digital input cannot not be used.
dout2_mode	R/W	Defines the output mode of digital output 2.
dout2_pwm_frequency	R/W	When PWM mode is selected, this parameter defines the PWM frequency in Hz.

dout2_transformation	R/W	May be used to transform a textual input to acceptable digital values. Example: OFF=0, ON=1. Or to accept other numeric ranges: 0=0,100=1.
controller_mode	R/W	When set to other then normal additional test or debug information are provided.
manual_get_input	X	May be used to manually read an input value. Syntax example: manual_get_input = ain2 [R]. Append R or raw for unprocessed value. Otherwise the scaled input is displayed.
manual_set_output	X	May be used to manually force an output value. Syntax example: manual_set_output = aout1 50 [raw]. Append raw if the value should be treated as a raw, unscaled value.
read_command	X	May be used to manually read an internal controller value. Syntax: read_command = parameter.
write_command	X	May be used to manually write an internal controller value. Syntax: write_command = parameter value.
smart_digital_io_config[DYNAMIC].		Add elements as required for the number of used controllers of this type.
name	R/W	Unique name must precisely match the device name specified under Device.SmartOffice.device_config.device_name for a device of product_type = SMART_IO_CONTROLLER.
din_idle_time	R/W	When unequal to 0, the value of the digital inputs is reported after the specified value in seconds. The time is restarted whenever a digital value is otherwise reported. This feature is useful to guarantee that a group update is executed even if the reported data never change.
din1_mode	R/W	Used to enable the digital input 1.
din1_attribute	R/W	This defines the attribute with which it will register the input to the system.
din1_transformation	R/W	May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.
din2_mode	R/W	Used to enable the digital input 2.
din2_attribute	R/W	This defines the attribute with which it will register the input to the system.
din2_transformation	R/W	May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.
din3_mode	R/W	Used to enable the digital input 3.
din3_attribute	R/W	This defines the attribute with which it will register the input to the system.
din3_transformation	R/W	May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.
din4_mode	R/W	Used to enable the digital input 4.
din4_attribute	R/W	This defines the attribute with which it will register the input to the system.

din4_transformation	R/W	May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.
din5_mode	R/W	Used to enable the digital input 5.
din5_attribute	R/W	This defines the attribute with which it will register the input to the system.
din5_transformation	R/W	May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.
din6_mode	R/W	Used to enable the digital input 6.
din6_attribute	R/W	This defines the attribute with which it will register the input to the system.
din6_transformation	R/W	May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.
din7_mode	R/W	Used to enable the digital input 7.
din7_attribute	R/W	This defines the attribute with which it will register the input to the system.
din7_transformation	R/W	May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.
din8_mode	R/W	Used to enable the digital input 8.
din8_attribute	R/W	This defines the attribute with which it will register the input to the system.
din8_transformation	R/W	May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.
din9_mode	R/W	Used to enable the digital input 9.
din9_attribute	R/W	This defines the attribute with which it will register the input to the system.
din9_transformation	R/W	May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.
din10_mode	R/W	Used to enable the digital input 10.
din10_attribute	R/W	This defines the attribute with which it will register the input to the system.
din10_transformation	R/W	May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.
dout1_mode	R/W	Used to enable digital output 1.
dout1_attribute	R/W	Defines the attribute with which this digital output registered in the system.
dout1_transformation	R/W	May be used to transform a textual input to acceptable digital values. Example: OFF=0, ON=1. Or to accept other numeric ranges: 0=0,100=1.
dout2_mode	R/W	Used to enable digital output 2.
dout2_attribute	R/W	Defines the attribute with which this digital output registered in the system.

dout2_transformation	R/W	May be used to transform a textual input to acceptable digital values. Example: OFF=0, ON=1. Or to accept other numeric ranges: 0=0,100=1.
dout3_mode	R/W	Used to enable digital output 3.
dout3_attribute	R/W	Defines the attribute with which this digital output registered in the system.
dout3_transformation	R/W	May be used to transform a textual input to acceptable digital values. Example: OFF=0, ON=1. Or to accept other numeric ranges: 0=0,100=1.
dout4_mode	R/W	Used to enable digital output 4.
dout4_attribute	R/W	Defines the attribute with which this digital output registered in the system.
dout4_transformation	R/W	May be used to transform a textual input to acceptable digital values. Example: OFF=0, ON=1. Or to accept other numeric ranges: 0=0,100=1.
dout5_mode	R/W	Used to enable digital output 5.
dout5_attribute	R/W	Defines the attribute with which this digital output registered in the system.
dout5_transformation	R/W	May be used to transform a textual input to acceptable digital values. Example: OFF=0, ON=1. Or to accept other numeric ranges: 0=0,100=1.
dout6_mode	R/W	Used to enable digital output 6.
dout6_attribute	R/W	Defines the attribute with which this digital output registered in the system.
dout6_transformation	R/W	May be used to transform a textual input to acceptable digital values. Example: OFF=0, ON=1. Or to accept other numeric ranges: 0=0,100=1.
dout7_mode	R/W	Used to enable digital output 7.
dout7_attribute	R/W	Defines the attribute with which this digital output registered in the system.
dout7_transformation	R/W	May be used to transform a textual input to acceptable digital values. Example: OFF=0, ON=1. Or to accept other numeric ranges: 0=0,100=1.
dout8_mode	R/W	Used to enable digital output 8.
dout8_attribute	R/W	Defines the attribute with which this digital output registered in the system.
dout8_transformation	R/W	May be used to transform a textual input to acceptable digital values. Example: OFF=0, ON=1. Or to accept other numeric ranges: 0=0,100=1.
controller_mode	R/W	When set to other then normal additional test or debug information are provided.
manual_get_value	X	May be used to manually read an input value. Syntax example: manual_get_input = din2 [R]. Append R or raw for unprocessed value. Otherwise the transformed input is displayed.
manual_set_value	X	May be used to manually force an output value. Syntax example: manual_set_output = dout1 1.

read_command	X	May be used to manually read an internal controller value. Syntax: read_command = parameter.
write_command	X	May be used to manually write an internal controller value. Syntax: write_command = parameter value.
cslc_config[DYNAMIC].		Add elements as required for the number of used controllers of this type.
name	R/W	Unique name must precisely match the device name specified under Device.SmartOffice.device_config.device_name for a device of product_type = SMARTLIGHT_CONTROLLER.
read_command	X	May be used to manually read an internal controller value. Syntax: read_command = parameter.
write_command	X	May be used to manually write an internal controller value. Syntax: write_command = parameter value.
cslc24_config[DYNAMIC].		Add elements as required for the number of used controllers of this type.
name	R/W	Unique name must precisely match the device name specified under Device.SmartOffice.device_config.device_name for a device of product_type = SMARTLIGHT_CONTROLLER.
read_command	X	May be used to manually read an internal controller value. Syntax: read_command = parameter.
write_command	X	May be used to manually write an internal controller value. Syntax: write_command = parameter value.

24.4 Controller Configuration Parameters

Group	smartlight_config , dynamical size	
Path	Device.Controller.smartlight_config	
Description	Add elements as required for the number of used controllers of this type.	
name	Unique name must precisely match the device name specified under Device.SmartOffice.device_config.device_name for a device of product_type = SMARTLIGHT_CONTROLLER.	
	Value	String, max. 31 characters.
	OID	1.3.6.1.4.1.3181.10.6.1.106.1.1.2 (smartlightConfigName)
type	Flags if RADIUS or TACACS+ is specified in this entry.	
	Values	VERSION_1 Can be recognized by its white boxy housing VERSION_2 Can be recognized by its flat bare metal enclosure
	OID	1.3.6.1.4.1.3181.10.6.1.106.1.1.3 (smartlightConfigType)
max_source_power	Defines the maximum electrical power in W that can be consumed from the attached PoE source.	
	Value	Number in range 0-40
	OID	1.3.6.1.4.1.3181.10.6.1.106.1.1.4 (smartlightConfigMaxSourcePower)
max_panel_power	Defines the maximum electrical power in W that is delivered to the attached light.	
	Value	Number in range 0-40
	OID	1.3.6.1.4.1.3181.10.6.1.106.1.1.5 (smartlightConfigMaxPanelPower)
manual_get_input	May be used to manually read an input value. Syntax example: manual_get_input = ain2 [R]. Append R or raw for unprocessed value. Otherwise the scaled input is displayed.	
	Action	Execute command with parameter string max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.1.106.1.1.6 (smartlightConfigManualGetInput)
manual_set_output	May be used to manually force an output value. Syntax example: manual_set_output = aout1 50 [raw]. Append raw if the value should be treated as a raw, unscaled value.	
	Action	Execute command with parameter string max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.1.106.1.1.7 (smartlightConfigManualSetOutput)

read_command	May be used to manually read an internal controller value. Syntax: read_command = parameter.										
Action	Execute command with parameter string max. 32 characters.										
OID	1.3.6.1.4.1.3181.10.6.1.106.1.1.8 (smartlightConfigReadCommand)										
write_command	May be used to manually write an internal controller value. Syntax: write_command = parameter value.										
Action	Execute command with parameter string max. 128 characters.										
OID	1.3.6.1.4.1.3181.10.6.1.106.1.1.9 (smartlightConfigWriteCommand)										
Group	smart_io_config , dynamical size										
Path	Device.Controller.smart_io_config										
Description	Add elements as required for the number of used controllers of this type.										
name	Unique name must precisely match the device name specified under Device.SmartOffice.device_config.device_name for a device of product_type = SMART_IO_CONTROLLER.										
Value	String, max. 31 characters.										
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.2 (smartIoConfigName)										
pt1_attribute	This defines the attribute with which it will register the PT1 temperature sensor to the system.										
Value	String, max. 32 characters.										
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.3 (smartIoConfigPt1Attribute)										
pt1_sensor_type	Defines the sensor connected to PT1 input.										
Values	<table> <tr> <td>UNUSED</td><td>Input is not connected</td></tr> <tr> <td>PT100_CELSIUS</td><td>PT100 sensor with 100 Ohm at 0C. Note: The dipswitch on the device must be set to match the configuration!</td></tr> <tr> <td>PT1000_CELSIUS</td><td>PT1000 sensor with 1000 Ohm at 0C. Note: The dipswitch on the device must be set to match the configuration!</td></tr> <tr> <td>PT100_FAHRENHEIT</td><td>PT100 sensor with 100 Ohm. Note: The dipswitch on the device must be set to match the configuration!</td></tr> <tr> <td>PT1000_FAHRENHEIT</td><td>PT1000 sensor with 1000 Ohm. Note: The dipswitch on the device must be set to match the configuration!</td></tr> </table>	UNUSED	Input is not connected	PT100_CELSIUS	PT100 sensor with 100 Ohm at 0C. Note: The dipswitch on the device must be set to match the configuration!	PT1000_CELSIUS	PT1000 sensor with 1000 Ohm at 0C. Note: The dipswitch on the device must be set to match the configuration!	PT100_FAHRENHEIT	PT100 sensor with 100 Ohm. Note: The dipswitch on the device must be set to match the configuration!	PT1000_FAHRENHEIT	PT1000 sensor with 1000 Ohm. Note: The dipswitch on the device must be set to match the configuration!
UNUSED	Input is not connected										
PT100_CELSIUS	PT100 sensor with 100 Ohm at 0C. Note: The dipswitch on the device must be set to match the configuration!										
PT1000_CELSIUS	PT1000 sensor with 1000 Ohm at 0C. Note: The dipswitch on the device must be set to match the configuration!										
PT100_FAHRENHEIT	PT100 sensor with 100 Ohm. Note: The dipswitch on the device must be set to match the configuration!										
PT1000_FAHRENHEIT	PT1000 sensor with 1000 Ohm. Note: The dipswitch on the device must be set to match the configuration!										
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.4 (smartIoConfigPt1SensorType)										

pt1_filter_time	Time in seconds used to average out the value.
Value	Number in range 0-10
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.5 (smartIoConfigPt1FilterTime)
pt1_transformation	May be used to transform the input value to another format. Example C to F: $=(\$*1.8)+32$. Use # to append a unit to the value. May also be used for further linearization of the value. Annotation example: [0=\$# (freezing),]40=\$# (too hot), =\$
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.6 (smartIoConfigPt1Transformation)
pt2_attribute	This defines the attribute with which it will register the PT2 temperature sensor to the system.
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.7 (smartIoConfigPt2Attribute)
pt2_sensor_type	Defines the sensor connected to PT2 input.
Values	<div><div>UNUSED</div><div>PT100_CELSIUS</div><div>PT1000_CELSIUS</div><div>PT100_FAHRENHEIT</div><div>PT1000_FAHRENHEIT</div></div> <div><div>Input is not connected</div><div>PT100 sensor with 100 Ohm at 0C. Note: The dipswitch on the device must be set to match the configuration!</div><div>PT1000 sensor with 1000 Ohm at 0C. Note: The dipswitch on the device must be set to match the configuration!</div><div>PT100 sensor with 100 Ohm. Note: The dipswitch on the device must be set to match the configuration!</div><div>PT1000 sensor with 1000 Ohm. Note: The dipswitch on the device must be set to match the configuration!</div></div>
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.8 (smartIoConfigPt2SensorType)
pt2_filter_time	Time in seconds used to average out the value.
Value	Number in range 0-10
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.9 (smartIoConfigPt2FilterTime)
pt2_transformation	May be used to transform the input value to another format. Example C to F: $=(\$*1.8)+32$. Use # to append a unit to the value. May also be used for further linearization of the value. Annotation example: [0=\$# (freezing),]40=\$# (too hot), =\$
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.10 (smartIoConfigPt2Transformation)

ain1_attribute	This defines the attribute with which it will register the analog input 1 to the system.
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.11 (smartIoConfigAin1Attribute)
ain1_sensor_type	Defines the sensor connected to the analog input 1.
Values	<i>UNUSED</i> Input is not connected
	<i>VOLT_0_TO_10</i> Input voltage range between 0 and 10VDC. Note: The dipswitch on the device must be set to match the configuration!
	<i>MILLIAMP_0_TO_20</i> Input current range between 0 and 20mA. Note: The dipswitch on the device must be set to match the configuration!
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.12 (smartIoConfigAin1SensorType)
ain1_raw_min	Defines the lowest raw value data point.
Value	String, max. 8 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.13 (smartIoConfigAin1RawMin)
ain1_raw_max	Defines the highest raw value data point.
Value	String, max. 8 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.14 (smartIoConfigAin1RawMax)
ain1_scaled_min	Defines the lower scaled value at the lower raw value data point.
Value	String, max. 8 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.15 (smartIoConfigAin1ScaledMin)
ain1_scaled_max	Defines the scaled value at the max raw value data point.
Value	String, max. 8 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.16 (smartIoConfigAin1ScaledMax)
ain1_filter_time	Time in seconds used to average out the value.
Value	Number in range 0-10
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.17 (smartIoConfigAin1FilterTime)

ain1_update_delta	<p>Defines how much the input value can deviate before a value change is reported. An absolute or a percent value is expected. An optional minimum update period in seconds can be defined as well. Syntax: delta, time. Example: 5%,60s</p>						
Value	String, max. 8 characters.						
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.18 (smartIoConfigAin1UpdateDelta)						
ain1_transformation	<p>May be used to transform the input value to another format. Syntax: value=text, value=text,.. Or calculations: =\$*10 Example C to F: =(\$*1.8)+32. Use # to append a unit to the value. Also in combination with calculation like: \$/1000#mW. For more options please refer to separate documentation.</p>						
Value	String, max. 128 characters.						
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.19 (smartIoConfigAin1Transformation)						
ain2_attribute	<p>This defines the attribute with which it will register the analog input 2 to the system.</p>						
Value	String, max. 32 characters.						
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.20 (smartIoConfigAin2Attribute)						
ain2_sensor_type	<p>Defines the sensor connected to the analog input 2.</p>						
Values	<table> <tr> <td data-bbox="724 1093 829 1120"><i>UNUSED</i></td><td data-bbox="970 1093 1214 1120">Input is not connected</td></tr> <tr> <td data-bbox="724 1133 906 1160"><i>VOLT_0_TO_10</i></td><td data-bbox="970 1133 1358 1240">Input voltage range between 0 and 10VDC. Note: The dipswitch on the device must be set to match the configuration!</td></tr> <tr> <td data-bbox="724 1254 954 1281"><i>MILLIAMP_0_TO_20</i></td><td data-bbox="970 1254 1426 1330">Input current range between 0 and 20mA. Note: The dipswitch on the device must be set to match the configuration!</td></tr> </table>	<i>UNUSED</i>	Input is not connected	<i>VOLT_0_TO_10</i>	Input voltage range between 0 and 10VDC. Note: The dipswitch on the device must be set to match the configuration!	<i>MILLIAMP_0_TO_20</i>	Input current range between 0 and 20mA. Note: The dipswitch on the device must be set to match the configuration!
<i>UNUSED</i>	Input is not connected						
<i>VOLT_0_TO_10</i>	Input voltage range between 0 and 10VDC. Note: The dipswitch on the device must be set to match the configuration!						
<i>MILLIAMP_0_TO_20</i>	Input current range between 0 and 20mA. Note: The dipswitch on the device must be set to match the configuration!						
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.21 (smartIoConfigAin2SensorType)						
ain2_raw_min	<p>Defines the lowest raw value data point.</p>						
Value	String, max. 8 characters.						
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.22 (smartIoConfigAin2RawMin)						
ain2_raw_max	<p>Defines the highest raw value data point.</p>						
Value	String, max. 8 characters.						
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.23 (smartIoConfigAin2RawMax)						
ain2_scaled_min	<p>Defines the lower scaled value at the lower raw value data point.</p>						
Value	String, max. 8 characters.						
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.24 (smartIoConfigAin2ScaledMin)						

ain2_scaled_max	Defines the scaled value at the max raw value data point.
Value	String, max. 8 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.25 (smartIoConfigAin2ScaledMax)

ain2_filter_time	Time in seconds used to average out the value.
Value	Number in range 0-10
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.26 (smartIoConfigAin2FilterTime)

ain2_update_delta	Defines how much the input value can deviate before a value change is reported. An absolute or a percent value is expected. An absolute or a percent value is expected. An optional minimum update period in seconds can be defined as well. Syntax: delta, time. Example: 10,3600 (update at least once an hour)
Value	String, max. 8 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.27 (smartIoConfigAin2UpdateDelta)

ain2_transformation	May be used to transform the input value to another format. Syntax: value=text, value=text,.. Or calculations: =\$*10 Example C to F: =(\$*1.8)+32. Use # to append a unit to the value. Also in combination with calculation like: \$/1000#mW. For more options please refer to separate documentation.
Value	String, max. 128 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.28 (smartIoConfigAin2Transformation)

ain3_attribute	This defines the attribute with which it will register the analog input 3 to the system.
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.29 (smartIoConfigAin3Attribute)

ain3_sensor_type	Defines the sensor connected to the analog input 3.
Values	UNUSED Input is not connected
	VOLT_0_TO_10 Input voltage range between 0 and 10VDC. Note: The dipswitch on the device must be set to match the configuration!
	MILLIAMP_0_TO_20 Input current range between 0 and 20mA. Note: The dipswitch on the device must be set to match the configuration!
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.30 (smartIoConfigAin3SensorType)

ain3_raw_min	Defines the lowest raw value data point.
Value	String, max. 8 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.31 (smartIoConfigAin3RawMin)

ain3_raw_max	<p>Defines the highest raw value data point.</p> <p>Value String, max. 8 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.32 (smartIoConfigAin3RawMax)</p>
ain3_scaled_min	<p>Defines the lower scaled value at the lower raw value data point.</p> <p>Value String, max. 8 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.33 (smartIoConfigAin3ScaledMin)</p>
ain3_scaled_max	<p>Defines the scaled value at the max raw value data point.</p> <p>Value String, max. 8 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.34 (smartIoConfigAin3ScaledMax)</p>
ain3_filter_time	<p>Time in seconds used to average out the value.</p> <p>Value Number in range 0-10</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.35 (smartIoConfigAin3FilterTime)</p>
ain3_update_delta	<p>Defines how much the input value can deviate before a value change is reported. An absolute or a percent value is expected. An absolute or a percent value is expected. An optional minimum update period in seconds can be defined as well. Syntax: delta, time. Example: 5%,60s</p> <p>Value String, max. 8 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.36 (smartIoConfigAin3UpdateDelta)</p>
ain3_transformation	<p>May be used to transform the input value to another format. Syntax: value=text, value=text,.. Or calculations: =\$*10 Example C to F: =(\$*1.8)+32. Use # to append a unit to the value. Also in combination with calculation like: \$/1000#mW. For more options please refer to separate documentation.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.37 (smartIoConfigAin3Transformation)</p>
ain4_attribute	<p>This defines the attribute with which it will register the analog input 4 to the system.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.38 (smartIoConfigAin4Attribute)</p>

ain4_sensor_type	Defines the sensor connected to the analog input 4.		
	Values	UNUSED	Input is not connected
		VOLT_0_TO_10	Input voltage range between 0 and 10VDC. Note: The dipswitch on the device must be set to match the configuration!
		MILLIAMP_0_TO_20	Input current range between 0 and 20mA. Note: The dipswitch on the device must be set to match the configuration!
	OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.39 (smartIoConfigAin4SensorType)	
<hr/>			
ain4_raw_min	Defines the lowest raw value data point.		
	Value	String, max. 8 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.40 (smartIoConfigAin4RawMin)	
<hr/>			
ain4_raw_max	Defines the highest raw value data point.		
	Value	String, max. 8 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.41 (smartIoConfigAin4RawMax)	
<hr/>			
ain4_scaled_min	Defines the lower scaled value at the lower raw value data point.		
	Value	String, max. 8 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.42 (smartIoConfigAin4ScaledMin)	
<hr/>			
ain4_scaled_max	Defines the scaled value at the max raw value data point.		
	Value	String, max. 8 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.43 (smartIoConfigAin4ScaledMax)	
<hr/>			
ain4_filter_time	Time in seconds used to average out the value.		
	Value	Number in range 0-10	
	OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.44 (smartIoConfigAin4FilterTime)	
<hr/>			
ain4_update_delta	Defines how much the input value can deviate before a value change is reported. An absolute or a percent value is expected. An absolute or a percent value is expected. An optional minimum update period in seconds can be defined as well. Syntax: delta, time. Example: 15%,5s		
	Value	String, max. 8 characters.	
	OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.45 (smartIoConfigAin4UpdateDelta)	

ain4_transformation	<p>May be used to transform the input value to another format. Syntax: value=text, value=text,.. Or calculations: =\$*10 Example C to F: =(\$*1.8)+32. Use # to append a unit to the value. Also in combination with calculation like: \$/1000#mW. For more options please refer to separate documentation.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.46 (smartIoConfigAin4Transformation)</p>
din_idle_time	<p>When unequal to 0, the value of the digital inputs is reported after the specified value in seconds. The time is restarted whenever a digital value is otherwise reported. This feature is useful to guarantee that a group update is executed even if the reported data never change.</p> <p>Value Number in range 0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.47 (smartIoConfigDinIdleTime)</p>
din1_mode	<p>Used to enable the digital input 1.</p> <p>Values <i>UNUSED</i> Input is not connected <i>ENABLED</i> Input is used and reporting</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.48 (smartIoConfigDin1Mode)</p>
din1_attribute	<p>This defines the attribute with which it will register the digital input 1 to the system. If left blank, the digital input is not reported (disabled).</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.49 (smartIoConfigDin1Attribute)</p>
din1_transformation	<p>May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.50 (smartIoConfigDin1Transformation)</p>
din2_mode	<p>Used to enable the digital input 2.</p> <p>Values <i>UNUSED</i> Input is not connected <i>ENABLED</i> Input is used and reporting</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.51 (smartIoConfigDin2Mode)</p>
din2_attribute	<p>This defines the attribute with which it will register the digital input 2 to the system. If left blank, the digital input is not reported (disabled).</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.52 (smartIoConfigDin2Attribute)</p>

din2_transformation	<p>May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.53 (smartIoConfigDin2Transformation)</p>
din3_mode	<p>Used to enable the digital input 3.</p> <p>Values <i>UNUSED</i> Input is not connected <i>ENABLED</i> Input is used and reporting</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.54 (smartIoConfigDin3Mode)</p>
din3_attribute	<p>This defines the attribute with which it will register the digital input 3 to the system. If left blank, the digital input is not reported (disabled).</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.55 (smartIoConfigDin3Attribute)</p>
din3_transformation	<p>May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.56 (smartIoConfigDin3Transformation)</p>
din4_mode	<p>Used to enable the digital input 4.</p> <p>Values <i>UNUSED</i> Input is not connected <i>ENABLED</i> Input is used and reporting</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.57 (smartIoConfigDin4Mode)</p>
din4_attribute	<p>This defines the attribute with which it will register the digital input 4 to the system. If left blank, the digital input is not reported (disabled).</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.58 (smartIoConfigDin4Attribute)</p>
din4_transformation	<p>May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.59 (smartIoConfigDin4Transformation)</p>
aout1_attribute	<p>This defines the attribute with which it will register the analog output 1 to the system. If left blank, this analog output cannot not be used.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.60 (smartIoConfigAout1Attribute)</p>

aout1_mode	Defines the output mode of digital output 1.
Values	<div>UNUSED Output is not connected</div> <div>VOLT_0_TO_10 Output voltage range between 0 and 10VDC</div> <div>MILLIAMP_0_TO_20 Output current range between 0 and 20mA</div> <div>RAW Output is used</div>
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.61 (smartIoConfigAout1Mode)
aout1_transformation	<p>May be used to transform a possible non compliant output value (of the actor group) into a compliant value. Note this transformation takes place before the scaling parameter are applied. Syntax: text=value, text=value,.. Or calculations like: =\$/1000 For more options please refer to separate documentation.</p>
Value	String, max. 128 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.62 (smartIoConfigAout1Transformation)
aout1_raw_min	Defines the lowest raw value data point.
Value	String, max. 8 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.63 (smartIoConfigAout1RawMin)
aout1_raw_max	Defines the highest raw value data point.
Value	String, max. 8 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.64 (smartIoConfigAout1RawMax)
aout1_scaled_min	Defines the lower scaled value at the lower raw value data point.
Value	String, max. 8 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.65 (smartIoConfigAout1ScaledMin)
aout1_scaled_max	Defines the scaled value at the max raw value data point.
Value	String, max. 8 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.66 (smartIoConfigAout1ScaledMax)
aout2_attribute	<p>This defines the attribute with which it will register the analog output 2 to the system. If left blank, this analog output cannot not be used.</p>
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.67 (smartIoConfigAout2Attribute)

aout2_mode	Defines the output mode of digital output 1.
Values	<div> <div><i>UNUSED</i></div> <div>Output is not connected</div> </div> <div> <div><i>VOLT_0_TO_10</i></div> <div>Output voltage range between 0 and 10VDC</div> </div> <div> <div><i>MILLIAMP_0_TO_20</i></div> <div>Output current range between 0 and 20mA</div> </div> <div> <div><i>RAW</i></div> <div>Output is used</div> </div>
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.68 (smartIoConfigAout2Mode)
aout2_transformation	<p>May be used to transform a possible non compliant output value (of the actor group) into a compliant value. Note this transformation takes place before the scaling parameter are applied. Syntax: text=value, text=value,.. Or calculations like: =\$/1000 For more options please refer to separate documentation.</p>
Value	String, max. 128 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.69 (smartIoConfigAout2Transformation)
aout2_raw_min	Defines the lowest raw value data point.
Value	String, max. 8 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.70 (smartIoConfigAout2RawMin)
aout2_raw_max	Defines the highest raw value data point.
Value	String, max. 8 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.71 (smartIoConfigAout2RawMax)
aout2_scaled_min	Defines the lower scaled value at the lower raw value data point.
Value	String, max. 8 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.72 (smartIoConfigAout2ScaledMin)
aout2_scaled_max	Defines the scaled value at the max raw value data point.
Value	String, max. 8 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.73 (smartIoConfigAout2ScaledMax)
dout1_attribute	<p>This defines the attribute with which it will register the digital output 1 to the system. If left blank, the digital input cannot not be used.</p>
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.74 (smartIoConfigDout1Attribute)

dout1_mode	Defines the output mode of digital output 1.
Values	<i>UNUSED</i> Output is not connected <i>DIGITAL</i> Output is switch on or off <i>PWM</i> Output uses pulse width modulation
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.75 (smartIoConfigDout1Mode)
dout1_pwm_frequency	When PWM mode is selected, this parameter defines the PWM frequency in Hz.
Value	Number in range 0-10000000
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.76 (smartIoConfigDout1PwmFrequency)
dout1_transformation	May be used to transform a textual input to acceptable digital values. Example: OFF=0, ON=1. Or to accept other numeric ranges: 0=0,100=1.
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.77 (smartIoConfigDout1Transformation)
dout2_attribute	This defines the attribute with which it will register the digital output 2 to the system. If left blank, the digital input cannot not be used.
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.78 (smartIoConfigDout2Attribute)
dout2_mode	Defines the output mode of digital output 2.
Values	<i>UNUSED</i> Output is not connected <i>DIGITAL</i> Output is switch on or off <i>PWM</i> Output uses pulse width modulation
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.79 (smartIoConfigDout2Mode)
dout2_pwm_frequency	When PWM mode is selected, this parameter defines the PWM frequency in Hz.
Value	Number in range 0-10000000
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.80 (smartIoConfigDout2PwmFrequency)
dout2_transformation	May be used to transform a textual input to acceptable digital values. Example: OFF=0, ON=1. Or to accept other numeric ranges: 0=0,100=1.
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.2.1.81 (smartIoConfigDout2Transformation)

controller_mode	<p>When set to other than normal additional test or debug information are provided.</p> <p>Values</p> <p><i>NORMAL</i> Normal operation mode</p> <p><i>TEST</i> Test mode</p> <p><i>DEBUG</i> Debug mode displays additional infos</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.82 (smartIoConfigControllerMode)</p>
manual_get_input	<p>May be used to manually read an input value. Syntax example: manual_get_input = ain2 [R]. Append R or raw for unprocessed value. Otherwise the scaled input is displayed.</p> <p>Action Execute command with parameter string max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.83 (smartIoConfigManualGetInput)</p>
manual_set_output	<p>May be used to manually force an output value. Syntax example: manual_set_output = aout1 50 [raw]. Append raw if the value should be treated as a raw, unscaled value.</p> <p>Action Execute command with parameter string max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.84 (smartIoConfigManualSetOutput)</p>
read_command	<p>May be used to manually read an internal controller value. Syntax: read_command = parameter.</p> <p>Action Execute command with parameter string max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.85 (smartIoConfigReadCommand)</p>
write_command	<p>May be used to manually write an internal controller value. Syntax: write_command = parameter value.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.2.1.86 (smartIoConfigWriteCommand)</p>
Group Path Description	<p>smart_digital_io_config, dynamical size</p> <p>Device.Controller.smart_digital_io_config</p> <p>Add elements as required for the number of used controllers of this type.</p>
name	<p>Unique name must precisely match the device name specified under Device.SmartOffice.device_config.device_name for a device of product_type = SMART_IO_CONTROLLER.</p> <p>Value String, max. 31 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.2 (smartDigitalIoConfigName)</p>

din_idle_time	<p>When unequal to 0, the value of the digital inputs is reported after the specified value in seconds. The time is restarted whenever a digital value is otherwise reported. This feature is useful to guarantee that a group update is executed even if the reported data never change.</p> <p>Value Number in range 0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.3 (smartDigitalIoConfigDinIdleTime)</p>
din1_mode	<p>Used to enable the digital input 1.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.4 (smartDigitalIoConfigDin1Mode)</p>
din1_attribute	<p>This defines the attribute with which it will register the input to the system.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.5 (smartDigitalIoConfigDin1Attribute)</p>
din1_transformation	<p>May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.6 (smartDigitalIoConfigDin1Transformation)</p>
din2_mode	<p>Used to enable the digital input 2.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.7 (smartDigitalIoConfigDin2Mode)</p>
din2_attribute	<p>This defines the attribute with which it will register the input to the system.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.8 (smartDigitalIoConfigDin2Attribute)</p>
din2_transformation	<p>May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.9 (smartDigitalIoConfigDin2Transformation)</p>
din3_mode	<p>Used to enable the digital input 3.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.10 (smartDigitalIoConfigDin3Mode)</p>

din3_attribute	<p>This defines the attribute with which it will register the input to the system.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.11 (smartDigitalIoConfigDin3Attribute)</p>
din3_transformation	<p>May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.12 (smartDigitalIoConfigDin3Transformation)</p>
din4_mode	<p>Used to enable the digital input 4.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.13 (smartDigitalIoConfigDin4Mode)</p>
din4_attribute	<p>This defines the attribute with which it will register the input to the system.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.14 (smartDigitalIoConfigDin4Attribute)</p>
din4_transformation	<p>May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.15 (smartDigitalIoConfigDin4Transformation)</p>
din5_mode	<p>Used to enable the digital input 5.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.16 (smartDigitalIoConfigDin5Mode)</p>
din5_attribute	<p>This defines the attribute with which it will register the input to the system.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.17 (smartDigitalIoConfigDin5Attribute)</p>
din5_transformation	<p>May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.18 (smartDigitalIoConfigDin5Transformation)</p>

din6_mode	Used to enable the digital input 6.
Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.1.106.3.1.19 (smartDigitalIoConfigDin6Mode)
din6_attribute	This defines the attribute with which it will register the input to the system.
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.3.1.20 (smartDigitalIoConfigDin6Attribute)
din6_transformation	May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.3.1.21 (smartDigitalIoConfigDin6Transformation)
din7_mode	Used to enable the digital input 7.
Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.1.106.3.1.22 (smartDigitalIoConfigDin7Mode)
din7_attribute	This defines the attribute with which it will register the input to the system.
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.3.1.23 (smartDigitalIoConfigDin7Attribute)
din7_transformation	May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100.
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.3.1.24 (smartDigitalIoConfigDin7Transformation)
din8_mode	Used to enable the digital input 8.
Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.1.106.3.1.25 (smartDigitalIoConfigDin8Mode)
din8_attribute	This defines the attribute with which it will register the input to the system.
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.3.1.26 (smartDigitalIoConfigDin8Attribute)

din8_transformation	May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.27 (smartDigitalIoConfigDin8Transformation)
din9_mode	Used to enable the digital input 9. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.28 (smartDigitalIoConfigDin9Mode)
din9_attribute	This defines the attribute with which it will register the input to the system. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.29 (smartDigitalIoConfigDin9Attribute)
din9_transformation	May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.30 (smartDigitalIoConfigDin9Transformation)
din10_mode	Used to enable the digital input 10. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.31 (smartDigitalIoConfigDin10Mode)
din10_attribute	This defines the attribute with which it will register the input to the system. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.32 (smartDigitalIoConfigDin10Attribute)
din10_transformation	May be used to transform the input value to another format. Syntax: 0=text, 1=text. Or 0=0,1=100 to make the digital value toggle between 0 and 100. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.33 (smartDigitalIoConfigDin10Transformation)
dout1_mode	Used to enable digital output 1. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.34 (smartDigitalIoConfigDout1Mode)

dout1_attribute	<p>Defines the attribute with which this digital output registered in the system.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.35 (smartDigitalIoConfigDout1Attribute)</p>
dout1_transformation	<p>May be used to transform a textual input to acceptable digital values. Example: OFF=0, ON=1. Or to accept other numeric ranges: 0=0,100=1.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.36 (smartDigitalIoConfigDout1Transformation)</p>
dout2_mode	<p>Used to enable digital output 2.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.37 (smartDigitalIoConfigDout2Mode)</p>
dout2_attribute	<p>Defines the attribute with which this digital output registered in the system.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.38 (smartDigitalIoConfigDout2Attribute)</p>
dout2_transformation	<p>May be used to transform a textual input to acceptable digital values. Example: OFF=0, ON=1. Or to accept other numeric ranges: 0=0,100=1.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.39 (smartDigitalIoConfigDout2Transformation)</p>
dout3_mode	<p>Used to enable digital output 3.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.40 (smartDigitalIoConfigDout3Mode)</p>
dout3_attribute	<p>Defines the attribute with which this digital output registered in the system.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.41 (smartDigitalIoConfigDout3Attribute)</p>
dout3_transformation	<p>May be used to transform a textual input to acceptable digital values. Example: OFF=0, ON=1. Or to accept other numeric ranges: 0=0,100=1.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.42 (smartDigitalIoConfigDout3Transformation)</p>

dout4_mode	Used to enable digital output 4. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.43 (smartDigitalIoConfigDout4Mode)
dout4_attribute	Defines the attribute with which this digital output registered in the system. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.44 (smartDigitalIoConfigDout4Attribute)
dout4_transformation	May be used to transform a textual input to acceptable digital values. Example: OFF=0, ON=1. Or to accept other numeric ranges: 0=0,100=1. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.45 (smartDigitalIoConfigDout4Transformation)
dout5_mode	Used to enable digital output 5. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.46 (smartDigitalIoConfigDout5Mode)
dout5_attribute	Defines the attribute with which this digital output registered in the system. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.47 (smartDigitalIoConfigDout5Attribute)
dout5_transformation	May be used to transform a textual input to acceptable digital values. Example: OFF=0, ON=1. Or to accept other numeric ranges: 0=0,100=1. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.48 (smartDigitalIoConfigDout5Transformation)
dout6_mode	Used to enable digital output 6. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.49 (smartDigitalIoConfigDout6Mode)
dout6_attribute	Defines the attribute with which this digital output registered in the system. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.50 (smartDigitalIoConfigDout6Attribute)

dout6_transformation	May be used to transform a textual input to acceptable digital values. Example: OFF=0, ON=1. Or to accept other numeric ranges: 0=0,100=1. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.51 (smartDigitalIoConfigDout6Transformation)
dout7_mode	Used to enable digital output 7. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.52 (smartDigitalIoConfigDout7Mode)
dout7_attribute	Defines the attribute with which this digital output registered in the system. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.53 (smartDigitalIoConfigDout7Attribute)
dout7_transformation	May be used to transform a textual input to acceptable digital values. Example: OFF=0, ON=1. Or to accept other numeric ranges: 0=0,100=1. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.54 (smartDigitalIoConfigDout7Transformation)
dout8_mode	Used to enable digital output 8. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.55 (smartDigitalIoConfigDout8Mode)
dout8_attribute	Defines the attribute with which this digital output registered in the system. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.56 (smartDigitalIoConfigDout8Attribute)
dout8_transformation	May be used to transform a textual input to acceptable digital values. Example: OFF=0, ON=1. Or to accept other numeric ranges: 0=0,100=1. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.57 (smartDigitalIoConfigDout8Transformation)
controller_mode	When set to other then normal additional test or debug information are provided. Values <i>NORMAL</i> Normal operation mode <i>TEST</i> Test mode <i>DEBUG</i> Debug mode displays additional infos OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.58 (smartDigitalIoConfigControllerMode)

manual_get_value	<p>May be used to manually read an input value. Syntax example: manual_get_input = din2 [R]. Append R or raw for unprocessed value. Otherwise the transformed input is displayed.</p> <p>Action Execute command with parameter string max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.59 (smartDigitalIoConfigManualGetValue)</p>
manual_set_value	<p>May be used to manually force an output value. Syntax example: manual_set_output = dout1 1.</p> <p>Action Execute command with parameter string max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.60 (smartDigitalIoConfigManualSetValue)</p>
read_command	<p>May be used to manually read an internal controller value. Syntax: read_command = parameter.</p> <p>Action Execute command with parameter string max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.61 (smartDigitalIoConfigReadCommand)</p>
write_command	<p>May be used to manually write an internal controller value. Syntax: write_command = parameter value.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.3.1.62 (smartDigitalIoConfigWriteCommand)</p>

Group	cslc_config , dynamical size
Path	Device.Controller.cslc_config
Description	Add elements as required for the number of used controllers of this type.
name	<p>Unique name must precisely match the device name specified under Device.SmartOffice.device_config.device_name for a device of product_type = SMARTLIGHT_CONTROLLER.</p> <p>Value String, max. 31 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.4.1.2 (cslcConfigName)</p>
read_command	<p>May be used to manually read an internal controller value. Syntax: read_command = parameter.</p> <p>Action Execute command with parameter string max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.106.4.1.3 (cslcConfigReadCommand)</p>

write_command	May be used to manually write an internal controller value. Syntax: write_command = parameter value.
Action	Execute command with parameter string max. 128 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.4.1.4 (cslcConfigWriteCommand)

Group	cslc24_config , dynamical size
Path	Device.Controller.cslc24_config
Description	Add elements as required for the number of used controllers of this type.

name	Unique name must precisely match the device name specified under Device.SmartOffice.device_config.device_name for a device of product_type = SMARTLIGHT_CONTROLLER.
Value	String, max. 31 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.5.1.2 (cslc24ConfigName)

read_command	May be used to manually read an internal controller value. Syntax: read_command = parameter.
Action	Execute command with parameter string max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.5.1.3 (cslc24ConfigReadCommand)

write_command	May be used to manually write an internal controller value. Syntax: write_command = parameter value.
Action	Execute command with parameter string max. 128 characters.
OID	1.3.6.1.4.1.3181.10.6.1.106.5.1.4 (cslc24ConfigWriteCommand)

25 Wifi

25.1 Key Features

Micro Access Point Support

Support for Wifi Micro Access Point. Configure wireless parameter such as SSID and DHCP server address range. Note: the WIFI feature may not be enabled on your device.

The access point is suitable for SmartOffice connection of module devices. It may also be used as Internet access device.

Firewall

The Micro Access Point supports firewalling using configurable incoming and outgoing access control lists (ACL).

Access control list can be used to limit the wireless traffic to predetermined addresses.

Firmware Upgrade

The Micro Access Point firmware is part of the general G6 firmware package and can easily be updated from there.

This ensures that access point and G6 software always match up.

25.2 Functional Description

Wifi

Wireless Access Point setup and status parameters.

INFO: This feature requires additional MICROSENS Access Point hardware connected to the G6 device.

25.3 WIFI CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Device.						
	wifi.					Wireless Access Point setup
			enable_wifi		R/W	Generally enable the access point and its wireless interface.
	access_point.					Basic settings of the access point.
			hostname		R/W	Access point hostname.
			device_ip		R/W	Static device IP address of the access point.
			subnet_mask		R/W	Static subnet mask.
			gateway		R/W	Default gateway IP address. When DHCP is enabled, DHCP has preference over this setting.
			update_firmware		X	Update the access point firmware. When no file name is supplied, the latest version is automatically selected. Alternatively, a specific file name can be supplied to use another version. Use Management.files.firmware.display_files to view a list of available files under the AP section.
			reboot		X	This command will restart the access point only. All wireless communication will be disrupted for about a minute! Syntax: reboot = CONFIRM.
	interface.					This table defines the Ethernet interface available via Wife
			country_code		R/W	International country code. Use DE for Germany, FR for France, etc.
			ssid		R/W	Defines the name under which the access point can be reached. This will be displayed as network name.
			enter_preshared_key		X	Enter the password required to access the network. No spaces are permitted and at least 8 character are required.
			encrypted_preshared_key		R/W	Encrypted form of the entered key. This is automatically filled in when the enter_fa_auth command is executed.
			expose_ssid		R/W	Defines whether the network can be detected or is hidden.
			encryption		R/W	
			dhcp_server		R/W	Enable DHCP server to automatically provide an IP address to the attached wife devices.

dhcp_start_address	R/W	Lowest address served.
dhcp_number_of_addresses	R/W	The number of IP addresses served starting from the dhcp_start_address
channel_number	R/W	Zero is automatic selection.
channel_width	R/W	
firewall_config.		Each entry of this variable table defines the details of one test case.
enable_ingress_firewall	R/W	When disabled the ingress_firewall table is not in effect. This is intended for test purposes only.
enable_egress_firewall	R/W	When disabled the ingress_firewall table is not in effect. This is intended for test purposes only.
drop_invalid_packets	R/W	Drop invalid packets, not matching any active connection.
syn_rate_limiting	R/W	Defines how many SYN request are accepted per second. When the limit is reached, a SYN flooding attack is assumed and the port is protected. The value 0 disables the rate limit check.
use_syn_cookies	R/W	SYN cookie is a technique used to resist SYN flooding attacks.
tcp_window_scaling	R/W	Enable TCP window scaling.
firewall_rules.		Firewall settings for traffic ingressing on the Wi-Fi_33 interface.
incoming_acl_list	R/W	Name of the ACL (access control list) which declares which ACL applies to incoming traffic (redirects). Several ACL may be specified with a comma separated list. Example acl1, otherlist
incoming_acl_default	R/W	Defines which action is taken when none of the ACL records matches. Default is deny which blocks all traffic.
outgoing_acl_list	R/W	Name of the ACL (access control list) which declares which ACL applies to incoming traffic (redirects). Several ACL may be specified with a comma separated list. Example acl1, otherlist
outgoing_acl_default	R/W	Defines which action is taken when none of the ACL records matches. Default is deny which blocks all traffic.
status.		Indicates basic WIFI related status information
overall_status	R	Indicates if WIFI module is operational.
number_of_connections	R	
ip_v4_status.		This section shows a summary of IPv4 settings as they are currently active. These may reflect the statically configured values or may be dynamically assigned using DHCP.
dynamic_device_ip	R	Currently used access point IP address.
dynamic_subnet_mask	R	Currently used access point subnet mask.
dynamic_gateway	R	Currently used access point gateway IP address.

25.4 WIFI Configuration Parameters

Group Path	General Parameters Device.WIFI
enable_wifi	Generally enable the access point and its wireless interface. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.1.98.1 (wifiEnableWifi)

Group Path Description	access_point Device.WIFI.access_point Basic settings of the access point.
hostname	Access point hostname. Value String, max. 64 characters. OID 1.3.6.1.4.1.3181.10.6.1.98.2.1.2 (accessPointHostname)
device_ip	Static device IP address of the access point. Format IPv4 Address <i>ddd.ddd.ddd.ddd</i> (ddd = decimal number between 000 to 255) OID 1.3.6.1.4.1.3181.10.6.1.98.2.1.3 (accessPointDeviceIp)
subnet_mask	Static subnet mask. Format IPv4 Address <i>ddd.ddd.ddd.ddd</i> (ddd = decimal number between 000 to 255) OID 1.3.6.1.4.1.3181.10.6.1.98.2.1.4 (accessPointSubnetMask)
gateway	Default gateway IP address. When DHCP is enabled, DHCP has preference over this setting. Format IPv4 Address <i>ddd.ddd.ddd.ddd</i> (ddd = decimal number between 000 to 255) OID 1.3.6.1.4.1.3181.10.6.1.98.2.1.5 (accessPointGateway)

update_firmware	<p>Update the access point firmware. When no file name is supplied, the latest version is automatically selected. Alternatively, a specific file name can be supplied to use another version. Use Management.files.firmware.display_files to view a list of available files under the AP section.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.98.2.1.6 (accessPointUpdateFirmware)</p>
reboot	<p>This command will restart the access point only. All wireless communication will be disrupted for about a minute! Syntax: reboot = CONFIRM.</p> <p>Action Execute command with parameter string max. 16 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.98.2.1.7 (accessPointReboot)</p>

Group Path Description	interface Device.WIFI.interface This table defines the Ethernet interface available via Wife
country_code	<p>International country code. Use DE for Germany, FR for France, etc.</p> <p>Value String, max. 4 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.98.3.1.2 (interfaceCountryCode)</p>
ssid	<p>Defines the name under which the access point can be reached. This will be displayed as network name.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.98.3.1.3 (interfaceSsid)</p>
enter_preshared_key	<p>Enter the password required to access the network. No spaces are permitted and at least 8 character are required.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.98.3.1.4 (interfaceEnterPresharedKey)</p>
encrypted_preshared_key	<p>Encrypted form of the entered key. This is automatically filled in when the enter_fa_auth command is executed.</p> <p>Value String, max. 256 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.98.3.1.5 (interfaceEncryptedPresharedKey)</p>
expose_ssid	<p>Defines whether the network can be detected or is hidden.</p> <p>Values <i>HIDDEN</i> The SSID is not transmitted to hide the network <i>VISIBLE</i> SSID is transmitted so that user can easily connect</p> <p>OID 1.3.6.1.4.1.3181.10.6.1.98.3.1.6 (interfaceExposeSsid)</p>

encryption

Values	<i>NONE</i>	No encryption is used
	<i>WEP</i>	Use WEP encryption
	<i>WPA_PSK</i>	Use PSK encryption
	<i>WPA_PSK2</i>	Use PSK2 encryption
OID	1.3.6.1.4.1.3181.10.6.1.98.3.1.7 (interfaceEncryption)	

dhcp_server

Enable DHCP server to automatically provide an IP address to the attached wifi devices.

Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.1.98.3.1.8 (interfaceDhcpServer)

dhcp_start_address

Lowest address served.

Format	IPv4 Address <i>ddd.ddd.ddd.ddd</i> (<i>ddd</i> = decimal number between 000 to 255)
OID	1.3.6.1.4.1.3181.10.6.1.98.3.1.9 (interfaceDhcpStartAddress)

dhcp_number_of_addresses

The number of IP addresses served starting from the dhcp_start_address

Value	Number in range 0-255
OID	1.3.6.1.4.1.3181.10.6.1.98.3.1.10 (interfaceDhcpNumberOfAddresses)

channel_number

Zero is automatic selection.

Value	Number in range 0-11
OID	1.3.6.1.4.1.3181.10.6.1.98.3.1.11 (interfaceChannelNumber)

channel_width

Values	<i>HT20</i>	Single 20MHz channel
	<i>HT40P</i>	2x 20MHz channels, primary control channel is upper, secondary channel is below
	<i>HT40N</i>	2x 20MHz channels, primary control channel is lower, secondary channel is above
OID	1.3.6.1.4.1.3181.10.6.1.98.3.1.12 (interfaceChannelWidth)	

Group**Path****Description****firewall_config**

Device.WIFI.firewall_config

Each entry of this variable table defines the details of one test case.

enable_ingress_firewall	When disabled the ingress_firewall table is not in effect. This is intended for test purposes only. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.1.98.4.1.2 (firewallConfigEnableIngressFirewall)
enable_egress_firewall	When disabled the ingress_firewall table is not in effect. This is intended for test purposes only. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.1.98.4.1.3 (firewallConfigEnableEgressFirewall)
drop_invalid_packets	Drop invalid packets, not matching any active connection. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.1.98.4.1.4 (firewallConfigDropInvalidPackets)
syn_rate_limiting	Defines how many SYN request are accepted per second. When the limit is reached, a SYN flooding attack is assumed and the port is protected. The value 0 disables the rate limit check. Value Number in range 0-255 OID 1.3.6.1.4.1.3181.10.6.1.98.4.1.5 (firewallConfigSynRateLimiting)
use_syn_cookies	SYN cookie is a technique used to resist SYN flooding attacks. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.1.98.4.1.6 (firewallConfigUseSynCookies)
tcp_window_scaling	Enable TCP window scaling. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.1.98.4.1.7 (firewallConfigTcpWindowScaling)

Group	firewall_rules
Path	Device.WIFI.firewall_rules
Description	Firewall settings for traffic ingressing on the Wi-Fi__33 interface.
incoming_acl_list	Name of the ACL (access control list) which declares which ACL applies to incoming traffic (redirects). Several ACL may be specified with a comma separated list. Example acl1, otherlist Value String, max. 128 characters. OID 1.3.6.1.4.1.3181.10.6.1.98.5.1.2 (firewallRulesIncomingAclList)

incoming_acl_default Defines which action is taken when none of the ACL records matches. Default is deny which blocks all traffic.

Values

<i>DENY</i>	When no entry matches the ACL then the ARP is denied
<i>PERMIT</i>	When no entry matches the ACL then the ARP is accepted.

OID 1.3.6.1.4.1.3181.10.6.1.98.5.1.3
(firewallRulesIncomingAcIDefault)

outgoing_acl_list Name of the ACL (access control list) which declares which ACL applies to incoming traffic (redirects). Several ACL may be specified with a comma separated list. Example acl1, otherlist

Value String, max. 128 characters.

OID 1.3.6.1.4.1.3181.10.6.1.98.5.1.4 (firewallRulesOutgoingAcIList)

outgoing_acl_default Defines which action is taken when none of the ACL records matches. Default is deny which blocks all traffic.

Values

<i>DENY</i>	When no entry matches the ACL then the ARP is denied
<i>PERMIT</i>	When no entry matches the ACL then the ARP is accepted.

OID 1.3.6.1.4.1.3181.10.6.1.98.5.1.5
(firewallRulesOutgoingAcIDefault)

25.5 WIFI Status Parameters

Group	status
Path	Device.WIFI.status
Description	Indicates basic WIFI related status information
overall_status	Indicates if WIFI module is operational.
	Values <div> <div><i>NOT_PRESENT</i></div> <div>No WIFI module connected</div> </div> <div> <div><i>DISABLED</i></div> <div>WIFI module is not configured</div> </div> <div> <div><i>FAULT</i></div> <div>WIFI module has some fault and cannot operate</div> </div> <div> <div><i>OPERATIONAL</i></div> <div>WIFI module is up and running</div> </div>
	OID 1.3.6.1.4.1.3181.10.6.1.98.100.1.2 (statusOverallStatus)
number_of_connections	
	Value Number in range 0-0xFFFFFFFF
	OID 1.3.6.1.4.1.3181.10.6.1.98.100.1.3 (statusNumberOfConnections)
Group	ip_v4_status
Path	Device.WIFI.ip_v4_status
Description	This section shows a summary of IPv4 settings as they are currently active. These may reflect the statically configured values or may be dynamically assigned using DHCP.
dynamic_device_ip	Currently used access point IP address.
	Format IPv4 Address <i>ddd.ddd.ddd.ddd</i> (ddd = decimal number between 000 to 255)
	OID 1.3.6.1.4.1.3181.10.6.1.98.101.1.2 (ipV4StatusDynamicDeviceIp)
dynamic_subnet_mask	Currently used access point subnet mask.
	Format IPv4 Address <i>ddd.ddd.ddd.ddd</i> (ddd = decimal number between 000 to 255)
	OID 1.3.6.1.4.1.3181.10.6.1.98.101.1.3 (ipV4StatusDynamicSubnetMask)

dynamic_gateway	Currently used access point gateway IP address.
Format	IPv4 Address <i>ddd.ddd.ddd.ddd</i> (<i>ddd</i> = decimal number between 000 to 255)
OID	1.3.6.1.4.1.3181.10.6.1.98.101.1.4 (ipV4StatusDynamicGateway)

26 Virtual LANs (VLANs)

26.1 Key Features

VLAN Filter

Up to 256 VLAN's may be configured.

Very high number of VLANs can be assigned. Previous product only supported 64 VLANs.

Access Mode

For the connection of non-VLAN capable end devices (e.g. PCs). Outgoing packets are sent untagged. Incoming packets are tagged with the port default VLAN ID (PVID).

Trunk Mode

For the interconnection of VLAN capable switches. Outgoing packets are always sent tagged. Incoming packets are received tagged. Incoming packets without VLAN tag are tagged with the port default VLAN ID (PVID).

Hybrid Mode

For the connection of VLAN capable and non-VLAN capable devices on the same port (e.g. VoIP-phone (tagged) and PC (untagged)). Outgoing packets are sent tagged, except packets for the port default VLAN ID (PVID), which are untagged. Incoming packets are received untagged for the port default VLAN (PVID), all other packets are tagged.

Ideal setup for the desktop application of one PC and one IP telephone connected to one switch port.

Multiple VLAN Reservation Protocol (MVRP)

Multiple VLAN Reservation Protocol. This protocol automates and centralizes VLAN assignment in large networks.

Greatly simplifies VLAN deployment in larger networks.

Extreme Auto Attach (former Avaya Fabric Attach)

Support to attach to an SPB based network by mapping local VLANs to SPB I-SIDs. SPB is the basis of the Avaya Fabric, now Extreme.

The connected application need not be SPB aware to make use of the advanced network functionality.

Extreme (Avaya) Zero Touch

Attach to an SPB based network, automatically obtaining the VLANs - I-SID bindings over the network. Note: Requires preset of authentication key to match network.

Ports can be placed into VLANs from central network, which simplifies network management.

Stacked VLANs (Q-in-Q)

Stacked VLAN are used to transport customer VLAN traffic accross a carrier network using VLAN itself. The feature is also known as Q-in-Q and provider bridging. Configurable Ethertype fields are provided.

The feature permit use of the switch as access device to a carrier network using VLANs.

Priority Override

VLAN priority code point of incoming packets can be overwritten with the VLAN specific priority defined in the VLAN filter.

Voice VLAN

VLAN ID used by LLDP/CDP to assign VLAN to connected VoIP-phone.

RSTP VLAN

VLAN ID used by Spanning Tree instance for BPDU tagging.

Unauthorized VLAN

VLAN ID assigned by Port Based Access Control to unauthorized ports (guest VLAN).

Management VLAN

VLAN ID used by the management agent (device internal port).

26.2 Functional Description

Virtual LANs (VLANs) allow the logical structuring of networks into groups independent from the physical network structure. These groups (called 'VLANs') are completely isolated from each other, no network traffic (including broadcasts) can pass between them. Up to 4095 VLANs can be defined in a network, each identified by a unique number between 1 and 4095. This number is added to each packet transmitted in the network (VLAN-Tag).

When VLAN filtering mode is enabled, the switch forwards and filters all packets based on their VLAN tag according to IEEE Std. 802.1Q. The VLAN filtering table determines if a packet is allowed to be forwarded to a switch port. The final forwarding decision based on the packets destination MAC address is then made within the VLAN.

For each port it can be defined, if the VLAN tag is stripped on outgoing packets (untagged) or remains unchanged (tagged). An individual VLAN can be defined for the device internal management port.

26.2.1 VLAN filter table

Each VLAN that shall be forwarded by the switch must be defined in the VLAN filter table.

A maximum of 256 VLAN ID entries can be defined in the table. Each of these VLAN IDs can be selected out of the full range of 4095 possible IDs. For testing purposes, single entries can be disabled without deleting them, so they can be simply re-enabled if required.

To simplify the handling of VLANs, for each VLAN ID an individual name string ('alias') can be assigned. This makes the administration and configuration of VLANs more intuitive.

For each VLAN ID the allowed ports must be defined. The so called port membership defines, if a port is part of the VLAN (member) or not. Packets are only forwarded to ports that are defined member of the VLAN ID the packet is tagged with.

Device internal management ports must also be member of the VLAN they shall communicate with. This setting is made via a separate parameter.

26.2.2 Port VLAN Mode

Access Mode

Outgoing frames are send untagged. Incoming frames must be untagged and become tagged with the ports default VLAN ID and Priority. This port mode is normally used for the connection of end devices like PCs that cannot handle VLAN tagged packets

Trunk Mode

Outgoing frames are always send tagged. Incoming frames are expected to be received tagged. Incoming frames without VLAN tag were processed with the ports default VLAN ID. This mode is normally used as inter switch connection.

Hybrid Mode

Outgoing frames are send tagged, except the frames of the port default VLAN. Incoming frames of the port default VLAN are expected untagged, frames of other VLANs are always expected tagged. This mode is normally used for combined connection of a VoIP phone and a PC at a port. In this setup the phone is communicating tagged and the PC is communicating untagged.

26.2.3 Port Default VLAN and Priority

Packets entering on a port without VLAN tag (untagged) are assigned an VLAN tag with the port default VLAN and priority value before further internal processing.

26.2.4 Priority Overwrite

When the priority overwrite mode is enabled on the port and for the VLAN, the priority field of incoming packets on that port is overwritten with the priority value of that VLAN, defined in the VLAN filter table.

26.2.5 Force Default VLAN ID

When the 'Force Default VLAN' mode is enabled for a port, the VLAN ID of all incoming packets on that port is overwritten with the Port Default VLAN ID, even if they are tagged with a NULL value. A NULL value in the VID indicates that the VLAN tag is only used for prioritization. The prioritization field in the VLAN tag remains unchanged by the VID replacement.

This mode can be used as additional security measure to prevent network intrusion by injecting VLAN-tagged packets into a port.

26.2.6 Best Practice: How to configure VLANs

Disable VLAN filtering

While changing the VLAN configuration, VLAN filtering should be disabled. This prevents unwanted effects when unfinished or partial configurations become active, e.g. if you change the default VLAN ID of a port before adding this VLAN ID to the filter table, all traffic through that port is discarded. If this happens to be the port by which you are connected to the switch, this was the last action you have performed on the device.

Finally, if all settings have been applied and checked, VLAN filtering should be enabled.

```
# Disable VLAN filtering
Protocol.VLAN.enable_vlan_filtering = Disabled

# Enable VLAN filtering
Protocol.VLAN.enable_vlan_filtering = Enabled
```

If you cannot disable VLAN filtering, as the device is already deployed, then take special care that you are not accidentally changing the management VLAN ID and the corresponding VLAN filter table entry.

Define VLAN filter table entries first

For each VLAN ID used add a corresponding VLAN Filter table entry. The following example shows the CLI command script to add new entries for VLAN IDs 101 to 104:

```
# Add port VLAN filter entries
Protocol.VLAN.filter_config[*].vlan_id = 101
Protocol.VLAN.filter_config[*].vlan_id = 102
Protocol.VLAN.filter_config[*].vlan_id = 103
Protocol.VLAN.filter_config[*].vlan_id = 104
```

Now the port membership for external ports and the membership of internal management ports for this VLAN ID can be defined.

Do not forget to add the port membership for the uplink and downlink ports. The following example script assigns local port 1, uplink (5) and downlink port (6) as members of VLAN 101:

```
# Add port membership for VLANs
Protocol.VLAN.filter_config[101].port_members = 1/1, 1/5, 1/6
Protocol.VLAN.filter_config[102].port_members = 1/2, 1/5, 1/6
Protocol.VLAN.filter_config[103].port_members = 1/3, 1/5, 1/6
Protocol.VLAN.filter_config[104].port_members = 1/4, 1/5, 1/6
```

Define port default VLANs last

When a VLAN ID is defined in the filter table, the VLAN ID can now be set for those ports that are member of that VLAN and shall tag incoming traffic accordingly.

Additionally the port VLAN mode must be defined. For local ports, Access or Hybrid mode is commonly used for the connection of end-devices. Up- and downlink ports should operate in VLAN Trunk mode, as they are inter-switch connections.

The following example sets the local ports 1-4 to Access mode and the up- and downlink ports (5 + 6) to Trunk mode:

```
# Set port VLAN mode
Protocol.VLAN.port_config[1/1].vlan_mode = ACCESS
Protocol.VLAN.port_config[1/2].vlan_mode = ACCESS
Protocol.VLAN.port_config[1/3].vlan_mode = ACCESS
Protocol.VLAN.port_config[1/4].vlan_mode = ACCESS
Protocol.VLAN.port_config[1/5].vlan_mode = TRUNK
Protocol.VLAN.port_config[1/6].vlan_mode = TRUNK
```

Now the port default VLAN ID is set to an individual value for each port. Up- and downlink have the management VLAN ID assigned:

```
# Set port default VLAN
Protocol.VLAN.port_config[1/1].default_vlan_id = 101
Protocol.VLAN.port_config[1/2].default_vlan_id = 102
Protocol.VLAN.port_config[1/3].default_vlan_id = 103
Protocol.VLAN.port_config[1/4].default_vlan_id = 104
```

Add VLAN for management port

For security reasons, normally the network management is placed in a separate VLAN. Access to this management VLAN should only be possible by a network administrator from the central network via the up- and downlink ports, but never from the local ports.

This means for configuration, that only the internal management port and the up- and downlink ports must be member of the management VLAN.

Furthermore the management port VLAN ID must be set to the VLAN ID used for the management. The following example shows the configuration steps necessary to configure a device with uplink on port 5 for a management VLAN using the VLAN ID 99:

```
# Add Management VLAN settings
Protocol.VLAN.filter_config[*].vlan_id = 99
Protocol.VLAN.filter_config[99].port_members = 1/5, 1/6
Protocol.VLAN.filter_config[99].management_members = ALL
Protocol.VLAN.vlan_id_config.management_vlan_id = 99
Protocol.VLAN.port_config[1/5].default_vlan_id = 99
Protocol.VLAN.port_config[1/6].default_vlan_id = 99
```

26.2.7 Best Practice: VLAN standard application

In normal VLAN mode, each copper port and the management port has exactly one VLAN ID assigned. It is possible to assign the same VLAN ID to multiple ports to group ports in the same VLAN. All traffic entering the port is tagged automatically with the assigned port VID and priority, all traffic output on the port has the VLAN tag automatically removed.

The fiber uplink port normally operates in VLAN trunk mode, meaning it passes all traffic from the other ports to the central switch. The connected port on the central side must operate in VLAN trunk mode accordingly. All traffic entering the switch is filtered and forwarded based on the VLAN table setting.

26.3 VLAN CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Protocol.	vlan.					VLAN related settings
			enable_vlan_filtering		R/W	Generally enable VLAN filtering function:
	vlan_id_config.					This section defines some default VLAN settings.
			management_vlan_id		R/W	VLAN ID for internal management port. Packets sent by the management agent are tagged with this VLAN ID,
			management_priority		R/W	VLAN Priority for internal management port. Packets sent by the internal management agent are tagged with this priority value.
			voice_vlan_id		R/W	Voice VLAN ID. Special VLAN for IP phones.
			rstp_vlan_id		R/W	RSTP VLAN ID. When using single instance Spanning Tree (STP or RSTP) in combination with VLANs, all spanning tree messages are tagged with this VLAN ID.
			unauthorized_vlan_id		R/W	When using port access control with dynamic VLANs, unauthorized ports are attached to this VLAN.
			smartoffice_vlan_id		R/W	VLAN ID used for SmartOffice control traffic between director and controllers. Also used by the SmartOffice GUI.
	port_config[PORT].					These settings define the default VLANs per port and defines how untagged data are treated.
			vlan_mode		R/W	Defines how the VLAN tag of incoming and outgoing packets shall be handled on port.
			default_vlan_id		R/W	Default VLAN ID for port. Incoming packets without VLAN tag are automatically tagged using the default VLAN ID and default priority values.
			force_default_vlan_id		R/W	When enabled, incoming packets with existing VLAN tag are overwritten with the default port VLAN ID.

default_priority	R/W	Default priority value for port. Incoming packets without VLAN tag are automatically tagged using the default VLAN ID and default priority values.
priority_override	R/W	When enabled, incoming packets with existing VLAN tag are overwritten with the default priority value.
unauthorized_vlan_id	R/W	When using port access control with dynamic VLANs, unauthorized ports are attached to this VLAN. When set to 0 the global <code>vlan_id_config.unauthorized_vlan_id</code> parameter applies. Use this parameter to set an independent port specific unauthorized vlan.
fallback_vlan_id	R/W	When using port access control with dynamic VLANs and a RADIUS server, the fallback vlan is assigned when the RADIUS server is unavailable. If this parameter is set to 0 the unauthorized vlan is used instead. If this is also 0 then the global <code>vlan_id_config.unauthorized_vlan_id</code> parameter applies.
q_in_q_ethertype	R/W	Ethertype configuration only applies for <code>vlan_mode Q_IN_Q</code> .
filter_config[DYNAMIC].		Defines the used VLANs and their associated ports.
vlan_id	R/W	Defines filter table entry for this VLAN ID. This is the key value for the table. Type '=' to edit, use index '['*] = new_vlan:' to add an entry. Edit string to nothing to delete entry.
entry_mode	R/W	When disabled, filtering for this VLAN ID is disabled without deleting the table entry. This can be used for testing and configuration.
alias	R/W	User-definable name string for VLAN.
mstp_group	R/W	All filter entries with the same <code>mstp_group</code> number will share an MSTP instance. A group may consist of one or many vlan entries. A value of 0 indicates that MSTP is not used for this VLAN.
fabric_attach_i_sid	R/W	This parameter defines the VLAN to I-SID binding when the shortest path bridging (SPB) fabric attach feature is used.
port_members	R/W	Defines port memberships for VLAN. Syntax: slot/port, slot/port or use hex value for quick setup = 0x3f (ports 1-6)
management_members	R/W	Defines the port membership for the internal management port(s).

priority_override	R/W	When enabled the priority value of packets tagged with this VLAN is overwritten with the new_priority value.
new_priority	R/W	VLAN priority value when priority_override is enabled.
enable_mvrp	R/W	Generally enable MVRP (Multiple VLAN Registration Protocol) function. MVRP is operational on 802.1q trunk ports only.
mvrp_port_config[PORT].		Configuration parameter concerning the port specific MVRP settings.
enable_mvrp	R/W	Enable MVRP (Multiple VLAN Registration Protocol) on this port.
registration_mode	R/W	Configuration of the MVRP registration mode.
join_timer	R/W	Number of milliseconds that the interface must wait before sending MVRP PDUs.
leave_timer	R/W	Number of milliseconds that the switch retains a VLAN in the Leave state before the VLAN is unregistered. At a minimum, set the leave-timer interval at twice the join-timer interval.
leaveall_timer	R/W	Number of milliseconds between the sending of Leave All messages.
fabric_attach_port_config[PORT].		Configuration parameter controlling the fabric attach feature. Each port can be configured individually.
enable_fabric_attach	R/W	Shortest path bridging (SPB) fabric attach feature can be used to simplify configuration in an SBP enabled network. Please also generally enable the LLDP function to use this feature. When enabled the port will act as client to a fabric attach network.
msg_authentication	R/W	when enabled message authentication using the fa_auth key is used.
enter_fa_auth_key	X	Enter the fabric attach authentication keys required to access the network. No spaces are permitted.
encrypted_fa_auth_key	R/W	Encrypted form of the entered key. This is automatically filled in when the enter_fa_auth command is executed.
number_of_entries	R	Number of VLAN entries in the table.
status[256].		This table lists the status of all defined VLANs.
vlan_id	R	VLAN identifier
time_mark	R	
alias	R	Contains the alias name for static entries.
port_members	R	Lists all ports that belong to this VLAN.

filter_database	R	filter data base
egress_ports	R	The set of ports which are transmitting traffic for this VLAN as either tagged or untagged frames.
untagged_ports	R	The set of ports which are transmitting traffic for this VLAN as untagged frames.
fabric_attach_state	R	Indicates if auto attachment to the fabric was successful.
fabric_attach_i_sid	R	This indicates the VLAN to I-SID binding when the shortest path bridging (SPB) fabric attach feature is used.
creation_mode	R	Indicates by which means this VLAN entry was created.
creation_time	R	The value of system.uptime when this VLAN was created.
port_status[PORT].		Port related view of the currently active VLAN setup.
assigned_vlan_ids	R	List of all VLAN ids that are configured or dynamically assigned to this port.
dynamic_default_vlan_id	R	Indicates the current port default VLAN. The value may change due to port authentication or configuration.
last_update_method	R	Indicates what caused the last VLAN reconfiguration.
last_updating_mac	R	Indicates which MAC address, if any, was involve in changing the VLAN setting for this port last.
last_update_time	R	Indicates the time when the VLAN settings were last changed.
mvrp_status[PORT].		This table lists MVRP status information.
last_source_mac	R	The Source MAC Address of the last MVRP message received on this port.
failed_registrations	R	The total number of failed MVRP registrations, for any reason, on this port.

26.4 VLAN Configuration Parameters

Group	General Parameters
Path	Protocol.VLAN
enable_vlan_filtering	<p>Generally enable VLAN filtering function:</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.82.1 (vlanEnableVlanFiltering) 1.3.6.1.2.1.17.7.1.4.5.1.3 (dot1qPortIngressFiltering)</p>
enable_mvrp	<p>Generally enable MVRP (Multiple VLAN Registration Protocol) function. MVRP is operational on 802.1q trunk ports only.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.82.5 (vlanEnableMvrp) 1.3.111.2.802.1.1.4.1.1.1.1.6 (ieee8021QBridgeMvrpEnabledStatus)</p>
Group	port_config, for each port[0..24]
Path	Protocol.VLAN.port_config[port]
Description	These settings define the default VLANs per port and defines how untagged data are treated.

vlan_mode	Defines how the VLAN tag of incoming and outgoing packets shall be handled on port.		
Values	ACCESS	All packets received or transmitted by the port are untagged. Received packets are tagged with the port default VLAN ID and priority. Transmitted packets have their VLAN tag removed before they are sent out.	
	HYBRID	Outgoing packets remain unchanged except for packets tagged with the port default VLAN ID. These packets have their VLAN tag removed before they are sent out. Received packets are forwarded unchanged depending on the VLAN filter table settings, except for untagged packets that are tagged with the port default VLAN ID and priority.	
	TRUNK	All packets received or transmitted by the port are tagged. Received packets are forwarded unchanged depending on the VLAN filter table settings. Outgoing packets are sent out unchanged.	
	Q_IN_Q_CUSTOMER	802.1ad (Q in Q) setting. Defines VLAN of the customer side.	
	Q_IN_Q_PROVIDER	802.1ad (Q in Q) setting. Defines VLAN of the provider side.	
OID	1.3.6.1.4.1.3181.10.6.2.82.3.1.2 (portConfigVlanMode)		

default_vlan_id	Default VLAN ID for port. Incoming packets without VLAN tag are automatically tagged using the default VLAN ID and default priority values.		
Value	Number in range 0-4095		
OID	1.3.6.1.4.1.3181.10.6.2.82.3.1.3 (portConfigDefaultVlanId) 1.3.6.1.2.1.17.7.1.4.5.1.1 (dot1qPvid)		

force_default_vlan_id	When enabled, incoming packets with existing VLAN tag are overwritten with the default port VLAN ID.		
Values	enabled, disabled		
OID	1.3.6.1.4.1.3181.10.6.2.82.3.1.4 (portConfigForceDefaultVlanId)		

default_priority	Default priority value for port. Incoming packets without VLAN tag are automatically tagged using the default VLAN ID and default priority values.		
Values	PRIORITY_0	Background (lowest)	
	PRIORITY_1	Best Effort	
	PRIORITY_2	Excellent Effort	
	PRIORITY_3	Critical Applications	
	PRIORITY_4	Video	
	PRIORITY_5	Voice	
	PRIORITY_6	Internetwork Control	
	PRIORITY_7	Network Control (highest)	
OID	1.3.6.1.4.1.3181.10.6.2.82.3.1.5 (portConfigDefaultPriority)		

priority_override	<p>When enabled, incoming packets with existing VLAN tag are overwritten with the default priority value.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.82.3.1.6 (portConfigPriorityOverride)</p>
unauthorized_vlan_id	<p>When using port access control with dynamic VLANs, unauthorized ports are attached to this VLAN. When set to 0 the global <code>vlan_id_config.unauthorized_vlan_id</code> parameter applies. Use this parameter to set an independent port specific unauthorized vlan.</p> <p>Value Number in range 0-4095</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.82.3.1.7 (portConfigUnauthorizedVlanId)</p>
fallback_vlan_id	<p>When using port access control with dynamic VLANs and a RADIUS server, the fallback vlan is assigned when the RADIUS server is unavailable. If this parameter is set to 0 the unauthorized vlan is used instead. If this is also 0 then the global <code>vlan_id_config.unauthorized_vlan_id</code> parameter applies.</p> <p>Value Number in range 0-4095</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.82.3.1.8 (portConfigFallbackVlanId)</p>
q_in_q_ethertype	<p>Ethertype configuration only applies for <code>vlan_mode Q_IN_Q</code>.</p> <p>Values</p> <ul style="list-style-type: none"> <code>OX_88A8</code> Standard value for 802.1ad <code>OX_9100</code> Cisco standard value for 802.1ad <code>OX_9200</code> Alternate Ethertype <code>OX_8100</code> Normal VLAN tag usually not used for double tagged application. (801.1q) <p>OID 1.3.6.1.4.1.3181.10.6.2.82.3.1.9 (portConfigQInQEthertype)</p>
Group Path Description	<p>filter_config, dynamical size</p> <p>Protocol.VLAN.filter_config</p> <p>Defines the used VLANs and their associated ports.</p>
vlan_id	<p>Defines filter table entry for this VLAN ID. This is the key value for the table. Type '=' to edit, use index '['*] = new_vlan:' to add an entry. Edit string to nothing to delete entry.</p> <p>Value String, max. 4 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.82.4.1.2 (filterConfigVlanId)</p>
entry_mode	<p>When disabled, filtering for this VLAN ID is disabled without deleting the table entry. This can be used for testing and configuration.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.82.4.1.3 (filterConfigEntryMode)</p>

alias	User-definable name string for VLAN.
	Value String, max. 32 characters.
	OID 1.3.6.1.4.1.3181.10.6.2.82.4.1.4 (filterConfigAlias)
mstp_group	All filter entries with the same mstp_group number will share an MSTP instance. A group may consist of one or many vlan entries. A value of 0 indicates that MSTP is not used for this VLAN.
	Value Number in range 0-64
	OID 1.3.6.1.4.1.3181.10.6.2.82.4.1.5 (filterConfigMstpGroup)
fabric_attach_i_sid	This parameter defines the VLAN to I-SID binding when the shortest path bridging (SPB) fabric attach feature is used.
	Value Number in range 0-0xFFFFFFFF
	OID 1.3.6.1.4.1.3181.10.6.2.82.4.1.6 (filterConfigFabricAttachISid)
port_members	Defines port memberships for VLAN. Syntax: slot/port, slot/port or use hex value for quick setup = 0x3f (ports 1-6)
	Value PORTMASK0-0xFFFFFFFF
	OID 1.3.6.1.4.1.3181.10.6.2.82.4.1.7 (filterConfigPortMembers)
management_members	Defines the port membership for the internal management port(s).
	Values <div> <div><i>NONE</i></div> <div>Internal management ports are not a member of this VLAN.</div> </div> <div> <div><i>CPU_1</i></div> <div>Internal management port is a member of this VLAN.</div> </div> <div> <div><i>CPU_2</i></div> <div>Second internal CPU port is member of this VLAN. Note: This setting is only valid for devices with two internal CPU ports.</div> </div> <div> <div><i>ALL</i></div> <div>All available internal management ports are member of this VLAN.</div> </div>
	OID 1.3.6.1.4.1.3181.10.6.2.82.4.1.8 (filterConfigManagementMembers)
priority_override	When enabled the priority value of packets tagged with this VLAN is overwritten with the new_priority value.
	Values enabled, disabled
	OID 1.3.6.1.4.1.3181.10.6.2.82.4.1.9 (filterConfigPriorityOverride)

new_priority	VLAN priority value when priority_override is enabled.
Values	<i>PRIORITY_0</i> Background (lowest) <i>PRIORITY_1</i> Best Effort <i>PRIORITY_2</i> Excellent Effort <i>PRIORITY_3</i> Critical Applications <i>PRIORITY_4</i> Video <i>PRIORITY_5</i> Voice <i>PRIORITY_6</i> Internetwork Control <i>PRIORITY_7</i> Network Control (highest)
OID	1.3.6.1.4.1.3181.10.6.2.82.4.1.10 (filterConfigNewPriority)
Group Path Description	mvrp_port_config , for each port[0..24] Protocol.VLAN.mvrp_port_config[port] Configuration parameter concerning the port specific MVRP settings.
enable_mvrp	Enable MVRP (Multiple VLAN Registration Protocol) on this port.
Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.2.82.6.1.2 (mvrpPortConfigEnableMvrp) 1.3.111.2.802.1.1.4.1.4.5.1.4 (ieee8021QBridgePortMvrpEnabledStatus)
registration_mode	Configuration of the MVRP registration mode.
Values	<i>NORMAL</i> Normal registration mode <i>FIXED</i> Fixed registration mode <i>FORBIDDEN</i> An interface in forbidden registration mode does not participate in MVRP even if MVRP is enabled on the switch
OID	1.3.6.1.4.1.3181.10.6.2.82.6.1.3 (mvrpPortConfigRegistrationMode)
join_timer	Number of milliseconds that the interface must wait before sending MVRP PDUs.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.2.82.6.1.4 (mvrpPortConfigJoinTimer)
leave_timer	Number of milliseconds that the switch retains a VLAN in the Leave state before the VLAN is unregistered. At a minimum, set the leave-timer interval at twice the join-timer interval.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.2.82.6.1.5 (mvrpPortConfigLeaveTimer)

leaveall_timer	Number of milliseconds between the sending of Leave All messages. Value Number in range 0-0xFFFFFFFF OID 1.3.6.1.4.1.3181.10.6.2.82.6.1.6 (mvrpPortConfigLeaveallTimer)
Group Path Description	fabric_attach_port_config , for each port[0..24] Protocol.VLAN.fabric_attach_port_config[port] Configuration parameter controlling the fabric attach feature. Each port can be configured individually.
enable_fabric_attach	Shortest path bridging (SPB) fabric attach feature can be used to simplify configuration in an SBP enabled network. Please also generally enable the LLDP function to use this feature. When enabled the port will act as client to a fabric attach network. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.2.82.7.1.2 (fabricAttachPortConfigEnableFabricAttach) 1.3.111.2.802.1.1.4.1.4.5.1.4 (ieee8021QBridgePortMvrpEnabledStatus)
msg_authentication	when enabled message authentication using the fa_auth key is used. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.2.82.7.1.3 (fabricAttachPortConfigMsgAuthentication) 1.3.111.2.802.1.1.4.1.4.5.1.4 (ieee8021QBridgePortMvrpEnabledStatus)
enter_fa_auth_key	Enter the fabric attach authentication keys required to access the network. No spaces are permitted. Action Execute command with parameter string max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.2.82.7.1.4 (fabricAttachPortConfigEnterFaAuthKey)
encrypted_fa_auth_key	Encrypted form of the entered key. This is automatically filled in when the enter_fa_auth command is executed. Value String, max. 128 characters. OID 1.3.6.1.4.1.3181.10.6.2.82.7.1.5 (fabricAttachPortConfigEncryptedFaAuthKey)

Group Path Description	vlan_id_config Protocol.VLAN.vlan_id_config This section defines some default VLAN settings.
---	---

management_vlan_id	VLAN ID for internal management port. Packets sent by the management agent are tagged with this VLAN ID, Value Number in range 0-4095 OID 1.3.6.1.4.1.3181.10.6.2.82.2.1.2 (vlanIdConfigManagementVlanId)
management_priority	VLAN Priority for internal management port. Packets sent by the internal management agent are tagged with this priority value. Values <i>PRIORITY_0</i> Background (lowest) <i>PRIORITY_1</i> Best Effort <i>PRIORITY_2</i> Excellent Effort <i>PRIORITY_3</i> Critical Applications <i>PRIORITY_4</i> Video <i>PRIORITY_5</i> Voice <i>PRIORITY_6</i> Internetwork Control <i>PRIORITY_7</i> Network Control (highest) OID 1.3.6.1.4.1.3181.10.6.2.82.2.1.3 (vlanIdConfigManagementPriority)
voice_vlan_id	Voice VLAN ID. Special VLAN for IP phones. Value Number in range 0-4095 OID 1.3.6.1.4.1.3181.10.6.2.82.2.1.4 (vlanIdConfigVoiceVlanId)
rstp_vlan_id	RSTP VLAN ID. When using single instance Spanning Tree (STP or RSTP) in combination with VLANs, all spanning tree messages are tagged with this VLAN ID. Value Number in range 0-4095 OID 1.3.6.1.4.1.3181.10.6.2.82.2.1.5 (vlanIdConfigRstpVlanId)
unauthorized_vlan_id	When using port access control with dynamic VLANs, unauthorized ports are attached to this VLAN. Value Number in range 0-4095 OID 1.3.6.1.4.1.3181.10.6.2.82.2.1.6 (vlanIdConfigUnauthorizedVlanId)
smartoffice_vlan_id	VLAN ID used for SmartOffice control traffic between director and controllers. Also used by the SmartOffice GUI. Value Number in range 0-4095 OID 1.3.6.1.4.1.3181.10.6.2.82.2.1.7 (vlanIdConfigSmartofficeVlanId)

26.5 VLAN Status Parameters

Group Path	General Parameters Protocol.VLAN	
number_of_entries	Number of VLAN entries in the table.	
	Value	Number in range 0-65535
	OID	1.3.6.1.4.1.3181.10.6.2.82.100 (vlanNumberOfEntries) 1.3.6.1.2.1.17.7.1.1.4 (dot1qNumVlans)
Group Path Description	status , for all VLAN filters [0..255] Protocol.VLAN.status[VLAN_id] This table lists the status of all defined VLANs.	
vlan_id	VLAN identifier	
	Value	Number in range 0-65535
	OID	1.3.6.1.4.1.3181.10.6.2.82.101.1.2 (statusVlanId)
time_mark		
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.2.82.101.1.3 (statusTimeMark)
alias	Contains the alias name for static entries.	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.82.101.1.4 (statusAlias) 1.3.6.1.2.1.17.7.1.4.3.1.1 (dot1qVlanStaticName)
port_members	Lists all ports that belong to this VLAN.	
	Value	PORTMASK0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.2.82.101.1.5 (statusPortMembers)
filter_database	filter data base	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.2.82.101.1.6 (statusFilterDatabase) 1.3.6.1.2.1.17.7.1.4.2.1.3 (dot1qVlanFdbId)

egress_ports	The set of ports which are transmitting traffic for this VLAN as either tagged or untagged frames.
Value	PORTMASK0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.2.82.101.1.7 (statusEgressPorts) 1.3.6.1.2.1.17.7.1.4.2.1.4 (dot1qVlanCurrentEgressPorts) 1.3.6.1.2.1.17.7.1.4.3.1.2 (dot1qVlanStaticEgressPorts)
untagged_ports	The set of ports which are transmitting traffic for this VLAN as untagged frames.
Value	PORTMASK0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.2.82.101.1.8 (statusUntaggedPorts) 1.3.6.1.2.1.17.7.1.4.2.1.5 (dot1qVlanCurrentUntaggedPorts) 1.3.6.1.2.1.17.7.1.4.3.1.4 (dot1qVlanStaticUntaggedPorts)
fabric_attach_state	Indicates if auto attachment to the fabric was successful.
Values	<i>DISABLED</i> Fabric Attach feature is not enabled <i>ACTIVE</i> This VLAN is successfully attached <i>REJECTED</i> This VLAN was not attached <i>PENDING</i> This network has not responded <i>UNKNOWN</i> The state is unknown
OID	1.3.6.1.4.1.3181.10.6.2.82.101.1.9 (statusFabricAttachState)
fabric_attach_i_sid	This indicates the VLAN to I-SID binding when the shortest path bridging (SPB) fabric attach feature is used.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.2.82.101.1.10 (statusFabricAttachISid)
creation_mode	Indicates by which means this VLAN entry was created.
Values	<i>FILTER_TABLE</i> Static and permanent definition using the vlan_filter table <i>PACC</i> Dynamically allocated through port access control and RADIUS response <i>MVRP</i> Dynamically allocated through MVRP protocol
OID	1.3.6.1.4.1.3181.10.6.2.82.101.1.11 (statusCreationMode) 1.3.6.1.2.1.17.7.1.4.2.1.6 (dot1qVlanStatus)
creation_time	The value of system.uptime when this VLAN was created.
Value	PERIOD0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.2.82.101.1.12 (statusCreationTime) 1.3.6.1.2.1.17.7.1.4.2.1.7 (dot1qVlanCreationTime)

Group	port_status , for each port[0..24]
Path	Protocol.VLAN.port_status[port]
Description	Port related view of the currently active VLAN setup.

assigned_vlan_ids	List of all VLAN ids that are configured or dynamically assigned to this port. Value String, max. 1024 characters. OID 1.3.6.1.4.1.3181.10.6.2.82.102.1.2 (portStatusAssignedVlanIds)								
dynamic_default_vlan_id	Indicates the current port default VLAN. The value may change due to port authentication or configuration. Value Number in range 0-65535 OID 1.3.6.1.4.1.3181.10.6.2.82.102.1.3 (portStatusDynamicDefaultVlanId)								
last_update_method	Indicates what caused the last VLAN reconfiguration. Values <table> <tr> <td><i>CONFIG</i></td><td>The values reflect the static configuration settings.</td></tr> <tr> <td><i>VIA_MAC_TABLE</i></td><td>VLAN set while authenticated via match to local mac_table</td></tr> <tr> <td><i>MAC_VIA_RADIUS</i></td><td>VLAN set while authenticated via a RADIUS server</td></tr> <tr> <td><i>802_1X_VIA_RADIUS</i></td><td>VLAN set while authenticated via using 802.1X protocol. The login was authenticated by a RADIUS server.</td></tr> </table> OID 1.3.6.1.4.1.3181.10.6.2.82.102.1.4 (portStatusLastUpdateMethod)	<i>CONFIG</i>	The values reflect the static configuration settings.	<i>VIA_MAC_TABLE</i>	VLAN set while authenticated via match to local mac_table	<i>MAC_VIA_RADIUS</i>	VLAN set while authenticated via a RADIUS server	<i>802_1X_VIA_RADIUS</i>	VLAN set while authenticated via using 802.1X protocol. The login was authenticated by a RADIUS server.
<i>CONFIG</i>	The values reflect the static configuration settings.								
<i>VIA_MAC_TABLE</i>	VLAN set while authenticated via match to local mac_table								
<i>MAC_VIA_RADIUS</i>	VLAN set while authenticated via a RADIUS server								
<i>802_1X_VIA_RADIUS</i>	VLAN set while authenticated via using 802.1X protocol. The login was authenticated by a RADIUS server.								
last_updating_mac	Indicates which MAC address, if any, was involve in changing the VLAN setting for this port last. Format MAC Address <i>hh-hh-hh-hh-hh-hh</i> (<i>hh</i> = hexadecimal number between 00 to ff) OID 1.3.6.1.4.1.3181.10.6.2.82.102.1.5 (portStatusLastUpdatingMac)								
last_update_time	Indicates the time when the VLAN settings were last changed. Value TIMESTAMP0-0xFFFFFFFF OID 1.3.6.1.4.1.3181.10.6.2.82.102.1.6 (portStatusLastUpdateTime)								

Group	mvrp_status , for each port[0..24]
Path	Protocol.VLAN.mvrp_status[port]
Description	This table lists MVRP status information.

last_source_mac	The Source MAC Address of the last MVRP message received on this port.
Format	MAC Address <i>hh-hh-hh-hh-hh-hh</i> (<i>hh</i> = hexadecimal number between 00 to ff)
OID	1.3.6.1.4.1.3181.10.6.2.82.103.1.2 (mvrpStatusLastSourceMac) 1.3.111.2.802.1.1.4.1.4.5.1.6 (ieee8021QBridgePortMvrpLastPduOrigin)

failed_registrations	The total number of failed MVRP registrations, for any reason, on this port.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.2.82.103.1.3 (mvrpStatusFailedRegistrations) 1.3.111.2.802.1.1.4.1.4.5.1.5 (ieee8021QBridgePortMvrpFailedRegistrations)

27 Quality of Service (QoS)

27.1 Key Features

Priority Queues

4 priority queues per port.

Prioritization Scheme

Strict priority (higher priority always first) or weighted fair queuing (8:4:2:1 highest to lowest).

Layer1 Priority

Static priority queue can be assigned for each port.

Layer2 Priority (802.1p)

Incoming packets are forwarded according to the priority code point in their VLAN tag. The 8 VLAN priority code points can be individually mapped on the 4 priority queues.

Layer3 Priority (IPv4 / IPv6)

Incoming packets are forwarded according to the value of the DiffServ Codepoint (IPv4) / TrafficClass (IPv6) in their IP header. Maximum 64 codepoints are supported. For each code point the corresponding priority queue can be mapped.

Egress Rate Shaping

Egress rate shaping may be used to limit the data traffic coming out of a port. (bandwidth limitation)

Rate shaping can be used to limit the traffic burden an attached device needs to handle.

Ingress Rate Shaping

Ingress rate shaping may be used to limit the amount of data traffic an access port can accept. (bandwidth limitation)

27.2 Functional Description

When enabled, all packets entering the switch are classified for their priority class and placed into the corresponding output queues. The switch hardware supports 4 queues per port to handle four different traffic priorities.

27.2.1 Classification

Prioritisation marking with a higher number of priorities are mapped on these four queues. The mapping can be configured for different methods.

For classification of the priority of incoming packets, the following methods are supported:

DiffServ Codepoint (Layer 3)

The content of the TOS field of the IP header is interpreted as Differentiated Services Codepoint (DSCP) value. For each DSCP (0-63) an individual mapping on the device internal 4 queues is defined.

802.1p VLAN priority field (Layer 2)

The content of the priority field of the VLAN tag is interpreted as priority value. For each VLAN priority value (0-7) an individual mapping on the device internal 4 queues is defined.

Port based priority (Layer 1)

The port the packet is received is interpreted as priority value. For each device port an individual priority directly mapped on the corresponding internal queue is defined.

27.2.2 Prioritisation

When classified, the packet is placed into the corresponding queue of the outgoing port. The transmission scheme of these queues can be selected:

Weighted prioritisation scheme

The content of the 4 queues is sent out with a ratio of 8:4:2:1. This means that when 8 packets of the highest priority queue (queue 3) are sent out, 4 packets of the second highest queue are sent out, then 2 of the second lowest and one of the lowest queue (queue 0). This ensures that highly congested queues do not block lower queues completely.

27.3 QOS CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Protocol.						
	qos.					Quality of Service priority queues
			enable_qos		R/W	Generally enables quality of service functions.
		config[PORT].				This section configures the base QOS settings.
			enable_802dot1p		R/W	Enable prioritization of received packets based on their VLAN priority value according to IEEE 802.1p.
			enable_diffserv		R/W	Enable prioritization of received packets based on the DSCP value in their IP header.
			priority_scheme		R/W	Selection of prioritization method.
			force_default_priority_queue		R/W	When enabled the default_priority_queue value is used for this port.
			default_priority_queue		R/W	Default priority value for port. Received packets are handled according to this setting if VLAN tag and IP header priority is disabled.
		internal.				This section configures the base QOS settings for internal backplane slot to slot connections.
			enable_802dot1p		R/W	Enable prioritization of received packets based on their VLAN priority value according to IEEE 802.1p.
			enable_diffserv		R/W	Enable prioritization of received packets based on the DSCP value in their IP header.
			prioritise_802dot1p		R/W	When both diffserv and 802.1p tags are available use 802.1p.
			priority_scheme		R/W	Selection of prioritization method.
		ieee_802dot1p_prio_mapping.				Mapping of the 8 VLAN priority values on the device internal 4 queues (0-3). 802.1p mapping: Prio 0-7 on Queues 1/0/0/1/2/2/3/3.
			tag_0		R/W	Default value: QUEUE_1

tag_1	R/W	Default value: QUEUE_0
tag_2	R/W	Default value: QUEUE_0
tag_3	R/W	Default value: QUEUE_1
tag_4	R/W	Default value: QUEUE_2
tag_5	R/W	Default value: QUEUE_2
tag_6	R/W	Default value: QUEUE_3
tag_7	R/W	Default value: QUEUE_3
diffserv_prio_mapping[64].		
dscp	R/W	Mapping of the 64 DiffServ Codepoints (0-63) on the device internal queues.
rate_shaping[PORT].		This section defines optional bandwidth limiting features.
egress_bandwidth_percent	R/W	Limits the outgoing frame rate by extending the interframe gap. Egress rate shaping is independent of the frame type. Provide a percentage value of the selected port data rate. Set to 0 or 100 for unlimited normal operation.
ingress_unicast_percent	R/W	Limits the incoming unicast frame rate. Excess unicast frames are dropped and lead to port flow control frames. Provide a percentage value of the selected port data rate. Set to 0 or 100 for unlimited normal operation.
ingress_multicast_percent	R/W	Limits the incoming multicast frame rate. Excess multicast frames are dropped. Provide a percentage value of the selected port data rate. Set to 0 or 100 for unlimited normal operation.
ingress_broadcast_percent	R/W	Limits the incoming broadcast frame rate. Excess broadcast frames are dropped. Provide a percentage value of the selected port data rate. Set to 0 or 100 for unlimited normal operation.
ingress_user_1_percent	R/W	Limits the incoming frames as defined for this group. Excess broadcast frames are dropped. Provide a percentage value of the selected port data rate. Set to 0 or 100 for unlimited normal operation.
ingress_user_2_percent	R/W	Limits the incoming frames as defined for this group. Excess broadcast frames are dropped. Provide a percentage value of the selected port data rate. Set to 0 or 100 for unlimited normal operation.
user_1_frame_types	R/W	Select for which frame types ingress rate shaping should be applied.

user_2_frame_types	R/W	Select for which frame types ingress rate shaping should be applied and which leads to port flow control frames.
egress_multicast_filter	R/W	Suppress multicast traffic to egress on this port. This parameter cannot be used in combination with IGMP snooping.

27.4 QOS Configuration Parameters

Group Path	General Parameters Protocol.QOS
enable_qos	<p>Generally enables quality of service functions.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.83.1 (qosEnableQos)</p>
Group Path Description	config , for each port[0..24] Protocol.QOS.config[port] This section configures the base QOS settings.
enable_802dot1p	<p>Enable prioritization of received packets based on their VLAN priority value according to IEEE 802.1p.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.83.2.1.2 (configEnable802dot1p)</p>
enable_diffserv	<p>Enable prioritization of received packets based on the DSCP value in their IP header.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.83.2.1.3 (configEnableDiffserv)</p>
priority_scheme	<p>Selection of prioritization method.</p> <p>Values <i>WEIGHTED</i> Weighted prioritization of queues (ratio 8:4:2:1) <i>STRICT</i> Highest priority queue is always transmitted first</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.83.2.1.4 (configPriorityScheme)</p>
force_default_priority_queue	<p>When enabled the default_priority_queue value is used for this port.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.83.2.1.5 (configForceDefaultPriorityQueue)</p>

default_priority_queue	Default priority value for port. Received packets are handled according to this setting if VLAN tag and IP header priority is disabled.
Values	<i>QUEUE_0</i> Lowest priority <i>QUEUE_1</i> Default priority <i>QUEUE_2</i> Second highest priority <i>QUEUE_3</i> Highest priority
OID	1.3.6.1.4.1.3181.10.6.2.83.2.1.6 (configDefaultPriorityQueue)

Group Path Description	diffserv_prio_mapping , for all DiffServ CodePoints [0..63] Protocol.QOS.diffserv_prio_mapping[diffserv_codepoint]
dscp	Mapping of the 64 DiffServ Codepoints (0-63) on the device internal queues.
Values	<i>QUEUE_0</i> Lowest priority <i>QUEUE_1</i> Default priority <i>QUEUE_2</i> Second highest priority <i>QUEUE_3</i> Highest priority
OID	1.3.6.1.4.1.3181.10.6.2.83.5.1.2 (diffservPrioMappingDscp)

Group Path Description	rate_shaping , for each port[0..24] Protocol.QOS.rate_shaping[port] This section defines optional bandwidth limiting features.
egress_bandwidth_percent	Limits the outgoing frame rate by extending the interframe gap. Egress rate shaping is independent of the frame type. Provide a percentage value of the selected port data rate. Set to 0 or 100 for unlimited normal operation.
Value	Number in range 0-100
OID	1.3.6.1.4.1.3181.10.6.2.83.6.1.2 (rateShapingEgressBandwidthPercent)
ingress_unicast_percent	Limits the incoming unicast frame rate. Excess unicast frames are dropped and lead to port flow control frames. Provide a percentage value of the selected port data rate. Set to 0 or 100 for unlimited normal operation.
Value	Number in range 0-100
OID	1.3.6.1.4.1.3181.10.6.2.83.6.1.3 (rateShapingIngressUnicastPercent)

ingress_multicast_percent	Limits the incoming multicast frame rate. Excess multicast frames are dropped. Provide a percentage value of the selected port data rate. Set to 0 or 100 for unlimited normal operation.										
Value	Number in range 0-100										
OID	1.3.6.1.4.1.3181.10.6.2.83.6.1.4 (rateShapingIngressMulticastPercent)										
ingress_broadcast_percent	Limits the incoming broadcast frame rate. Excess broadcast frames are dropped. Provide a percentage value of the selected port data rate. Set to 0 or 100 for unlimited normal operation.										
Value	Number in range 0-100										
OID	1.3.6.1.4.1.3181.10.6.2.83.6.1.5 (rateShapingIngressBroadcastPercent)										
ingress_user_1_percent	Limits the incoming frames as defined for this group. Excess broadcast frames are dropped. Provide a percentage value of the selected port data rate. Set to 0 or 100 for unlimited normal operation.										
Value	Number in range 0-100										
OID	1.3.6.1.4.1.3181.10.6.2.83.6.1.6 (rateShapingIngressUser1Percent)										
ingress_user_2_percent	Limits the incoming frames as defined for this group. Excess broadcast frames are dropped. Provide a percentage value of the selected port data rate. Set to 0 or 100 for unlimited normal operation.										
Value	Number in range 0-100										
OID	1.3.6.1.4.1.3181.10.6.2.83.6.1.7 (rateShapingIngressUser2Percent)										
user_1_frame_types	Select for which frame types ingress rate shaping should be applied.										
Values	<table> <tr> <td><i>DISABLED</i></td><td>No special frame checking</td></tr> <tr> <td><i>ARP</i></td><td>Select ARP related frame to prevent malicious ARP flooding</td></tr> <tr> <td><i>TCP_CONTROL</i></td><td>Limit TCP control frames to prevent certain denial of service attacks</td></tr> <tr> <td><i>ARP_AND_TCP_CTRL</i></td><td>Limit ARP and TCP control frames to help prevent denial of service attacks</td></tr> </table>	<i>DISABLED</i>	No special frame checking	<i>ARP</i>	Select ARP related frame to prevent malicious ARP flooding	<i>TCP_CONTROL</i>	Limit TCP control frames to prevent certain denial of service attacks	<i>ARP_AND_TCP_CTRL</i>	Limit ARP and TCP control frames to help prevent denial of service attacks		
<i>DISABLED</i>	No special frame checking										
<i>ARP</i>	Select ARP related frame to prevent malicious ARP flooding										
<i>TCP_CONTROL</i>	Limit TCP control frames to prevent certain denial of service attacks										
<i>ARP_AND_TCP_CTRL</i>	Limit ARP and TCP control frames to help prevent denial of service attacks										
OID	1.3.6.1.4.1.3181.10.6.2.83.6.1.8 (rateShapingUser1FrameTypes)										
user_2_frame_types	Select for which frame types ingress rate shaping should be applied and which leads to port flow control frames.										
Values	<table> <tr> <td><i>DISABLED</i></td><td>No special frame checking</td></tr> <tr> <td><i>UDP_DATA</i></td><td>Limit UDP data traffic</td></tr> <tr> <td><i>TCP_DATA</i></td><td>Limit TCP data traffic</td></tr> <tr> <td><i>UDP_AND_TCP_DATA</i></td><td>Limit UDP and TCP data traffic</td></tr> <tr> <td><i>NON_UDP_TCP_DATA</i></td><td>Limit traffic which is neither based on UDP nor on TCP</td></tr> </table>	<i>DISABLED</i>	No special frame checking	<i>UDP_DATA</i>	Limit UDP data traffic	<i>TCP_DATA</i>	Limit TCP data traffic	<i>UDP_AND_TCP_DATA</i>	Limit UDP and TCP data traffic	<i>NON_UDP_TCP_DATA</i>	Limit traffic which is neither based on UDP nor on TCP
<i>DISABLED</i>	No special frame checking										
<i>UDP_DATA</i>	Limit UDP data traffic										
<i>TCP_DATA</i>	Limit TCP data traffic										
<i>UDP_AND_TCP_DATA</i>	Limit UDP and TCP data traffic										
<i>NON_UDP_TCP_DATA</i>	Limit traffic which is neither based on UDP nor on TCP										
OID	1.3.6.1.4.1.3181.10.6.2.83.6.1.9 (rateShapingUser2FrameTypes)										

egress_multicast_filter	Suppress multicast traffic to egress on this port. This parameter cannot be used in combination with IGMP snooping. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.2.83.6.1.10 (rateShapingEgressMulticastFilter)
--------------------------------	---

Group	internal
Path	Protocol.QOS.internal
Description	This section configures the base QOS settings for internal backplane slot to slot connections.
enable_802dot1p	Enable prioritization of received packets based on their VLAN priority value according to IEEE 802.1p. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.2.83.3.1.2 (internalEnable802dot1p)
enable_diffserv	Enable prioritization of received packets based on the DSCP value in their IP header. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.2.83.3.1.3 (internalEnableDiffserv)
prioritise_802dot1p	When both diffserv and 802.1p tags are available use 802.1p. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.2.83.3.1.4 (internalPrioritise802dot1p)
priority_scheme	Selection of prioritization method. Values <i>WEIGHTED</i> Weighted prioritization of queues (ratio 8:4:2:1) <i>STRICT</i> Highest priority queue is always transmitted first OID 1.3.6.1.4.1.3181.10.6.2.83.3.1.5 (internalPriorityScheme)

Group	ieee_802dot1p_prio_mapping
Path	Protocol.QOS.ieee_802dot1p_prio_mapping
Description	Mapping of the 8 VLAN priority values on the device internal 4 queues (0-3). 802.1p mapping: Prio 0-7 on Queues 1/0/0/1/2/2/3/3.

tag_0	Default value: QUEUE_1
Values	<i>QUEUE_0</i> Lowest priority <i>QUEUE_1</i> Default priority <i>QUEUE_2</i> Second highest priority <i>QUEUE_3</i> Highest priority
OID	1.3.6.1.4.1.3181.10.6.2.83.4.1.2 (ieee802dot1pPrioMappingTag0)
tag_1	Default value: QUEUE_0
Values	<i>QUEUE_0</i> Lowest priority <i>QUEUE_1</i> Default priority <i>QUEUE_2</i> Second highest priority <i>QUEUE_3</i> Highest priority
OID	1.3.6.1.4.1.3181.10.6.2.83.4.1.3 (ieee802dot1pPrioMappingTag1)
tag_2	Default value: QUEUE_0
Values	<i>QUEUE_0</i> Lowest priority <i>QUEUE_1</i> Default priority <i>QUEUE_2</i> Second highest priority <i>QUEUE_3</i> Highest priority
OID	1.3.6.1.4.1.3181.10.6.2.83.4.1.4 (ieee802dot1pPrioMappingTag2)
tag_3	Default value: QUEUE_1
Values	<i>QUEUE_0</i> Lowest priority <i>QUEUE_1</i> Default priority <i>QUEUE_2</i> Second highest priority <i>QUEUE_3</i> Highest priority
OID	1.3.6.1.4.1.3181.10.6.2.83.4.1.5 (ieee802dot1pPrioMappingTag3)
tag_4	Default value: QUEUE_2
Values	<i>QUEUE_0</i> Lowest priority <i>QUEUE_1</i> Default priority <i>QUEUE_2</i> Second highest priority <i>QUEUE_3</i> Highest priority
OID	1.3.6.1.4.1.3181.10.6.2.83.4.1.6 (ieee802dot1pPrioMappingTag4)

tag_5	Default value: QUEUE_2
Values	<i>QUEUE_0</i> Lowest priority <i>QUEUE_1</i> Default priority <i>QUEUE_2</i> Second highest priority <i>QUEUE_3</i> Highest priority
OID	1.3.6.1.4.1.3181.10.6.2.83.4.1.7 (ieee802dot1pPrioMappingTag5)

tag_6	Default value: QUEUE_3
Values	<i>QUEUE_0</i> Lowest priority <i>QUEUE_1</i> Default priority <i>QUEUE_2</i> Second highest priority <i>QUEUE_3</i> Highest priority
OID	1.3.6.1.4.1.3181.10.6.2.83.4.1.8 (ieee802dot1pPrioMappingTag6)

tag_7	Default value: QUEUE_3
Values	<i>QUEUE_0</i> Lowest priority <i>QUEUE_1</i> Default priority <i>QUEUE_2</i> Second highest priority <i>QUEUE_3</i> Highest priority
OID	1.3.6.1.4.1.3181.10.6.2.83.4.1.9 (ieee802dot1pPrioMappingTag7)

28 Rapid Spanning Tree Protocol (RSTP)

28.1 Key Features

Spanning Tree (STP)

Automatic detection of loops and redundant network paths. Single STP instance running in configurable VLAN.

Rapid Spanning Tree (RSTP)

Automatic detection of loops and redundant network paths. Rapid Spanning Tree Protocol (RSTP) is backwards compatible to Spanning Tree standard (STP) but uses a faster algorithm.

Multiple Spanning Tree (MSTP)

Up to 64 STP instances running in configurable VLAN groups.

BPDU Guard

BPDU guard monitors if STP protocol is running on a local access port and removes such packets. Option to shut down the port for security or to just send an event.

This function ensures that no user can accidentally or purposefully hijack all data traffic to path through his computer.

Bridge Assurance

Detects unidirectional link failures that may occur with fiber optic links whereby one fiber direction breaks.

This function ensures that the root bridge does not make false detection about the traffic path under fiber failure conditions.

28.2 Functional Description

28.2.1 Rapid Spanning Tree Protocol (RSTP)

The Spanning Tree Protocol (STP), defined in the IEEE Standard 802.1D, creates a spanning tree within a mesh network of connected layer-2 bridges (typically Ethernet switches) and disables the links which are not part of that tree, leaving a single active path between any two network nodes.

28.2.2 Basic Spanning Tree Operation

Multiple active paths between network nodes cause a bridge loop. Bridge loops create several problems. First, the MAC address table used by the switch or bridge can fail, since the same MAC addresses (and hence the same network hosts) are seen on multiple ports. Second, a broadcast storm occurs. This is caused by broadcast packets being forwarded in an endless loop between switches. A broadcast storm can consume all available CPU resources and bandwidth.

Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manually enabling/disabling these backup links.

28.2.3 Rapid Spanning Tree Improvement

To provide faster spanning tree convergence after a topology change, an evolution of the Spanning Tree Protocol: Rapid Spanning Tree Protocol (RSTP), introduced by IEEE with document 802.1w. RSTP, is a refinement of STP; therefore, it shares most of its basic operation characteristics. This essentially creates a cascading effect away from the root bridge where each designated bridge proposes to its neighbors to determine if it can make a rapid transition. This is one of the major elements which allows RSTP to achieve faster convergence times than STP.

28.3 STP CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Protocol.	stp.	bridge_config.				Spanning Tree (STP), Rapid STP (RSTP) protocol and Multiple STP (MSTP) Protocol
						Configuration parameter concerning the general bridge settings
			mode		R/W	Set base operating mode of spanning tree protocol.
			priority		R/W	The value of the writeable portion of the Bridge ID.
			hello_time		R/W	The amount of time between the transmission of Configuration bridge PDUs by this node on any port when it is the root of the spanning tree, or trying to become so, in seconds.
			max_age		R/W	The maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in seconds.
			forward_delay		R/W	Bridge forward delay in seconds.
			tx_hold_count		R/W	Limits the maximum transmission rate.
			ieee_path_cost_model		R/W	Defines to which standard the admin_path_cost are compliant.
			mstp_region_name		R/W	
			mstp_revision_level		R/W	
			mstp_max_hops		R/W	Defines the initial value of remaining hops for MSTI information generated at the boundary of an MSTI region.
			mstp_stp_aging_time		R/W	This parameter is used only when MSTP is forced into STP mode for rapid aging.
		port_config[PORT].				Configuration parameter concerning the port specific STP settings
			enable		R/W	Enable (R)STP for this port.
			priority		R/W	Port priority value.

admin_p2p_port	R/W	A value of force True indicates that this port should always be treated as if it is connected to a point-to-point link. A value of force False indicates that this port should be treated as having a shared media connection.
admin_edge_port	R/W	When enabled this port is assumed to be an edge port.
admin_path_cost	R/W	The contribution of this port to the path cost of paths towards the spanning tree root which include this port.
protocol_migration	X	When operating in RSTP mode, setting this object forces this port to transmit RSTP BPDUs.
bridge_assurance	R/W	The bridge assurance is used to detect unidirectional link failures or remote devices that stop sending spanning tree information due to a software fault. Important: Only enable when the other directly connected switches also support this feature.
mstp_default_priority	R/W	The port priority used in all MSTP instances unless otherwise configured in mstp_port_priority.
mstp_port_priority	R/W	The port priority used in all specific MSTP instances. Syntax: mstp_id:port_priority. E.g.: 1:32, 2:128, 5:128
mstp_default_admin_path_cost	R/W	The port path cost used in all MSTP instances unless otherwise configured in mstp_port_admin_path_cost.
mstp_port_admin_path_cost	R/W	The port path cost used in specific MSTP instances. Syntax: mstp_id:port_path_cost. E.g.: 1:4, 2:100
bpdu_guard	R/W	When enabled STP attempts from a user port are blocked. This prevents a malicious user from influencing the overall network routing.
bpdu_receive_only	R/W	When enabled this port listens to incoming BPDU packets for spanning tree algorithm but never transmits any.
restrict_tcn	R/W	When enabled the port does not forward topology change notification BPDUs.
restrict_root	R/W	When enabled this port cannot become a root bridge port for the spanning tree protocol.

mstp_group[DYNAMIC].		This table defines MSTP parameter that may be different between instances. The mstp_id is referenced from vlan.filter_config.mstp_group. Several VLAN may share the same MSTP group. If needed up to 63 table entries can be created.
mstp_id	R/W	Defines filter table entry for this MSTP Group Id. This is the key value for the table. Type '=' to edit, use index '['*]' = new_id:' to add an entry. Edit string to nothing to delete entry.
bridge_priority	R/W	The value of the writeable portion of the Bridge ID for this MSTP instance.
bridge_status.		This status table collects all bridge related status fields.
stp_protocol	R	Step protocol specification = 3 for 802.1D.
hello_time	R	The amount of time between the transmission of Configuration bridge PDUs by this node on any port when it is the root of the spanning tree, or trying to become so, in seconds. This is the actual value that this bridge is currently using.
max_age	R	The maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in seconds. This is the actual value that this bridge is currently using.
hold_time	R	This time value determines the interval length during which no more than two Configuration bridge PDUs shall be transmitted by this node, in seconds.
forward_delay	R	This time controls how fast a port changes its spanning state when moving towards the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, which precede the Forwarding state.
root_port	R	The port number of the port that offers the lowest cost path from this bridge to the root bridge.
root_cost	R	The cost of the path to the root as seen from this bridge.

topology_changes	R	The total number of topology changes detected by this bridge since the management entity was last reset or initialized.
last_topology_change	R	The time in seconds when the last time a topology change was detected.
mstp_region_name	R	This the region name actually used.
msti_revision_level	R	This the revision level actually used.
cist_internal_root_path_cost	R	
cist_regional_root_id	R	The Bridge Identifier of the current CIST Regional Root
cist_regional_root_priority	R	The Bridge priority of the current CIST Regional Root
cist_regional_root_mac	R	The Bridge MAC of the current CIST Regional Root
max_hops	R	
mstp_stp_aging_time	R	Aging time of the bridge
port_status[PORT].		
port	R	The port for which these spanning tree information apply.
state	R	This state controls what action a port takes on reception of a frame.
local_port_cost	R	The contribution of this port to the path cost of paths towards the spanning tree root which include this port. This is the actually used value.
designated_port_id	R	The Port priority and identifier of the port on the Designated Bridge for this port's segment. Format: Priority:PortId.
designated_port	R	The Port Identifier of the port on the Designated Bridge for this port's segment.
designated_port_priority	R	The priority of the port on the Designated Bridge for this port's segment.
designated_cost	R	The path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received bridge PDUs.
designated_root_id	R	The priority of the Bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is connected. This is a 4-bit value included along with 12-bit of designated_root_mac as Root Bridge Identifier.

designated_root_mac	R	This contains just the MAC part of the bridge id.
designated_root_priority	R	This contains just the priority part of the bridge id.
designated_bridge_id	R	The priority of the Bridge that this port considers to be the Designated Bridge for this port segment. This is a 4-bit value included along with 12-bit of designated_bridge_mac as Bridge Identifier.
designated_bridge_mac	R	The Bridge Identifier of the bridge that this port considers to be the Designated Bridge for this port's segment.
designated_bridge_priority	R	This contains just the priority part of the bridge id.
forward_transition	R	The number of times this port has transitioned from the Learning state to the Forwarding state.
oper_edge_port	R	A value of true indicates that this port should be assumed as an edge-port.
oper_p2p_port	R	The operational point-to-point status of the LAN segment attached to this port. It indicates whether a port is considered to have a point-to-point connection.
role	R	Assigned port role
inconsistent_bridge	R	A value of true indicates that the port is inconsistent due to Bridge assurance.
mstp_status_table[2048].		This table contains a record for each MSTP instance and for each port thereof. Table ends with first record with mstp_id=0.
mstp_id	R	MSTP instance this entry
port	R	Port id of the port in relation to above MSTP instance.
state	R	This state controls what action a port takes on reception of a frame.
port_priority	R	
internal_admin_path_cost	R	
forward_transition	R	The number of times this port has transitioned from the Learning state to the Forwarding state.
role	R	Assigned port role
mstp_bridge_status[63].		This status table collects all multiple spanning tree bridge related status fields.
mstp_id	R	MSTP instance identifier.
bridge_priority	R	Bridge priority.

root_port	R	The port number of the port that offers the lowest cost path from this bridge to the root bridge.
root_cost	R	The cost of the path to the root as seen from this bridge.
max_hops	R	
regional_root_id	R	The priority of the Bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is connected. This is a 4-bit value included along with 12-bit of designated_root_mac as Root Bridge Identifier.
regional_root_priority	R	This contains just the MAC part of the bridge id.
regional_root_mac	R	This contains just the priority part of the bridge id.
topology_changes	R	The total number of topology changes detected by this most bridge instance since the management entity was last reset or initialized.
last_topology_change	R	The time in seconds when the last time a topology change was detected.

28.4 STP Configuration Parameters

Group	port_config , for each port[0..24]
Path	Protocol.STP.port_config[port]
Description	Configuration parameter concerning the port specific STP settings
enable	<p>Enable (R)STP for this port.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.2.1.2 (portConfigEnable) 1.3.6.1.2.1.17.2.15.1.4 (dot1dStpPortEnable)</p>
priority	<p>Port priority value.</p> <p>Value Number in range 0-240</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.2.1.3 (portConfigPriority) 1.3.6.1.2.1.17.2.15.1.2 (dot1dStpPortPriority)</p>
admin_p2p_port	<p>A value of force True indicates that this port should always be treated as if it is connected to a point-to-point link. A value of force False indicates that this port should be treated as having a shared media connection.</p> <p>Values <i>AUTO</i> <i>FORCE_FALSE</i> Indicates that this port should be treated as having a shared media connection. <i>FORCE_TRUE</i> Indicates that this port should always be treated as if it is connected to a point-to-point link.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.2.1.4 (portConfigAdminP2pPort) 1.3.6.1.2.1.17.2.19.1.4 (dot1dStpPortAdminPointToPoint)</p>
admin_edge_port	<p>When enabled this port is assumed to be an edge port.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.2.1.5 (portConfigAdminEdgePort) 1.3.6.1.2.1.17.2.19.1.2 (dot1dStpPortAdminEdgePort)</p>
admin_path_cost	<p>The contribution of this port to the path cost of paths towards the spanning tree root which include this port.</p> <p>Value Number in range 0-2000000000</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.2.1.6 (portConfigAdminPathCost) 1.3.6.1.2.1.17.2.19.1.6 (dot1dStpPortAdminPathCost)</p>

protocol_migration	<p>When operating in RSTP mode, setting this object forces this port to transmit RSTP BPDUs.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.2.1.7 (portConfigProtocolMigration) 1.3.6.1.2.1.17.2.19.1.1 (dot1dStpPortProtocolMigration)</p>
bridge_assurance	<p>The bridge assurance is used to detect unidirectional link failures or remote devices that stop sending spanning tree information due to a software fault. Important: Only enable when the other directly connected switches also support this feature.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.2.1.8 (portConfigBridgeAssurance)</p>
mstp_default_priority	<p>The port priority used in all MSTP instances unless otherwise configured in mstp_port_priority.</p> <p>Value Number in range 0-240</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.2.1.9 (portConfigMstpDefaultPriority) 1.3.6.1.2.1.17.2.19.1.1 (dot1dStpPortProtocolMigration)</p>
mstp_port_priority	<p>The port priority used in all specific MSTP instances. Syntax: mstp_id:port_priority. E.g.: 1:32, 2:128, 5:128</p> <p>Value String, max. 256 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.2.1.10 (portConfigMstpPortPriority)</p>
mstp_default_admin_path_cost	<p>The port path cost used in all MSTP instances unless otherwise configured in mstp_port_admin_path_cost.</p> <p>Value Number in range 0-200000000</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.2.1.11 (portConfigMstpDefaultAdminPathCost)</p>
mstp_port_admin_path_cost	<p>The port path cost used in specific MSTP instances. Syntax: mstp_id:port_path_cost. E.g.: 1:4, 2:100</p> <p>Value String, max. 256 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.2.1.12 (portConfigMstpPortAdminPathCost)</p>

bpdu_guard	When enabled STP attempts from a user port are blocked. This prevents a malicious user from influencing the overall network routing.
Values	<div> <div><i>DISABLED</i></div> <div>STP BPDU frames are not removed</div> </div> <div> <div><i>DROP_AND_EVENT</i></div> <div>STP BPDU frames are removed and event is send</div> </div> <div> <div><i>BLOCK_PORT</i></div> <div>Port is blocked when STP BPDU is detected. Needs operator intervention to unblock</div> </div>
OID	1.3.6.1.4.1.3181.10.6.2.42.2.1.13 (portConfigBpduGuard)
bpdu_receive_only	When enabled this port listens to incoming BPDU packets for spanning tree algorithm but never transmits any.
Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.2.42.2.1.14 (portConfigBpduReceiveOnly)
restrict_tcn	When enabled the port does not forward topology change notification BPDUs.
Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.2.42.2.1.15 (portConfigRestrictTcn)
restrict_root	When enabled this port cannot become a root bridge port for the spanning tree protocol.
Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.2.42.2.1.16 (portConfigRestrictRoot)
Group Path Description	mstp_group , dynamical size Protocol.STP.mstp_group This table defines MSTP parameter that may be different between instances. The mstp_id is referenced from vlan.filter_config.mstp_group. Several VLAN may share the same MSTP group. If needed up to 63 table entries can be created.
mstp_id	Defines filter table entry for this MSTP Group Id. This is the key value for the table. Type '=' to edit, use index '['*] = new_id:' to add an entry. Edit string to nothing to delete entry.
Value	String, max. 4 characters.
OID	1.3.6.1.4.1.3181.10.6.2.42.3.1.2 (mstpGroupMstpId)
bridge_priority	The value of the writeable portion of the Bridge ID for this MSTP instance.
Value	Number in range 0-61440
OID	1.3.6.1.4.1.3181.10.6.2.42.3.1.3 (mstpGroupBridgePriority)

Group	bridge_config
Path	Protocol.STP.bridge_config
Description	Configuration parameter concerning the general bridge settings
mode	<p>Set base operating mode of spanning tree protocol.</p> <p>Values</p> <p><i>DISABLED</i> STP disabled</p> <p><i>STP</i> Spanning Tree Protocol</p> <p><i>RSTP</i> Rapid Spanning Tree Protocol</p> <p><i>MSTP</i> Multiple Spanning Tree Protocol</p> <p>OID</p> <p>1.3.6.1.4.1.3181.10.6.2.42.1.1.2 (bridgeConfigMode)</p> <p>1.3.6.1.2.1.17.2.16 (dot1dStpVersion)</p>
priority	<p>The value of the writeable portion of the Bridge ID.</p> <p>Value</p> <p>Number in range 0-61440</p> <p>OID</p> <p>1.3.6.1.4.1.3181.10.6.2.42.1.1.3 (bridgeConfigPriority)</p> <p>1.3.6.1.2.1.17.2.2 (dot1dStpPriority)</p>
hello_time	<p>The amount of time between the transmission of Configuration bridge PDUs by this node on any port when it is the root of the spanning tree, or trying to become so, in seconds.</p> <p>Value</p> <p>Number in range 1-10</p> <p>OID</p> <p>1.3.6.1.4.1.3181.10.6.2.42.1.1.4 (bridgeConfigHelloTime)</p> <p>1.3.6.1.2.1.17.2.13 (dot1dStpBridgeHelloTime)</p>
max_age	<p>The maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in seconds.</p> <p>Value</p> <p>Number in range 6-40</p> <p>OID</p> <p>1.3.6.1.4.1.3181.10.6.2.42.1.1.5 (bridgeConfigMaxAge)</p> <p>1.3.6.1.2.1.17.2.12 (dot1dStpBridgeMaxAge)</p>
forward_delay	<p>Bridge forward delay in seconds.</p> <p>Value</p> <p>Number in range 4-30</p> <p>OID</p> <p>1.3.6.1.4.1.3181.10.6.2.42.1.1.6 (bridgeConfigForwardDelay)</p> <p>1.3.6.1.2.1.17.2.14 (dot1dStpBridgeForwardDelay)</p>
tx_hold_count	<p>Limits the maximum transmission rate.</p> <p>Value</p> <p>Number in range 1-10</p> <p>OID</p> <p>1.3.6.1.4.1.3181.10.6.2.42.1.1.7 (bridgeConfigTxHoldCount)</p> <p>1.3.6.1.2.1.17.2.17 (dot1dStpTxHoldCount)</p>

ieee_path_cost_model Defines to which standard the admin_path_cost are compliant.

Values *1998_COMPLIANT* IEEE-802.1D-1998
 2004_COMPLIANT IEEE-802.1D-2004

OID 1.3.6.1.4.1.3181.10.6.2.42.1.1.8
 (bridgeConfigIeeePathCostModel)

mstp_region_name

Value String, max. 32 characters.

OID 1.3.6.1.4.1.3181.10.6.2.42.1.1.9
 (bridgeConfigMstpRegionName)

mstp_revision_level

Value Number in range 0-65535

OID 1.3.6.1.4.1.3181.10.6.2.42.1.1.10
 (bridgeConfigMstpRevisionLevel)

mstp_max_hops Defines the initial value of remaining hops for MSTI information generated at the boundary of an MSTI region.

Value Number in range 6-40

OID 1.3.6.1.4.1.3181.10.6.2.42.1.1.11 (bridgeConfigMstpMaxHops)

mstp_stp_aging_time This parameter is used only when MSTP is forced into STP mode for rapid aging.

Value Number in range 10-1000000

OID 1.3.6.1.4.1.3181.10.6.2.42.1.1.12
 (bridgeConfigMstpStpAgingTime)

28.5 STP Status Parameters

Group	port_status , for all ports[0..31]														
Path	Protocol.STP.port_status[port]														
Description															
port	<p>The port for which these spanning tree information apply.</p> <p>Value PORT0-255</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.101.1.2 (portStatusPort)</p>														
state	<p>This state controls what action a port takes on reception of a frame.</p> <p>Values</p> <table> <tr><td><i>UNKNOWN</i></td><td>Unknown</td></tr> <tr><td><i>DISCARDING</i></td><td>Discarding state</td></tr> <tr><td><i>LEARNING</i></td><td>Learning state</td></tr> <tr><td><i>FORWARDING</i></td><td>Forwarding state</td></tr> <tr><td><i>BLOCKING</i></td><td>Blocking state</td></tr> <tr><td><i>LISTENING</i></td><td>Listening state</td></tr> <tr><td><i>BROKEN</i></td><td>Broken state</td></tr> </table> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.101.1.3 (portStatusState) 1.3.6.1.2.1.17.2.15.1.3 (dot1dStpPortState)</p>	<i>UNKNOWN</i>	Unknown	<i>DISCARDING</i>	Discarding state	<i>LEARNING</i>	Learning state	<i>FORWARDING</i>	Forwarding state	<i>BLOCKING</i>	Blocking state	<i>LISTENING</i>	Listening state	<i>BROKEN</i>	Broken state
<i>UNKNOWN</i>	Unknown														
<i>DISCARDING</i>	Discarding state														
<i>LEARNING</i>	Learning state														
<i>FORWARDING</i>	Forwarding state														
<i>BLOCKING</i>	Blocking state														
<i>LISTENING</i>	Listening state														
<i>BROKEN</i>	Broken state														
local_port_cost	<p>The contribution of this port to the path cost of paths towards the spanning tree root which include this port. This is the actually used value.</p> <p>Value Number in range 0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.101.1.4 (portStatusLocalPortCost)</p>														
designated_port_id	<p>The Port priority and identifier of the port on the Designated Bridge for this port's segment. Format: Priority:PortId.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.101.1.5 (portStatusDesignatedPortId) 1.3.6.1.2.1.17.2.15.1.9 (dot1dStpPortDesignatedPort)</p>														
designated_port	<p>The Port Identifier of the port on the Designated Bridge for this port's segment.</p> <p>Value Number in range 0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.101.1.6 (portStatusDesignatedPort)</p>														
designated_port_priority	<p>The priority of the port on the Designated Bridge for this port's segment.</p> <p>Value Number in range 0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.101.1.7 (portStatusDesignatedPortPriority)</p>														

designated_cost	<p>The path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received bridge PDUs.</p> <p>Value Number in range 0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.101.1.8 (portStatusDesignatedCost) 1.3.6.1.2.1.17.2.15.1.7 (dot1dStpPortDesignatedCost)</p>
designated_root_id	<p>The priority of the Bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is connected. This is a 4-bit value included along with 12-bit of designated_root_mac as Root Bridge Identifier.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.101.1.9 (portStatusDesignatedRootId) 1.3.6.1.2.1.172.15.1.6 (dot1dStpPortDesignatedRoot)</p>
designated_root_mac	<p>This contains just the MAC part of the bridge id.</p> <p>Format MAC Address <i>hh-hh-hh-hh-hh-hh</i> (<i>hh</i> = hexadecimal number between 00 to ff)</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.101.1.10 (portStatusDesignatedRootMac)</p>
designated_root_priority	<p>This contains just the priority part of the bridge id.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.101.1.11 (portStatusDesignatedRootPriority)</p>
designated_bridge_id	<p>The priority of the Bridge that this port considers to be the Designated Bridge for this port segment. This is a 4-bit value included along with 12-bit of designated_bridge_mac as Bridge Identifier.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.101.1.12 (portStatusDesignatedBridgeId) 1.3.6.1.2.1.17.2.15.1.8 (dot1dStpPortDesignatedBridge)</p>
designated_bridge_mac	<p>The Bridge Identifier of the bridge that this port considers to be the Designated Bridge for this port's segment.</p> <p>Format MAC Address <i>hh-hh-hh-hh-hh-hh</i> (<i>hh</i> = hexadecimal number between 00 to ff)</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.101.1.13 (portStatusDesignatedBridgeMac)</p>
designated_bridge_priority	<p>This contains just the priority part of the bridge id.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.101.1.14 (portStatusDesignatedBridgePriority)</p>

forward_transition	<p>The number of times this port has transitioned from the Learning state to the Forwarding state.</p> <p>Value Number in range 0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.101.1.15 (portStatusForwardTransition) 1.3.6.1.2.1.17.2.15.1.10 (dot1dStpPortForwardTransitions)</p>
oper_edge_port	<p>A value of true indicates that this port should be assumed as an edge-port.</p> <p>Values true, false</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.101.1.16 (portStatusOperEdgePort) 1.3.6.1.2.1.17.2.19.1.3 (dot1dStpPortOperEdgePort)</p>
oper_p2p_port	<p>The operational point-to-point status of the LAN segment attached to this port. It indicates whether a port is considered to have a point-to-point connection.</p> <p>Values true, false</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.101.1.17 (portStatusOperP2pPort) 1.3.6.1.2.1.17.2.19.1.5 (dot1dStpPortOperPointToPoint)</p>
role	<p>Assigned port role</p> <p>Values <i>UNKNOWN</i> Unknown <i>ROOT</i> Root bridge <i>DESIGNATED</i> Designated bridge <i>ALTERNATE</i> Alternate bridge <i>BACKUP</i> Backup bridge <i>MASTER</i> Master bridge <i>DISABLED</i> Disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.101.1.18 (portStatusRole)</p>
inconsistent_bridge	<p>A value of true indicates that the port is inconsistent due to Bridge assurance.</p> <p>Values true, false</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.101.1.19 (portStatusInconsistentBridge)</p>

Group	bridge_status
Path	Protocol.STP.bridge_status
Description	This status table collects all bridge related status fields.
stp_protocol	<p>Step protocol specification = 3 for 802.1D.</p> <p>Value Number in range 0-255</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.100.1.2 (bridgeStatusStpProtocol) 1.3.6.1.2.1.17.2.1 (dot1dStpProtocolSpecification)</p>
hello_time	<p>The amount of time between the transmission of Configuration bridge PDUs by this node on any port when it is the root of the spanning tree, or trying to become so, in seconds. This is the actual value that this bridge is currently using.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.100.1.3 (bridgeStatusHelloTime) 1.3.6.1.2.1.17.2.9 (dot1dStpHelloTime)</p>
max_age	<p>The maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in seconds. This is the actual value that this bridge is currently using.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.100.1.4 (bridgeStatusMaxAge) 1.3.6.1.2.1.17.2.8 (dot1dStpMaxAge)</p>
hold_time	<p>This time value determines the interval length during which no more than two Configuration bridge PDUs shall be transmitted by this node, in seconds.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.100.1.5 (bridgeStatusHoldTime) 1.3.6.1.2.1.17.2.10 (dot1dStpHoldTime)</p>
forward_delay	<p>This time controls how fast a port changes its spanning state when moving towards the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, which precede the Forwarding state.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.100.1.6 (bridgeStatusForwardDelay) 1.3.6.1.2.1.17.2.11 (dot1dStpForwardDelay)</p>
root_port	<p>The port number of the port that offers the lowest cost path from this bridge to the root bridge.</p> <p>Value PORT0-255</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.42.100.1.7 (bridgeStatusRootPort) 1.3.6.1.2.1.17.2.7 (dot1dStpRootPort)</p>

root_cost	The cost of the path to the root as seen from this bridge.
	Value Number in range 0-0xFFFFFFFF
	OID 1.3.6.1.4.1.3181.10.6.2.42.100.1.8 (bridgeStatusRootCost) 1.3.6.1.2.1.17.2.6 (dot1dStpRootCost)
topology_changes	The total number of topology changes detected by this bridge since the management entity was last reset or initialized.
	Value Number in range 0-65535
	OID 1.3.6.1.4.1.3181.10.6.2.42.100.1.9 (bridgeStatusTopologyChanges) 1.3.6.1.2.1.17.2.4 (dot1dStpTopChanges)
last_topology_change	The time in seconds when the last time a topology change was detected.
	Value PERIOD0-0xFFFFFFFF
	OID 1.3.6.1.4.1.3181.10.6.2.42.100.1.10 (bridgeStatusLastTopologyChange) 1.3.6.1.2.1.17.2.3 (dot1dStpTimeSinceTopologyChange)
mstp_region_name	This the region name actually used.
	Value String, max. 32 characters.
	OID 1.3.6.1.4.1.3181.10.6.2.42.100.1.11 (bridgeStatusMstpRegionName)
msti_revision_level	This the revision level actually used.
	Value Number in range 0-65535
	OID 1.3.6.1.4.1.3181.10.6.2.42.100.1.12 (bridgeStatusMstiRevisionLevel)
cist_internal_root_path_cost	Value Number in range 0-0xFFFFFFFF
	OID 1.3.6.1.4.1.3181.10.6.2.42.100.1.13 (bridgeStatusCistInternalRootPathCost)
cist_regional_root_id	The Bridge Identifier of the current CIST Regional Root
	Value String, max. 32 characters.
	OID 1.3.6.1.4.1.3181.10.6.2.42.100.1.14 (bridgeStatusCistRegionalRootId)
cist_regional_root_priority	The Bridge priority of the current CIST Regional Root
	Value Number in range 0-0xFFFFFFFF
	OID 1.3.6.1.4.1.3181.10.6.2.42.100.1.15 (bridgeStatusCistRegionalRootPriority)

cist_regional_root_mac	The Bridge MAC of the current CIST Regional Root
Format	MAC Address <i>hh-hh-hh-hh-hh-hh</i> (<i>hh</i> = hexadecimal number between 00 to ff)
OID	1.3.6.1.4.1.3181.10.6.2.42.100.1.16 (bridgeStatusCistRegionalRootMac)

max_hops	
Value	Number in range 0-65535
OID	1.3.6.1.4.1.3181.10.6.2.42.100.1.17 (bridgeStatusMaxHops)

mstp_stp_aging_time	Aging time of the bridge
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.2.42.100.1.18 (bridgeStatusMstpStpAgingTime)

29 Port-based Access Control

29.1 Key Features

IEEE 802.1X Authentication

Multiple users can be authenticated using central RADIUS server based on username/password or certificate.

By using RADIUS a network wide authentication database can be used. This eliminates the need to configure each unit separately.

IEEE 802.1X Supplicant

An IEEE 802.1X Supplicant can authenticate the device at the port access controlled uplink port. Username/password and certificate based methods are supported (EAP-MD5, PEAP).

The switch can perform authentication on behalf of the attached device. Useful for devices that do not support authentication themselves.

RADIUS MAC Authentication

Multiple users can be authenticated using central RADIUS server based on their MAC addresses.

By using RADIUS a network wide authentication database can be used. This eliminates the need to configure each unit separately.

MAC locking

Multiple users can be authenticated based on their MAC addresses. Unlimited MAC addresses can be configured manually or automatically. Possibility to mix and match vendor MACs and specific MACs

This permits MAC based authentication in the absence of a centralized RADIUS setup. Strict manual security.

MAC learning

Up to 9 MAC addresses may be learned per port. Learned addresses are stored in the configuration. MAC learning can be preset prior to roll out. Simply the first n devices connected are automatically learned.

MAC learning simplifies initial configuration by eliminating the need to know the MAC addresses.

Limited number of MACs

A port may be limited to accept only a configurable number of MACs on a given port (1 - 255). Additional MACs are blocked in the hardware layer.

This is an effective method to protect against Denial-of-Service attacks caused by MAC storms.

Limited number of MACs per VLAN

A port may be limited to accept only a configurable number of MACs on a given port (1 - 255) and VLAN..

This is an effective method to protect against Denial-of-Service attacks caused by MAC storms.

Learned MAC time out

Time out of learned MACs to allow another computer to connect in MAC locking environment. Permits reuse of purposefully limited MACs on a given port.

Dynamic VLAN

RADIUS server can provide user specific VLAN ID using tunnel-attribute in accept message. Port VLAN is dynamically set accordingly. Unauthorized users may be placed in an unauthorized VLAN ('guest VLAN') or blocked completely. VLAN 4096 can be specified to indicate port default VLAN.

Allowed Outgoing Port (Port based VLANs)

This feature is used to limit the outgoing traffic for each port to certain destination ports. This feature is also known as port based VLAN.

Can for example be used to isolate user ports when switch is used as Internet access gateway.

IP Address Logging

The IP address of the connected user is detected via ARP snooping. User IP address information can be logged locally and using RADIUS accounting function.

Useful when switch is used in public internet provider situation where user information must be logged for legal reasons.

Wake-on-Lan support

A solution to send out Wake-on-LAN packets on a PACC blocked port. This feature is also called Unidirectional Controlled Port or Admin Controlled Directions in the IEEE 802.1X-2004 specification.

This feature is used to permit the use of Wake-On-Lan in combination with 802.1X authentication

Network Edge Authentication

The network edge authentication mode is used to authenticate a "supplicant switch" connected to a downlink port of the switch. After successful authentication the port should be open for any traffic from the downstream switch. Similar to Cisco NEAT feature.

This feature authenticates an authentication switch placed outside a wiring closet with an authentication switch placed in the wiring closet

Authentication Fail Retry Timer

When authentication has failed, the authentication is restarted after the defined time in seconds.

This is useful for unattended devices using MAC authentication or when access rights are centrally changed on the RADIUS server and the end unit cannot be reauthenticated manually.

29.2 Functional Description

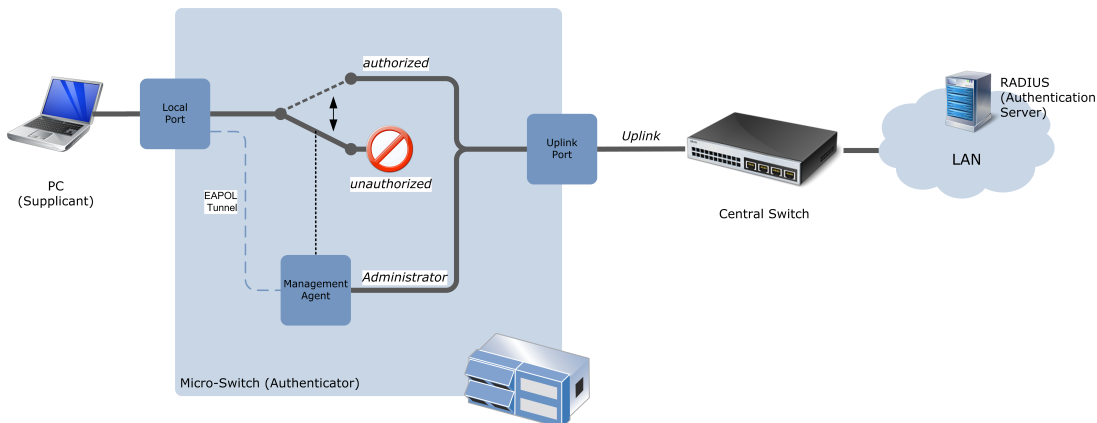
29.2.1 Introduction

With the growing number of LANs available for public access (Hotels, Hospitals, Universities, Conference Rooms, etc.), the physical control of access to restricted LANs is no more practical. Furthermore, even without a successful server login, already the access to the network can become a security threat (Denial of Service attacks, spoofing etc.). To address these security issues, the IEEE defined a standard to secure network ports already at the port level, thus preventing

unauthorized access directly at the edge. MICROSENS Micro Switches are designed to support different methods of port based access control, including IEEE Std. 802.1X.

IEEE 802.1X Authentication

A user (Supplicant) requests network access via the switch it is connected to (Authenticator) by presenting his credentials (username/password or certificate) to a RADIUS server (Authentication Server). When successfully verified by the RADIUS server, the switch port is opened, otherwise the network access remains blocked or limited.



If the supplicant does not support IEEE 802.1X authentication, an automatic fallback to authentication via user MAC address only is possible (configuration option).

RADIUS MAC Authentication

A user is identified by his MAC address only. This MAC address is checked by a RADIUS server. When successfully verified by the RADIUS server, the switch port the user is connected to is opened, otherwise the network access remains blocked or limited.

MAC Locking

If there is no central authentication server in the network, the network access can be locally restricted to a maximum of four MAC addresses per port. These MAC addresses can either be configured statically or the first MAC addresses learned on the port can be used. These authorized MAC addresses are then stored permanently in the switch.

Force-authorized

In this mode, the port is always forwarding all traffic. If VLAN filtering is enabled, the static VLAN configuration is valid. VLAN dependent settings for RADIUS based authentication modes are ignored.

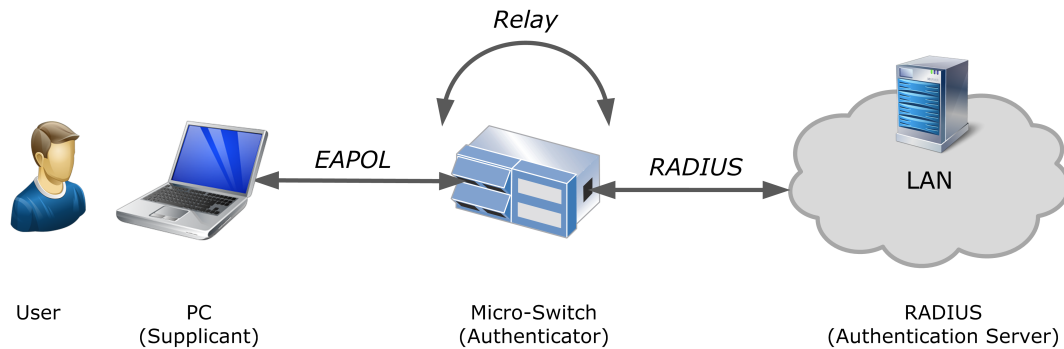
Force-unauthorized

In this mode, the port is permanently blocking all traffic. All other authentication mode settings are ignored.

29.2.2 IEEE 802.1X Authentication

System setup

An IEEE 802.1X compliant Port Based Network Access Control system consists of three components:



Supplicant

The supplicant is the device requesting access to the network. This is typically a PC, Printer, VoIP phone etc. The supplicant must implement an IEEE 802.1X compliant client which handles the communication during the authentication process.

Authenticator

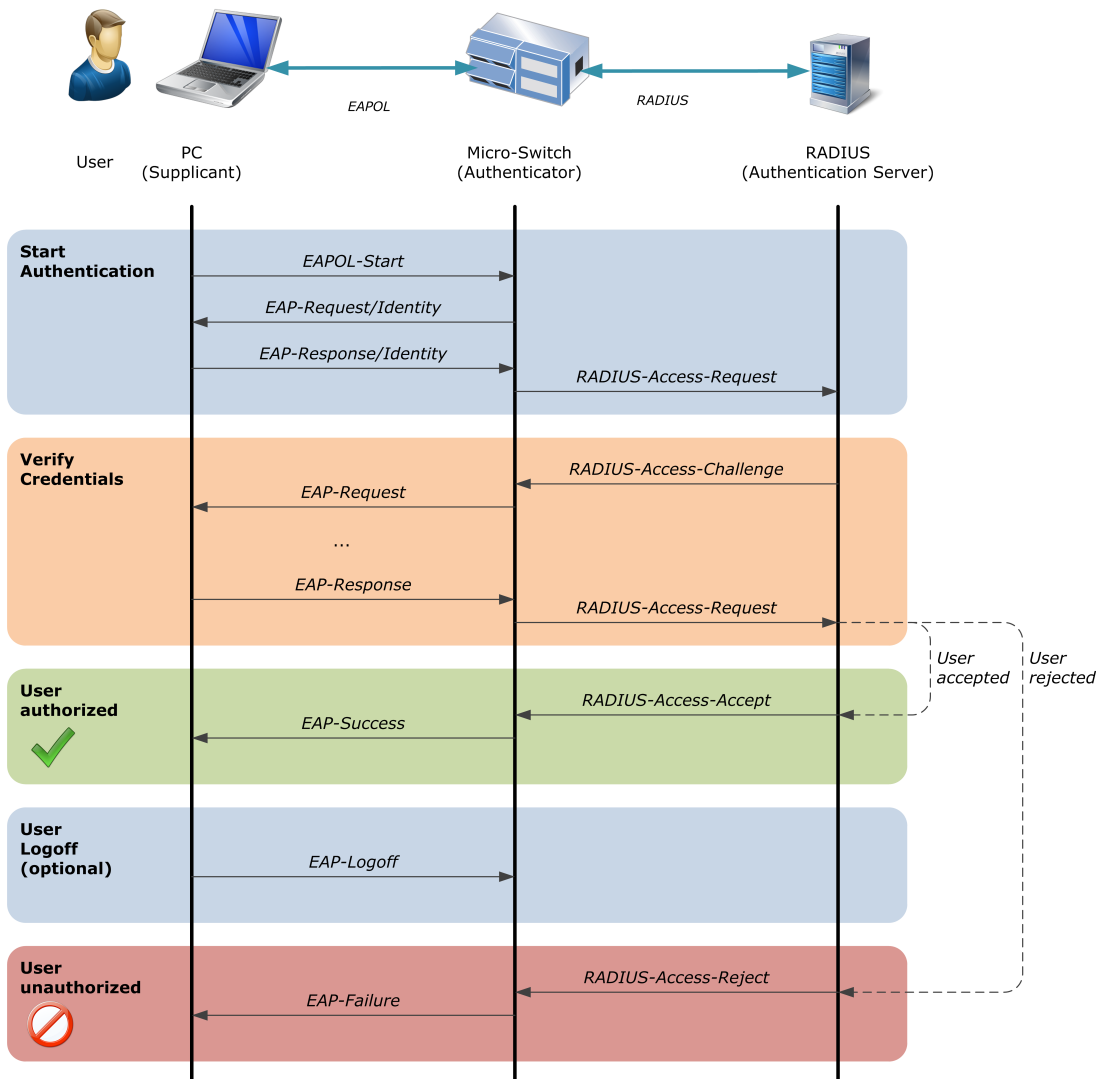
The authenticator is the switch by which the supplicant is connected to the network. The authenticator controls the network access of the supplicant and acts as a transfer agent between the supplicant and the authentication server during the authentication process. It forwards EAPOL packets encapsulated in RADIUS protocol to the authentication server.

Authentication Server

The authentication server is a RADIUS (Remote Authentication Dial In User Service) server hosting the user database. It validates the supplicant's access request. Depending on the result of the user validation, the server sends an 'Accept' or 'Reject' message to the authenticator to adjust the supplicant's network access accordingly.

IEEE 802.1X Communication flow

During the authentication process, supplicant and authentication server are communicating indirectly by the authenticator. The supplicant communicates with the authenticator using the EAPOL protocol, whereas the authenticator communicates with the authentication server using the RADIUS protocol. The authenticator acts as a transfer agent between the two protocols during the authentication process.



Upon link up, the authentication process can either be initiated by the supplicant sending a 'EAPOL_Start' message or by the authenticator sending a 'Request_Identity' message. The supplicant reacts with a 'Response_Identity' message. This message is encapsulated by the authenticator and sent to the RADIUS server (authentication server).

The RADIUS server verifies the supplicant's identity. If the identity is known, the RADIUS initiates the authentication challenge process. Different protocols can be used, depending on the RADIUS configuration:

- **EAP-MD5:** RADIUS server obtains user password via MD5 challenge method
- **EAP-PEAP:** Protected EAP
- **PEAP:** is a joint proposal by Cisco Systems, Microsoft and RSA Security as an open standard. Protocols supported: PEAP/EAP-MSCHAPv2
- **EAP-TTLS:** Tunnelled TLS with standard inner authentication protocols: EAP-MD5, EAP-TLS, PAP, MSCHAPv2
- **EAP-TLS:** Transport Layer Security

When the user is authenticated successfully, the RADIUS server finally sends an 'RADIUS-Access-Accept' message to the authenticator. This causes the authenticator to grant the supplicant access to the network. The authenticator confirms the authorization to the supplicant by sending a 'EAP-Success' message. The authentication process terminates.

29.2.3 RADIUS MAC Authentication

In this mode, the user is authorized based on its MAC address. This is very useful to connect non-IEEE Std. 802.1X devices like VoIP-phones, printers or Wi-Fi access points to the network without generating a security leak.

ATTENTION: Authenticating a supplicant based on its MAC address only is not as strong as the use of IEEE 802.1X authentication protocols. MAC addresses can be copied easily, so an intruder can get network access if he is able to clone an authorized MAC address.

The MAC address must be registered as a valid user in the RADIUS user database. To authenticate a MAC address on a RADIUS server, the MAC address is treated as username by the RADIUS. The format of the MAC address field and the value used for the password can be configured.

A maximum of 4 MAC addresses are permitted on a port. If the maximum number of permitted users is exceeded, the whole port becomes unauthorized for all users.

As long as the MAC discovery phase is not finalized, the network port is blocked to prevent any network interference.

29.3 PACC Configuration Parameters

Group Path	General Parameters
	Protocol.PACC
enable_port_access_control	<p>Generally enables the port access control function.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.1 (paccEnablePortAccessControl) 1.0.8802.1.1.1.1.1.1 (dot1xPaeSystemAuthControl)</p>
reauthentication_period	<p>EAP reauthentication period in seconds. To disable reauthentication set value to 0.</p> <p>Value Number in range 0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.2 (paccReauthenticationPeriod)</p>
nas_identifier	<p>Optional NAS-Identifier string for RADIUS messages.</p> <p>Value String, max. 256 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.3 (paccNasIdentifier)</p>
mac_separator_char	<p>Defines the character which separates the bytes of a MAC address.</p> <p>Value String, max. 2 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.4 (paccMacSeparatorChar)</p>
mac_spelling	<p>Defines in which case the MAC is defined.</p> <p>Values <i>LOWER_CASE</i> MAC address written in lower case <i>UPPER_CASE</i> MAC address written in upper case</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.5 (paccMacSpelling)</p>
mac_password_source	<p>Defines if MAC or Password is used for authentication.</p> <p>Values <i>USE_MAC</i> Use MAC <i>USE_PASSWORD</i> Use password</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.6 (paccMacPasswordSource)</p>
mac_password_string	<p>User defined password string.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.7 (paccMacPasswordString)</p>
primary_auth_server_name	<p>Symbolic name of the RADIUS server used for authentication.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.8 (paccPrimaryAuthServerName)</p>

primary_acct_server_name	Symbolic name of the RADIUS server used for accounting. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.2.46.9 (paccPrimaryAcctServerName)
fallback_auth_server_name	Symbolic name of the RADIUS server used for authentication if the primary server is down. Leave empty when no fallback is required. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.2.46.10 (paccFallbackAuthServerName)
fallback_acct_server_name	Symbolic name of the RADIUS server used for accounting if the primary server is down. Leave empty when no fallback is required. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.2.46.11 (paccFallbackAcctServerName)
server_down_timeout	Retry interval in seconds for trying to return to the primary RADIUS server. Value Number in range 0-65535 OID 1.3.6.1.4.1.3181.10.6.2.46.12 (paccServerDownTimeout)
filter_authorized_mac	Filter user_status table to show only entries for specified MAC. Supply MAC address as parameter. Enter only the first 3 value pairs of the MAC to search for vendor MACs. Syntax example: mac.filter_mac = 01:22:3A. Action Execute command with parameter string max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.2.46.13 (paccFilterAuthorizedMac)
filter_authorized_port	Filter user_status table to show only entries associated with a given port range. The shorthand port format like 1 for 1/1 may be used. Syntax examples: mac.filter_port = 1/1,2/5 or mac.filter_port = 1-3,5. Action Execute command with parameter string max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.2.46.14 (paccFilterAuthorizedPort)
filter_authorized_user	Filter user_status table to show only entries for the given user name. Wildcards *name* automatically apply so that only a part of the expected name needs to be supplied. Action Execute command with parameter string max. 128 characters. OID 1.3.6.1.4.1.3181.10.6.2.46.15 (paccFilterAuthorizedUser)

Group
Path
Description

port_config, for each port[0..24]
Protocol.PACC.port_config[port]

authorize_mode	Defines method for authorization of user on port.	
Values	<i>ALWAYS_AUTHORIZED</i>	Port access control is not used for this port. The port is always in forwarding state.
	<i>VIA_MAC_TABLE</i>	Received MAC address is locally checked against <i>mac_table</i> . If matched, the port is set to forwarding state.
	<i>MAC_VIA_RADIUS</i>	Received MAC address is authenticated by a RADIUS server.
	<i>802_1X_VIA_RADIUS</i>	802.1X protocol is used (login on the Ethernet port). The login is authenticated by a RADIUS server.
	<i>MAC_OR_802_1X_VIA_RADIUS</i>	Both RADIUS based mechanisms are used. When at least one method matches, the port is set to forwarding state.
	<i>FORCE_UNAUTHORIZED</i>	Port is set port to the unauthorized state and <i>unauthorized_mode</i> setting applies
	<i>MAC_EVENT_ONLY</i>	Port is always authorized plus for each new MAC a <i>MAC_ACCEPTED</i> event is generated.
	<i>EDGE_802_1X_VIA_RADIUS</i>	802.1X protocol is used to authenticate a downstream authentication switch. Once authenticated the port is open for any traffic from that port.
OID	1.3.6.1.4.1.3181.10.6.2.46.16.1.2 (portConfigAuthorizeMode)	
authorize_priority	When two methods provide positive authorization, then this parameter decides which method is used.	
Values	<i>PREFER_802_1X</i> Use 802.X credentials if possible	
	<i>PREFER_MAC</i> Use MAC related credentials if possible	
OID	1.3.6.1.4.1.3181.10.6.2.46.16.1.3 (portConfigAuthorizePriority)	
unauthorized_mode	Defines how unauthorized ports are treated.	
Values	<i>BLOCKED</i>	Port is blocked completely for incoming and outgoing traffic when unauthorized
	<i>USE_UNAUTHORIZED_VLAN</i>	Port is attached to unauthorized VLAN when unauthorized
	<i>INCOMING_BLOCKED</i>	Port is blocked for incoming traffic but outgoing packets like a wake-on-lan packet can still be send out.
OID	1.3.6.1.4.1.3181.10.6.2.46.16.1.4 (portConfigUnauthorizedMode)	

auth_fail_retry_timer	<p>When authentication has failed, the authentication is restarted after the defined time in seconds. This is useful for unattended devices using MAC authentication or when access rights are centrally changed on the RADIUS server and the end unit cannot be reauthenticated manually. The default value of 0 disables the automatic retry.</p> <p>Value Number in range 0-86400</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.16.1.5 (portConfigAuthFailRetryTimer)</p>
mac_timeout	<p>Defines how long authorized MACs remain authorized after inactivity of the MAC.</p> <p>Values <i>NONE</i> MAC on this port remain authorized until a link change occurs</p> <p> <i>SLOW</i> MAC on this port remain authorized for the full duration of mac.global_aging_time when inactive</p> <p> <i>FAST</i> MAC on this port remain authorized for the half duration of mac.global_aging_time when inactive</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.16.1.6 (portConfigMacTimeout)</p>
limited_number_of_macs	<p>The effect of this parameter depends on other settings: If PACC is disabled or PACC is enabled and authorize_mode = ALWAYS_AUTHORIZED is used, then the parameter limits the total number of permitted MACs on the port. If PACC is enabled and an authorize mode via RADIUS is selected, the parameter sets the total number of permitted MACs per VLAN for this port. Set to 0 for normal unlimited operation.</p> <p>Value Number in range 0-255</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.16.1.7 (portConfigLimitedNumberOfMacs)</p>
drop_unknown_unicasts	<p>When set only unicast frames with learned or known MAC address will be send out of this port. ATTENTION: Not implemented.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.16.1.8 (portConfigDropUnknownUnicasts)</p>
drop_egress_broadcasts	<p>When set no broadcast frames with egress this port. ATTENTION: Not implemented.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.16.1.9 (portConfigDropEgressBroadcasts)</p>
learn_mac_now	<p>Learn the next incoming MAC(s) of this port and enter them into the mac_table. Syntax: learn_mac_now = 3 will learn the next 3 MAC addresses. Use pacc.port_status.number_of_learned_macs to verify progress. Type learn_mac_now = 0 to cancel further learning.</p> <p>Action Execute command with parameter string max. 20 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.16.1.10 (portConfigLearnMacNow)</p>

reauthenticate	<p>This action forces re-authentication of the port using the configured method. No parameter required.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.16.1.11 (portConfigReauthenticate)</p>
unauthorize_mac	<p>This action will unauthorize a specific MAC. When no MAC is specified, the entire port is unauthorized.</p> <p>Action Execute command with parameter string max. 20 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.16.1.12 (portConfigUnauthorizeMac)</p>

Group	authorized_macs , dynamical size
Path	Protocol.PACC.authorized_macs
Description	This table defines statically permitted MACs that do not require the device to perform any further authorization process.
name	<p>Unique name to reference this entry and to remember whose MAC address is entered.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.17.1.2 (authorizedMacsName)</p>
mac_address	<p>MAC address of authorized user for port.</p> <p>Format MAC Address <i>hh-hh-hh-hh-hh-hh</i> (<i>hh</i> = hexadecimal number between 00 to ff)</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.17.1.3 (authorizedMacsMacAddress)</p>
permitted_ports	<p>Mask which defines at which port(s) this MAC is permitted. A value of 0 disables this entry. Syntax: slot/port, slot/port or use hex value for quick setup. Example: = 0xf (ports 1-4)</p> <p>Value PORTMASK0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.17.1.4 (authorizedMacsPermittedPorts)</p>
treat_as_vendor_mac	<p>When set, the MAC is treated as vendor MAC. All MACs from this vendor are permitted then.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.17.1.5 (authorizedMacsTreatAsVendorMac)</p>

Group Path Description	supplicant Protocol.PACC.supplicant The 802.1x supplicant permits automatic login when a port is activated.
enable_supplicant	<p>Generally enables the 802.1x supplicant function.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.18.1.2 (supplicantEnableSupplicant)</p>
port	<p>Port through which the authorizing authority is reached. Usually this is the link port.</p> <p>Value PORT0-255</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.18.1.3 (supplicantPort)</p>
action_on_link_down	<p>When the supplicant link goes down, the local authenticated user ports can be deauthenticated as well.</p> <p>Values <i>NONE</i> The user ports are not directly affected by the link down of the trunk. <i>DEAUTHENTICATE</i> The user ports are deauthenticated (dropped) on link down of the trunk. They can reauthenticate when the trunk link resumes and the supplicant itself is authenticated again.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.18.1.4 (supplicantActionOnLinkDown)</p>
identity	<p>Inner identity for tunneled EAP methods (e.g. EAP-TTLS)</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.18.1.5 (supplicantIdentity)</p>
anonymous_identity	<p>Identity string for EAP-MD5. Also used as the unencrypted anonymous outer identity with EAP types that support different tunneled identity, e.g. EAP-TTLS.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.18.1.6 (supplicantAnonymousIdentity)</p>
authentication_protocol	<p>Space-separated list of accepted EAP methods. If not set, all listed methods are allowed. MD5 = insecure and does not generate keying material to be used as a Phase 2 method with PEAP or TTLS. PEAP = with tunneled EAP authentication. TTLS = with tunneled EAP or PAP/CHAP/MSCHAP/MSCHAPV2 authentication. TLS = client and server certificate.</p> <p>Value String, max. 16 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.18.1.7 (supplicantAuthenticationProtocol)</p>

enter_password	<p>Set a new authentication password which replaces the previous one. Note: trailing spaces or multiple spaces in the password are automatically removed.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.18.1.8 (supplicantEnterPassword)</p>
encrypted_auth_password	<p>The encrypted EAP password. Can be set with enter_password action.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.18.1.9 (supplicantEncryptedAuthPassword)</p>
enter_private_key_password	<p>Set a new private key password which replaces the previous one. Note: trailing spaces or multiple spaces in the password are automatically removed.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.18.1.10 (supplicantEnterPrivateKeyPassword)</p>
encrypted_key_password	<p>The encrypted private key password. Can be set with enter_client_cert_password action.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.18.1.11 (supplicantEncryptedKeyPassword)</p>
reauthenticate	<p>Restarts the authentication process for testing and display the results.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.18.1.12 (supplicantReauthenticate)</p>

29.4 PACC Status Parameters

Group	port_status , for each port[0..24]	
Path	Protocol.PACC.port_status[port]	
Description	This table indicates the current port authentication state and contains the data for the last user or MAC that tried to authorize on a given port. To see all users in a multiuser environment refer to user_status table.	
authorization_state	Indicates the port access control state.	
	Values	
	<i>UNDEFINED</i>	Startup condition
	<i>DISABLED</i>	PACC function is disabled
	<i>UNAUTHORIZED</i>	No authorization requests since last port link up or link is currently down
	<i>PROCESSING</i>	Authorization protocol in process
	<i>AUTHORIZED</i>	Port authorized successfully
	<i>REJECTED</i>	Last authorization request was rejected
	OID	1.3.6.1.4.1.3181.10.6.2.46.100.1.2 (portStatusAuthorizationState)
authorization_mode	Last authorization method applied on this port.	
	Values	
	<i>NONE</i>	Default value. No authentication requested yet
	<i>VIA_MAC_TABLE</i>	Authenticated via match to local mac_table
	<i>MAC_VIA_RADIUS</i>	Authenticated via a RADIUS server
	<i>802_1X_VIA_RADIUS</i>	Authenticated via using 802.1X protocol. The login was authenticated by a RADIUS server.
	<i>VIA_MAC_EVENT_ONLY</i>	Port is authorized due to setting MAC_EVENT_ONLY
	<i>EDGE_802_1X_VIA_RADIUS</i>	802.1X protocol was used for authentication. The authenticated the port is now open for any traffic from the connected port.
	OID	1.3.6.1.4.1.3181.10.6.2.46.100.1.3 (portStatusAuthorizationMode)
last_state_change	Indicates the last time the authorization state of this port was modified.	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.46.100.1.4 (portStatusLastStateChange)

number_of_macs_to_learn	Indicates how many MAC addresses will be learned. This is a result of the learn_macs_now action command.
Value	Number in range 0-255
OID	1.3.6.1.4.1.3181.10.6.2.46.100.1.5 (portStatusNumberOfMacsToLearn)
number_of_learned_macs	This value indicates how many MAC addresses have actually been learned since the learn_macs_now command had been issued.
Value	Number in range 0-255
OID	1.3.6.1.4.1.3181.10.6.2.46.100.1.6 (portStatusNumberOfLearnedMacs)
Group	port_mac_status , for each port[0..24]
Path	Protocol.PACC.port_mac_status[port]
Description	This table indicates the current port authentication state and contains the data for the last user or MAC that tried to authorize on a given port. To see all users in a multiuser environment refer to user_status table.
authorization_state	Indicates the port access control state.
Values	<i>UNDEFINED</i> Startup condition <i>DISABLED</i> PACC function is disabled <i>UNAUTHORIZED</i> No authorization requests since last port link up or link is currently down <i>PROCESSING</i> Authorization protocol in process <i>AUTHORIZED</i> Port authorized successfully <i>REJECTED</i> Last authorization request was rejected
OID	1.3.6.1.4.1.3181.10.6.2.46.101.1.2 (portMacStatusAuthorizationState)
user_mac	Last MAC that attempted authorization.
Format	MAC Address hh-hh-hh-hh-hh-hh (hh = hexadecimal number between 00 to ff)
OID	1.3.6.1.4.1.3181.10.6.2.46.101.1.3 (portMacStatusUserMac)
user_name	Last user that attempted authorization unless MAC authentication was used in which case this field is blank.
Value	String, max. 128 characters.
OID	1.3.6.1.4.1.3181.10.6.2.46.101.1.4 (portMacStatusUserName)

vlan_alias	Last dynamically through radius assigned VLAN alias.	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.46.101.1.5 (portMacStatusVlanAlias)
vlan_id	Last dynamically through radius assigned VLAN.	
	Value	Number in range 0-65535
	OID	1.3.6.1.4.1.3181.10.6.2.46.101.1.6 (portMacStatusVlanId)
idle_timeout	This value reflects the idle timeout setting as received via RADIUS. It sets the maximum number of seconds before an idle session is terminated.	
	Value	Number in range 0-65535
	OID	1.3.6.1.4.1.3181.10.6.2.46.101.1.7 (portMacStatusIdleTimeout)
session_timeout	This value reflects the session timeout setting as received via RADIUS. It sets the maximum number of seconds of service to be provided to the user before the session is terminated.	
	Value	Number in range 0-65535
	OID	1.3.6.1.4.1.3181.10.6.2.46.101.1.8 (portMacStatusSessionTimeout)
filter_id	If the RADIUS attribute filter-id is used its value is reflected here.	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.46.101.1.9 (portMacStatusFilterId)
last_state_change	Indicates the last time the authorization state of this port was modified.	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.46.101.1.10 (portMacStatusLastStateChange)
Group	port_802_1x_status , for each port[0..24]	
Path	Protocol.PACC.port_802_1x_status[port]	
Description	This table indicates the current port authentication state and contains the data for the last user or MAC that tried to authorize on a given port. To see all users in a multiuser environment refer to user_status table.	

authorization_state	Indicates the port access control state.		
	Values	UNDEFINED	Startup condition
		DISABLED	PACC function is disabled
		UNAUTHORIZED	No authorization requests since last port link up or link is currently down
		PROCESSING	Authorization protocol in process
		AUTHORIZED	Port authorized successfully
		REJECTED	Last authorization request was rejected
OID	1.3.6.1.4.1.3181.10.6.2.46.102.1.2 (port8021xStatusAuthorizationState)		
<hr/>			
user_mac	Last MAC that attempted authorization.		
	Format	MAC Address hh-hh-hh-hh-hh-hh (hh = hexadecimal number between 00 to ff)	
	OID	1.3.6.1.4.1.3181.10.6.2.46.102.1.3 (port8021xStatusUserMac)	
<hr/>			
user_name	Last user that attempted authorization unless MAC authentication was used in which case this field is blank.		
	Value	String, max. 128 characters.	
	OID	1.3.6.1.4.1.3181.10.6.2.46.102.1.4 (port8021xStatusUserName)	
<hr/>			
vlan_alias	Last dynamically through radius assigned VLAN alias.		
	Value	String, max. 32 characters.	
	OID	1.3.6.1.4.1.3181.10.6.2.46.102.1.5 (port8021xStatusVlanAlias)	
<hr/>			
vlan_id	Last dynamically through radius assigned VLAN.		
	Value	Number in range 0-65535	
	OID	1.3.6.1.4.1.3181.10.6.2.46.102.1.6 (port8021xStatusVlanId)	
<hr/>			
idle_timeout	This value reflects the idle timeout setting as received via RADIUS. It sets the maximum number of seconds before an idle session is terminated.		
	Value	Number in range 0-65535	
	OID	1.3.6.1.4.1.3181.10.6.2.46.102.1.7 (port8021xStatusIdleTimeout)	
<hr/>			
session_timeout	This value reflects the session timeout setting as received via RADIUS. It sets the maximum number of seconds of service to be provided to the user before the session is terminated.		
	Value	Number in range 0-65535	
	OID	1.3.6.1.4.1.3181.10.6.2.46.102.1.8 (port8021xStatusSessionTimeout)	
<hr/>			
filter_id	If the RADIUS attribute filter-id is used its value is reflected here.		
	Value	String, max. 32 characters.	
	OID	1.3.6.1.4.1.3181.10.6.2.46.102.1.9 (port8021xStatusFilterId)	

last_state_change	Indicates the last time the authorization state of this port was modified.
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.2.46.102.1.10 (port8021xStatusLastStateChange)

Group	user_status , for all PACC user status indices [1..250]
Path	Protocol.PACC.user_status[index]
Description	This table lists all users authorized or rejected via some form of port access control. Use filter actions for easier viewing.

entry_state	Indicates if this record displays a currently active login or a history entry of a previous authentication which is invalidated by now.
Values	<i>UNUSED</i> Entry is not yet used <i>INACTIVE</i> Entry displays history of a previous active entry <i>ACTIVE</i> Entry indicates a currently active entry
OID	1.3.6.1.4.1.3181.10.6.2.46.103.1.2 (userStatusEntryState)

authorization_state	Indicates the port access control state resulting from this authorization attempt .
Values	<i>UNDEFINED</i> Startup condition <i>DISABLED</i> PACC function is disabled <i>UNAUTHORIZED</i> No authorization requests since last port link up or link is currently down <i>PROCESSING</i> Authorization protocol in process <i>AUTHORIZED</i> Port authorized successfully <i>REJECTED</i> Last authorization request was rejected
OID	1.3.6.1.4.1.3181.10.6.2.46.103.1.3 (userStatusAuthorizationState)

authorization_mode	Authorization method used for this authorization attempt.		
	Values	NONE	Default value. No authentication requested yet
		VIA_MAC_TABLE	Authenticated via match to local mac_table
		MAC_VIA_RADIUS	Authenticated via a RADIUS server
		802_1X_VIA_RADIUS	Authenticated via using 802.1X protocol. The login was authenticated by a RADIUS server.
		VIA_MAC_EVENT_ONLY	Port is authorized due to setting MAC_EVENT_ONLY
		EDGE_802_1X_VIA_RADIUS	802.1X protocol was used for authentication. The authenticated the port is now open for any traffic from the connected port.
	OID	1.3.6.1.4.1.3181.10.6.2.46.103.1.4 (userStatusAuthorizationMode)	
port	Indicates the port at which this MAC is connected.		
	Value	PORT0-255	
	OID	1.3.6.1.4.1.3181.10.6.2.46.103.1.5 (userStatusPort)	
user_mac	MAC used for this authorization attempt.		
	Format	MAC Address hh-hh-hh-hh-hh-hh (hh = hexadecimal number between 00 to ff)	
	OID	1.3.6.1.4.1.3181.10.6.2.46.103.1.6 (userStatusUserMac)	
user_name	User that attempted authorization unless MAC authentication was used in which case this field is blank.		
	Value	String, max. 128 characters.	
	OID	1.3.6.1.4.1.3181.10.6.2.46.103.1.7 (userStatusUserName)	
vlan_alias	Dynamically through radius assigned VLAN alias.		
	Value	String, max. 32 characters.	
	OID	1.3.6.1.4.1.3181.10.6.2.46.103.1.8 (userStatusVlanAlias)	
vlan_id	Dynamically through radius assigned VLAN.		
	Value	Number in range 0-65535	
	OID	1.3.6.1.4.1.3181.10.6.2.46.103.1.9 (userStatusVlanId)	
idle_timeout	This value reflects the idle timeout setting as received via RADIUS. It sets the maximum number of seconds before an idle session is terminated.		
	Value	Number in range 0-65535	
	OID	1.3.6.1.4.1.3181.10.6.2.46.103.1.10 (userStatusIdleTimeout)	

session_timeout	<p>This value reflects the session timeout setting as received via RADIUS. It sets the maximum number of seconds of service to be provided to the user before the session is terminated.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.103.1.11 (userStatusSessionTimeout)</p>
filter_id	<p>If the RADIUS attribute filter-id is used its value is reflected here.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.103.1.12 (userStatusFilterId)</p>
login_time_stamp	<p>Indicates the time when this record was created.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.103.1.13 (userStatusLoginTimeStamp)</p>
login_epoch	<p>Indicates the time when this record was created. in Linux time since the epoch format.</p> <p>Value Number in range 0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.46.103.1.14 (userStatusLoginEpoch)</p>

30 Multicast Traffic Filtering (IGMP Snooping)

30.1 Key Features

IGMP Snooping

Snooping of Internet Group Management Protocol (IGMPv1/v2/v3) for IPv4. Automatic detection and forwarding of IPv4 multicast-streams. Unregistered packets can be flooded or blocked. Multicast routers can be detected by discovery or by query message.

IGMP snooping constrains IPv4 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv4 multicast traffic only to those ports that want to receive it.

IGMP Snooping per VLAN

Automatic detection and forwarding of IPv4 multicast-streams independent for each configured VLAN.

MLD Snooping

Snooping of Multicast Listener Discovery (MLDv1/v2) for IPv6. Automatic detection and forwarding of IPv6 multicast-streams. Multicast routers can be detected by discovery or by query message.

MLD snooping constrains IPv6 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv6 multicast traffic only to those ports that want to receive it.

30.2 Functional Description

IGMP Snooping

To reduce multicast network traffic, the switch can listen to IGMP communications between Multicast sender and receiver ('Snooping') and adjust its internal forwarding database accordingly. By this means, multicast traffic is only forwarded to those ports where receivers are connected that have joined the corresponding multicast group.

30.3 IGMP CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Protocol.						
	igmp.					IGMP snooping constrains IPv4 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv4 multicast traffic only to those ports that want to receive it. MLD does the same for IPv6 traffic.
			enable_igmp_snooping		R/W	General enable of the IGMP snooping function. When disabled all IGMP snooping in all VLANs is disabled as well.
			enable_mld_snooping		R/W	General enable of the MLD snooping function. When disabled all MLD snooping in all VLANs is disabled as well.
			show_multicast_for_vlan		X	Filter MAC table to show only multicast MACs associated with a given VLAN range. Supply VLAN ID as parameter. Syntax example: <code>igmp.show_multicast_for_vlan = 1-4,1000-2000</code> .
			show_multicast_for_port		X	Filter MAC table to show only multicast MACs associated with a given port range. Supply port as parameter. The shorthand port format like 1 for 1/1 may be used. Syntax examples: <code>igmp.show_multicast_for_port = 1/2,1/5</code> or <code>igmp.show_multicast_for_port = 1-3,5</code> .

config[DYNAMIC].		This table defines IGMP snooping parameter per VLAN. The table entries are referenced by VLAN ID and must match corresponding VLAN filter entries defined under <code>vlan.filter_config.vlan_id</code> . Any number of table entries can be created to configure unique settings for different VLANs. The default entry for VLAN ID=0 cannot be deleted and it used when no VLAN are used in the system.
vlan_id	R/W	Defines IGMP snooping table entry associated with this VLAN ID. This is the key value for the table. VLAN ID 0 is used to define the IGMP settings when VLANs are not used. Type '=' to edit, use index '['*] = new_vlan:' to add an entry. Edit string to nothing to delete entry.
enable_igmp_snooping	R/W	Enable IGMP (IPv4) snooping for this particular VLAN.
enable_mld_snooping	R/W	Enable MLD (IPv6) snooping for this particular VLAN.
snooping_ports	R/W	This parameter permits port selective IGMP/MLD snooping enabling. When empty all ports are enabled! Syntax: slot/port, slot/port or use hex value for quick setup. Example: = 0xf (ports 1-4)
static_router_ports	R/W	When set corresponding ports will be marked as static router ports. Upon default no ports will be marked. Syntax: slot/port, slot/port or use hex value for quick setup. Example: = 0x30 (ports 5-6)
multicast_router_detection	R/W	Defines the mode for detecting the router port.
enable_report_aggregation	R/W	When enabled limits the number of reports received from same subnet to be transmitted only once to the router.
enable_flooding_unregister_pkt	R/W	When enabled unregistered multicast streams are flooded on all ports (which are member of the source VLAN of this stream). When disabled unregistered multicast streams are forwarded on static router ports only.
mcast_group_limit	R/W	Indicates the number of multicast groups in the table.

group_membership_interval	R/W	IGMP group_membership_interval time in seconds.
max_response_time	R/W	IGMP response time in seconds.
enable_fast_leave	R/W	Enables the software to remove the multicast group when it receives an IGMP leave report without first sending an IGMP query message to check if other users still require this group. This parameter is used for IGMPv2 hosts when only one host is present on each VLAN port.
last_member_query_time	R/W	Sets the interval in seconds that the software waits after sending an IGMP query to verify that no hosts that want to receive a particular multicast group to remain on a network segment. If no hosts respond before the last_member_query_time expires, the multicast group is removed from the associated VLAN port.
neighbor_dead_interval	R/W	IGMP neighbor dead interval in seconds in case of router_discovery mode.
router_aging_time	R/W	IGMP router aging time in seconds.
static_multicast_groups[DYNAMIC].		This table may be used to enter the multicast addresses of other protocols beside IGMP, that need to be forwarded when IGMP snooping is enabled. This can be used instead of flood_unregistered_packets parameter and reduces the traffic in the network.
name	R/W	Unique name to reference this entry and to remember whose MAC address is entered.
description	R/W	Enter any information required to remember what this rule is intended to do.
multicast_mac	R/W	MAC address entry.
forwarding_port_mask	R/W	Enter the ports to which this multicast should be forwarded. A value of 0 disables this entry. Syntax: slot/port, slot/port or use hex value for quick setup. Example: = 0xf (ports 1-4)
vlan_id	R/W	VLAN on which the packets is entering.
status.		This table contains operational counters of the IGMP snooping module.

igmp_router_ports	R	Displays the gimp router ports list
rx_general_queries	R	Displays the number of received general queries.
rx_group_queries	R	Displays the number of received group queries.
rx_reports	R	Displays the number of received report messages.
rx_leaves	R	Displays the number of received leave messages.
rx_advertisements	R	Displays the number of received advertisements.
rx_terminations	R	Displays the number of received terminations.
rx_unsupported	R	Displays the number of received unsupported messages.
rx_errors	R	Displays the number of received error packets.
tx_solicitations	R	Displays the number of transmitted solicitation messages.
mld_status.		This table contains operational counters of the MLD snooping module.
mld_router_ports	R	Displays the gimp router ports list
rx_general_queries	R	Displays the number of received general queries.
rx_group_queries	R	Displays the number of received group queries.
rx_reports	R	Displays the number of received report messages.
rx_leaves	R	Displays the number of received leave messages.
rx_advertisements	R	Displays the number of received advertisements.
rx_terminations	R	Displays the number of received terminations.
rx_unsupported	R	Displays the number of received unsupported messages.
rx_errors	R	Displays the number of received error packets.
tx_solicitations	R	Displays the number of transmitted solicitation messages.

30.4 IGMP Configuration Parameters

Group Path	General Parameters
	Protocol.IGMP
enable_igmp_snooping	<p>General enable of the IGMP snooping function. When disabled all IGMP snooping in all VLANs is disabled as well.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.1 (igmpEnableIgmpSnooping) 1.3.6.1.2.1.85.1.1.1.1 (igmpInterfaceIfIndex)</p>
enable_mld_snooping	<p>General enable of the MLD snooping function. When disabled all MLD snooping in all VLANs is disabled as well.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.2 (igmpEnableMldSnooping) 1.3.6.1.2.1.85.1.1.1.1 (igmpInterfaceIfIndex)</p>
show_multicast_for_vlan	<p>Filter MAC table to show only multicast MACs associated with a given VLAN range. Supply VLAN ID as parameter. Syntax example: igmp.show_multicast_for_vlan = 1-4,1000-2000.</p> <p>Action Execute command with parameter string max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.3 (igmpShowMulticastForVlan)</p>
show_multicast_for_port	<p>Filter MAC table to show only multicast MACs associated with a given port range. Supply port as parameter. The shorthand port format like 1 for 1/1 may be used. Syntax examples: igmp.show_multicast_for_port = 1/2,1/5 or igmp.show_multicast_for_port = 1-3,5.</p> <p>Action Execute command with parameter string max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.4 (igmpShowMulticastForPort)</p>
Group Path	config , dynamical size
Description	<p>Protocol.IGMP.config</p> <p>This table defines IGMP snooping parameter per VLAN. The table entries are referenced by VLAN ID and must match corresponding VLAN filter entries defined under vlan.filter_config.vlan_id. Any number of table entries can be created to configure unique settings for different VLANs. The default entry for VLAN ID=0 cannot be deleted and it used when no VLAN are used in the system.</p>

vlan_id	<p>Defines IGMP snooping table entry associated with this VLAN ID. This is the key value for the table. VLAN ID 0 is used to define the IGMP settings when VLANs are not used. Type '=' to edit, use index '['*] = new_vlan:' to add an entry. Edit string to nothing to delete entry.</p> <p>Value String, max. 4 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.5.1.2 (configVlanId)</p>
enable_igmp_snooping	<p>Enable IGMP (IPv4) snooping for this particular VLAN.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.5.1.3 (configEnableIgmpSnooping)</p>
enable_mld_snooping	<p>Enable MLD (IPv6) snooping for this particular VLAN.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.5.1.4 (configEnableMldSnooping)</p>
snooping_ports	<p>This parameter permits port selective IGMP/MLD snooping enabling. When empty all ports are enabled! Syntax: slot/port, slot/port or use hex value for quick setup. Example: = 0xf (ports 1-4)</p> <p>Value PORTMASK0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.5.1.5 (configSnoopingPorts)</p>
static_router_ports	<p>When set corresponding ports will be marked as static router ports. Upon default no ports will be marked. Syntax: slot/port, slot/port or use hex value for quick setup. Example: = 0x30 (ports 5-6)</p> <p>Value PORTMASK0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.5.1.6 (configStaticRouterPorts)</p>
multicast_router_detection	<p>Defines the mode for detecting the router port.</p> <p>Values <i>ROUTER_DISCOVERY</i> Mark router port only on receiving advertisements <i>QUERY_MESSAGE</i> Mark router port only on receiving query message</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.5.1.7 (configMulticastRouterDetection)</p>
enable_report_aggregation	<p>When enabled limits the number of reports received from same subnet to be transmitted only once to the router.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.5.1.8 (configEnableReportAggregation)</p>

enable_flooding_unregister_pkt	<p>When enabled unregistered multicast streams are flooded on all ports (which are member of the source VLAN of this stream). When disabled unregistered multicast streams are forwarded on static router ports only.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.5.1.9 (configEnableFloodingUnregisterPkt)</p>
mcast_group_limit	<p>Indicates the number of multicast groups in the table.</p> <p>Value Number in range 10-256</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.5.1.10 (configMcastGroupLimit)</p>
group_membership_interval	<p>IGMP group_membership_interval time in seconds.</p> <p>Value Number in range 200-1000</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.5.1.11 (configGroupMembershipInterval)</p>
max_response_time	<p>IGMP response time in seconds.</p> <p>Value Number in range 1-25</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.5.1.12 (configMaxResponseTime) 1.3.6.1.2.1.85.1.1.1.6 (igmpInterfaceQueryMaxResponseTime)</p>
enable_fast_leave	<p>Enables the software to remove the multicast group when it receives an IGMP leave report without first sending an IGMP query message to check if other users still require this group. This parameter is used for IGMPv2 hosts when only one host is present on each VLAN port.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.5.1.13 (configEnableFastLeave)</p>
last_member_query_time	<p>Sets the interval in seconds that the software waits after sending an IGMP query to verify that no hosts that want to receive a particular multicast group to remain on a network segment. If no hosts respond before the last_member_query_time expires, the multicast group is removed from the associated VLAN port.</p> <p>Value Number in range 1-175</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.5.1.14 (configLastMemberQueryTime) 1.3.6.1.2.1.85.1.1.1.15 (igmpInterfaceLastMembQueryIntvl)</p>

neighbor_dead_interval	<p>IGMP neighbor dead interval in seconds in case of router_discovery mode.</p> <p>Value Number in range 2-1000</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.5.1.15 (configNeighborDeadInterval) 1.3.6.1.2.1.85.1.1.1.8 (igmpInterfaceQuerierExpiryTime)</p>
router_aging_time	<p>IGMP router aging time in seconds.</p> <p>Value Number in range 2-1000</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.5.1.16 (configRouterAgingTime) 1.3.6.1.2.1.85.1.1.1.7 (igmpInterfaceQuerierUpTime)</p>
Group Path Description	<p>static_multicast_groups, dynamical size</p> <p>Protocol.IGMP.static_multicast_groups</p> <p>This table may be used to enter the multicast addresses of other protocols beside IGMP, that need to be forwarded when IGMP snooping is enabled. This can be used instead of flood_unregistered_packets parameter and reduces the traffic in the network.</p>
name	<p>Unique name to reference this entry and to remember whose MAC address is entered.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.6.1.2 (staticMulticastGroupsName)</p>
description	<p>Enter any information required to remember what this rule is intended to do.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.6.1.3 (staticMulticastGroupsDescription)</p>
multicast_mac	<p>MAC address entry.</p> <p>Format MAC Address <i>hh-hh-hh-hh-hh-hh</i> (<i>hh</i> = hexadecimal number between 00 to ff)</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.6.1.4 (staticMulticastGroupsMulticastMac)</p>
forwarding_port_mask	<p>Enter the ports to which this multicast should be forwarded. A value of 0 disables this entry. Syntax: slot/port, slot/port or use hex value for quick setup. Example: = 0xf (ports 1-4)</p> <p>Value PORTMASK0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.40.6.1.5 (staticMulticastGroupsForwardingPortMask)</p>

vlan_id	VLAN on which the packets is entering.	
	Value	Number in range 0-4095
	OID	1.3.6.1.4.1.3181.10.6.2.40.6.1.6 (staticMulticastGroupsVlanId)

30.5 IGMP Status Parameters

Group Path Description	status
	Protocol.IGMP.status This table contains operational counters of the IGMP snooping module.
igmp_router_ports	Displays the gimp router ports list Value PORTMASK0-0xFFFFFFFF OID 1.3.6.1.4.1.3181.10.6.2.40.100.1.2 (statusIgmpRouterPorts)
rx_general_queries	Displays the number of received general queries. Value Number in range 0-0xFFFFFFFF OID 1.3.6.1.4.1.3181.10.6.2.40.100.1.3 (statusRxGeneralQueries)
rx_group_queries	Displays the number of received group queries. Value Number in range 0-0xFFFFFFFF OID 1.3.6.1.4.1.3181.10.6.2.40.100.1.4 (statusRxGroupQueries)
rx_reports	Displays the number of received report messages. Value Number in range 0-0xFFFFFFFF OID 1.3.6.1.4.1.3181.10.6.2.40.100.1.5 (statusRxReports)
rx_leaves	Displays the number of received leave messages. Value Number in range 0-0xFFFFFFFF OID 1.3.6.1.4.1.3181.10.6.2.40.100.1.6 (statusRxLeaves)
rx_advertisements	Displays the number of received advertisements. Value Number in range 0-0xFFFFFFFF OID 1.3.6.1.4.1.3181.10.6.2.40.100.1.7 (statusRxAdvertisements)
rx_terminations	Displays the number of received terminations. Value Number in range 0-0xFFFFFFFF OID 1.3.6.1.4.1.3181.10.6.2.40.100.1.8 (statusRxTerminations)
rx_unsupported	Displays the number of received unsupported messages. Value Number in range 0-0xFFFFFFFF OID 1.3.6.1.4.1.3181.10.6.2.40.100.1.9 (statusRxUnsupported)

rx_errors	Displays the number of received error packets.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.2.40.100.1.10 (statusRxErrors)
tx_solicitations	Displays the number of transmitted solicitation messages.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.2.40.100.1.11 (statusTxSolicitations)
Group	mld_status	
Path	Protocol.IGMP.mld_status	
Description	This table contains operational counters of the MLD snooping module.	
mld_router_ports	Displays the gimp router ports list	
	Value	PORTMASK0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.2.40.101.1.2 (mldStatusMldRouterPorts)
rx_general_queries	Displays the number of received general queries.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.2.40.101.1.3 (mldStatusRxGeneralQueries)
rx_group_queries	Displays the number of received group queries.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.2.40.101.1.4 (mldStatusRxGroupQueries)
rx_reports	Displays the number of received report messages.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.2.40.101.1.5 (mldStatusRxReports)
rx_leaves	Displays the number of received leave messages.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.2.40.101.1.6 (mldStatusRxLeaves)
rx_advertisements	Displays the number of received advertisements.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.2.40.101.1.7 (mldStatusRxAdvertisements)

rx_terminations	Displays the number of received terminations.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.2.40.101.1.8 (mldStatusRxTerminations)

rx_unsupported	Displays the number of received unsupported messages.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.2.40.101.1.9 (mldStatusRxUnsupported)

rx_errors	Displays the number of received error packets.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.2.40.101.1.10 (mldStatusRxErrors)

tx_solicitations	Displays the number of transmitted solicitation messages.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.2.40.101.1.11 (mldStatusTxSolicitations)

31 Dynamic Host Configuration Protocol (DHCP)

31.1 Key Features

DHCP Snooping

DHCP snooping records IP addresses, VLAN information, etc. to record trusted interfaces. DHCP snooping suppresses DHCP traffic from untrusted interfaces.

Secures network against man-in-the-middle attacks.

IP-MAC Binding Table

A table lists the MAC-IP bindings of the untrusted ports (only) as discovered through DHCP snooping.

DHCP Filtering

DHCP Filtering prevents DHCP being injected from a user port. This feature acts on IPv4 and IPv6 alike.

Secures IP network against malicious users.

DHCP Flooding Detection

Attempts to detect a DHCP attack and shuts down the access port when too many DHCP messages ingress on the port.

Secures IP network against malicious users.

DHCP relay agent with option 82

When enabled, the switch will append a unique port/switch identification to a DHCP request from an access port. This enables the use of a distant DHCP server and to better control which IP address to serve. This feature supports IPv4 and IPv6. Port and unit information are configurable.

Supports accurate IP addressing policies: When equipment is exchanged it is ensured the IP address remains unchanged.

DHCP Options 66/67

Unit configuration or software updates controlled via DHCP option 66/67 mechanism. A CLI script can be downloaded which in turn may request further download or configuration changes

In large networks updates can be automated to take place as soon as a unit goes online. The script is a very powerful tool.

Dynamic ARP Inspection

Incoming ARPs are being verified against IP/MAC relation database provided by DHCP snooping. In addition an access list (ACL) is used for verification. In addition too many ARPs can lead to the port being blocked to prevent ARP attacks.

Dynamic ARP Inspection helps make sure of user integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.

PPPoE Snooping

PPP over Ethernet is used by carriers to identify the customer port. When a user signs-in, The Switch will automatically insert a configurable information that will allow the network to identify the originating port and device.

Permits carriers to use the Switch as Internet access gateway.

PPPoE variable Remote and Circuit Ids

PPP over Ethernet is used by carriers to identify the customer port. The fields for remote-id and circuit-id can be configured in various ways to match network requirements.

Permits carriers to use the better adapt the switch to the desired addressing needs.

RADIUS controlled dynamic IP-Address provisioning with DHCP

This function applies the IP configuration by DHCP to a successful authorized host. The IP parameters are received from the RADIUS server when granting network access to the host.

Permits centralized network provisioning via RADIUS. The attributes Framed-IP-Address(8) and Framed-IP-Netmask(9) are used.

31.2 Functional Description

Dynamic Host Configuration Protocol (DHCP) is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

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.

31.3 DHCP CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Protocol.	dhcp.					DHCP Relay Agent, DHCP snooping and related ARP inspection
			enable_dhcp_relay		R/W	General enable of DHCP relay function.
			enable_dhcp_snooping		R/W	General enable of DHCP snooping function.
			enable_pppoe_snooping		R/W	General enable of PPPoE snooping also known as PPPoE Intermediate Agent function.
			enable_arp_inspection		R/W	General enable of ARP inspection function.
			unblock_port		X	This function may be used to unblock a port that has been set to blocking state due to DHCP flooding or due to ARP storm detection. The shorthand port format like 1 for 1/1 may be used. Syntax examples: dhcp.unblock_port = 1/2,1/5 or dhcp.unblock_port = 1/1-1/4. Also the syntax .. = 0-5 to unblock the first 6 ports is supported.
			clear_snooping_table		X	This function may be used to clear the content of the DHCP snooping table.
	relay_config.					This configures the DHCP relay option 82. It can be used to supply information from which port a DHCP request came in order to supply an IP based on the physical location of the requestor.
			dhcp_server_address		R/W	Defines host address or network address where the DHCP server(s) resides. Also known as ip_helper_address.
			remote_id_source		R/W	Defines how the switch is identified when DHCP option 82 is used. (Suboption2)
			custom_remote_id		R/W	This remote id is used for option 82 when 'remote_id_source' is set to USER_DEFINED.

circuit_id_source	R/W	Defines how the ports are identified when option 82 is used. (Suboption1)
relay_port_config[PORT].		This configures the DHCP relay option 82. It can be used to supply information from which port a DHCP request came in order to supply an IP based on the physical location of the requestor.
enable_dhcp_relay	R/W	When enabled incoming DHCP requests are redirected to the DHCP server or network specified in 'dhcp.relay_config'
enable_option_82	R/W	When enabled incoming DHCP requests are modified in 'dhcp.relay_config'
snooping_port_config[PORT].		This configures the DHCP snooping function. DHCP snooping acts like a DHCP firewall between access and link ports. When enabled it ensures that for untrusted ports only DHCP requests are accepted. This prevents malicious users from injecting fake DHCP frames and thus invalid IP addresses.
enable_dhcp_snooping	R/W	This enables the DHCP snooping function per port.
dhcp_filtering	R/W	DHCP filtering prevents DHCP responses being injected from a local access port. It acts like a DHCP firewall between access and link ports.
snooping_trust	R/W	DHCP responses are only accepted when they ingress on a trusted port. Typically these are the link ports. AUTO uses the port role and declares all up or downlink ports as trusted.
accept_ingress_option82	R/W	Normally incoming DHCP request incoming with Option 82 set will be discarded. When enabled then this check is ignored.
mac_address_verification	R/W	When a packet is received on an untrusted interface, and the source MAC address and the DHCP client MAC address do not match and this feature is enabled, the packet is dropped.
dhcp_rate_limiting	R/W	Defines how many DHCP request are accepted per second. When the limit is reached, DHCP flooding is assumed and the port is blocked. The value 0 disables the rate limit check.
clear_snooping_statistics	X	Reset all DHCP related statistics and reason. The snooping binding table is not affected.

pppoe_config.		This table defines the general parameter for PPPoE Intermediate Agent feature.
vendor_id	R/W	Vendor identification that this device adds to a PPPoE request before forwarding it to the server.
remote_id_source	R/W	The remote id identifies the client that requests a PPPoE connection.
custom_remote_id	R/W	This field is only used in a PPPoE request when the remote_id_source is set to USER_DEFINED.
circuit_id_source	R/W	This field defines how the port on which a PPPoE request comes in is identified.
pppoe_port_config[PORT].		This table permits port specific enable of the PPPoE Intermediate Agent feature.
enable_pppoe_snooping	R/W	Enables PPPoE intermediate agent function also known as PPPoE Snooping for this port. Also observe the general enable parameter for PPPoE.
arp_inspection_port_config[PORT].		This table defines the parameter for Dynamic ARP Inspection per port. These features should generally be used with untrusted ports.
enable_arp_inspection	R/W	Generally enables Dynamic ARP Inspection. The details need to be configured per VLAN in separate table. This feature helps preventing from man-in-the-middle attacks to the network.
arp_rate_limiting	R/W	Defines how many ARP request are accepted per second. When the limit is reached, a DOS attack is assumed and the port is shut down. The value 0 disables the rate limit check.
inspection_database	R/W	When set to another value than NONE, the MAC-IP relationship of the incoming ARPs is verified against the selected table. This ensures that only valid MACs enter the network.
arp_acl_name	R/W	Name of the ACL (access control list) which declares which IP/MAC relations are acceptable. Note: ACLs are configured under Management.ACL. Several ACL may be specified with a comma separated list. Example acl1, otherlist
acl_default_logic	R/W	Defines which action is taken when none of the ACL records matches. Default is deny which blocks the ARP.

source_mac_validation	R/W	Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. Packets with different MAC addresses are dropped.
dest_mac_validation	R/W	Checks the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses. Packets with different MAC addresses are dropped.
ip_range_validation	R/W	Checks ARP for invalid addresses. Invalid addresses include 0.0.0.0, 255.255.255.255, and all IP multicast and loopback addresses. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.
radius_controlled_dhcp.		This feature permits a local DHCP server per port which takes the IP data to serve via a RADIUS session from a common server. The Framed-IP-Address attribute is expected.
enable_radius_dhcp	R/W	Generally enables RADIUS controlled DHCP server feature. Only ports are affected for which PACC is enabled and set to 802.1X or MAC_VIA_RADIUS controlled.
lease_time	R/W	Lease time in seconds.
default_subnet_mask	R/W	This subnet mask is used in the DHCP reply when the RADIUS attribute Framed-IP-Netmask is not received.
gateway	R/W	This gateway IP address is used in the DHCP reply. The value is not received via RADIUS. When the field is left blank no gateway information is send.
dns_server	R/W	This domain name server IP address is used in the DHCP reply. The value is not received via RADIUS. When the field is left blank no gateway information is send.
snooping_statistics[PORT].		Statistics indicating activity of DHCP snooping.
trust_mode	R	Reflects the determined trust mode.
number_of_dhcp_processed	R	Counts the number of DHCP messages processed.
number_of_dhcp_dropped	R	Counts the number of DHCP messages dropped.
last_drop_reason	R	

snooping_table[256].

This table lists the MAC-IP bindings of the untrusted ports (only) as discovered through DHCP snooping.

mac	R	MAC address entry
ip	R	IP address associated with this MAC.
port	R	Port number for MAC address
vlan	R	if non zero this MAC is part of this VLAN.
last_updated	R	Time stamp when this record was written
last_updated_epoch	R	Time stamp in alternate format
lease_time	R	Lease time as reported by DHCP server

31.4 DHCP Configuration Parameters

Group Path	General Parameters Protocol.DHCP
enable_dhcp_relay	<p>General enable of DHCP relay function.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.49.1 (dhcpEnableDhcpRelay)</p>
enable_dhcp_snooping	<p>General enable of DHCP snooping function.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.49.2 (dhcpEnableDhcpSnooping)</p>
enable_pppoe_snooping	<p>General enable of PPPoE snooping also known as PPPoE Intermediate Agent function.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.49.3 (dhcpEnablePppoeSnooping)</p>
enable_arp_inspection	<p>General enable of ARP inspection function.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.49.4 (dhcpEnableArpInspection)</p>
unblock_port	<p>This function may be used to unblock a port that has been set to blocking state due to DHCP flooding or due to ARP storm detection. The shorthand port format like 1 for 1/1 may be used. Syntax examples: dhcp.unblock_port = 1/2,1/5 or dhcp.unblock_port = 1/1-1/4. Also the syntax .. = 0-5 to unblock the first 6 ports is supported.</p> <p>Action Execute command with parameter string max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.49.5 (dhcpUnblockPort)</p>
clear_snooping_table	<p>This function may be used to clear the content of the DHCP snooping table.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.49.6 (dhcpClearSnoopingTable)</p>

Group Path	relay_port_config , for all ports[0..31] Protocol.DHCP.relay_port_config[port]
Description	This configures the DHCP relay option 82. It can be used to supply information from which port a DHCP request came in order to supply an IP based on the physical location of the requestor.

enable_dhcp_relay	When enabled incoming DHCP requests are redirected to the DHCP server or network specified in 'dhcp.relay_config'
Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.2.49.8.1.2 (relayPortConfigEnableDhcpRelay)

enable_option_82	When enabled incoming DHCP requests are modified in 'dhcp.relay_config'
Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.2.49.8.1.3 (relayPortConfigEnableOption82)

Group	snooping_port_config , for all ports[0..31]
Path	Protocol.DHCP.snooping_port_config[port]
Description	This configures the DHCP snooping function. DHCP snooping acts like a DHCP firewall between access and link ports. When enabled it ensures that for untrusted ports only DHCP requests are accepted. This prevents malicious users from injecting fake DHCP frames and thus invalid IP addresses.

enable_dhcp_snooping	This enables the DHCP snooping function per port.
Values	enabled, disabled
OID	1.3.6.1.4.1.3181.10.6.2.49.9.1.2 (snoopingPortConfigEnableDhcpSnooping)

dhcp_filtering	DHCP filtering prevents DHCP responses being injected from a local access port. It acts like a DHCP firewall between access and link ports.						
Values	<table> <tr> <td><i>DISABLED</i></td><td>DHCP frames are not removed</td></tr> <tr> <td><i>DROP_AND_EVENT</i></td><td>DHCP response frames incoming from a user port are removed and a PACKET_INTERCEPTED event is send</td></tr> <tr> <td><i>BLOCK_AND_EVENT</i></td><td>Port is blocked when an DHCP response incoming from a user port is detected. Needs operator intervention to unblock. Also a PACKET_INTERCEPTED event is send.</td></tr> </table>	<i>DISABLED</i>	DHCP frames are not removed	<i>DROP_AND_EVENT</i>	DHCP response frames incoming from a user port are removed and a PACKET_INTERCEPTED event is send	<i>BLOCK_AND_EVENT</i>	Port is blocked when an DHCP response incoming from a user port is detected. Needs operator intervention to unblock. Also a PACKET_INTERCEPTED event is send.
<i>DISABLED</i>	DHCP frames are not removed						
<i>DROP_AND_EVENT</i>	DHCP response frames incoming from a user port are removed and a PACKET_INTERCEPTED event is send						
<i>BLOCK_AND_EVENT</i>	Port is blocked when an DHCP response incoming from a user port is detected. Needs operator intervention to unblock. Also a PACKET_INTERCEPTED event is send.						
OID	1.3.6.1.4.1.3181.10.6.2.49.9.1.3 (snoopingPortConfigDhcpFiltering)						

snooping_trust	<p>DHCP responses are only accepted when they ingress on a trusted port. Typically these are the link ports. AUTO uses the port role and declares all up or downlink ports as trusted.</p> <p>Values</p> <p><i>AUTO</i> Use port role and declares link port as trusted</p> <p><i>UNTRUSTED</i> This port is untrusted and DHCP filtering applies</p> <p><i>TRUSTED</i> This port is trusted and no filtering occurs. Use when a DHCP server should be permitted on a local access port</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.49.9.1.4 (snoopingPortConfigSnoopingTrust)</p>
accept_ingress_option82	<p>Normally incoming DHCP request incoming with Option 82 set will be discarded. When enabled then this check is ignored.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.49.9.1.5 (snoopingPortConfigAcceptIngressOption82)</p>
mac_address_verification	<p>When a packet is received on an untrusted interface, and the source MAC address and the DHCP client MAC address do not match and this feature is enabled, the packet is dropped.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.49.9.1.6 (snoopingPortConfigMacAddressVerification)</p>
dhcp_rate_limiting	<p>Defines how many DHCP request are accepted per second. When the limit is reached, DHCP flooding is assumed and the port is blocked. The value 0 disables the rate limit check.</p> <p>Value Number in range 0-50</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.49.9.1.7 (snoopingPortConfigDhcpRateLimiting)</p>
clear_snooping_statistics	<p>Reset all DHCP related statistics and reason. The snooping binding table is not affected.</p> <p>Action Execute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.49.9.1.8 (snoopingPortConfigClearSnoopingStatistics)</p>

Group	pppoe_port_config , for all ports[0..31]
Path	Protocol.DHCP.pppoe_port_config[port]
Description	This table permits port specific enable of the PPPoE Intermediate Agent feature.

enable_pppoe_snooping	Enables PPPoE intermediate agent function also known as PPPoE Snooping for this port. Also observe the general enable parameter for PPPoE.
------------------------------	--

Values	enabled, disabled
---------------	-------------------

OID	1.3.6.1.4.1.3181.10.6.2.49.11.1.2 (pppoePortConfigEnablePppoeSnooping)
------------	---

Group	arp_inspection_port_config , for all ports[0..31]
Path	Protocol.DHCP.arp_inspection_port_config[port]
Description	This table defines the parameter for Dynamic ARP Inspection per port. These features should generally be used with untrusted ports.

enable_arp_inspection	Generally enables Dynamic ARP Inspection. The details need to be configured per VLAN in separate table. This feature helps preventing from man-in-the-middle attacks to the network.
------------------------------	--

Values	enabled, disabled
---------------	-------------------

OID	1.3.6.1.4.1.3181.10.6.2.49.12.1.2 (arpInspectionPortConfigEnableArpInspection)
------------	---

arp_rate_limiting	Defines how many ARP request are accepted per second. When the limit is reached, a DOS attack is assumed and the port is shut down. The value 0 disables the rate limit check.
--------------------------	--

Value	Number in range 0-50
--------------	----------------------

OID	1.3.6.1.4.1.3181.10.6.2.49.12.1.3 (arpInspectionPortConfigArpRateLimiting)
------------	---

inspection_database	When set to another value than NONE, the MAC-IP relationship of the incoming ARPs is verified against the selected table. This ensures that only valid MACs enter the network.
----------------------------	--

Values	<table border="0"> <tr> <td style="padding-right: 10px;"><i>NONE</i></td> <td>Only general ARP validity is checked</td> </tr> <tr> <td><i>DHCP</i></td> <td>The DHCP snooping table is used to verify MAC-IP relationship</td> </tr> <tr> <td><i>ARP_ACL</i></td> <td>The manually defined ARP access control list table is used to verify MAC-IP relationship</td> </tr> <tr> <td><i>BOTH</i></td> <td>The ARP is only rejected when both tables fail to verify MAC-IP relationship</td> </tr> </table>	<i>NONE</i>	Only general ARP validity is checked	<i>DHCP</i>	The DHCP snooping table is used to verify MAC-IP relationship	<i>ARP_ACL</i>	The manually defined ARP access control list table is used to verify MAC-IP relationship	<i>BOTH</i>	The ARP is only rejected when both tables fail to verify MAC-IP relationship
<i>NONE</i>	Only general ARP validity is checked								
<i>DHCP</i>	The DHCP snooping table is used to verify MAC-IP relationship								
<i>ARP_ACL</i>	The manually defined ARP access control list table is used to verify MAC-IP relationship								
<i>BOTH</i>	The ARP is only rejected when both tables fail to verify MAC-IP relationship								

OID	1.3.6.1.4.1.3181.10.6.2.49.12.1.4 (arpInspectionPortConfigInspectionDatabase)
------------	--

arp_acl_name	Name of the ACL (access control list) which declares which IP/MAC relations are acceptable. Note: ACLs are configured under Management.ACL. Several ACL may be specified with a comma separated list. Example acl1, otherlist
---------------------	---

Value	String, max. 128 characters.
--------------	------------------------------

OID	1.3.6.1.4.1.3181.10.6.2.49.12.1.5 (arpInspectionPortConfigArpAclName)
------------	--

acl_default_logic	<p>Defines which action is taken when none of the ACL records matches. Default is deny which blocks the ARP.</p> <p>Values <i>DENY</i> When no entry matches the ACL then the ARP is denied</p> <p> <i>PERMIT</i> When no entry matches the ACL then the ARP is accepted.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.49.12.1.6 (arpInspectionPortConfigAclDefaultLogic)</p>
source_mac_validation	<p>Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. Packets with different MAC addresses are dropped.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.49.12.1.7 (arpInspectionPortConfigSourceMacValidation)</p>
dest_mac_validation	<p>Checks the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses. Packets with different MAC addresses are dropped.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.49.12.1.8 (arpInspectionPortConfigDestMacValidation)</p>
ip_range_validation	<p>Checks ARP for invalid addresses. Invalid addresses include 0.0.0.0, 255.255.255.255, and all IP multicast and loopback addresses. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.49.12.1.9 (arpInspectionPortConfigIpRangeValidation)</p>
Group Path Description	<p>relay_config</p> <p>Protocol.DHCP.relay_config</p> <p>This configures the DHCP relay option 82. It can be used to supply information from which port a DHCP request came in order to supply an IP based on the physical location of the requestor.</p>
dhcp_server_address	<p>Defines host address or network address where the DHCP server(s) resides. Also known as ip_helper_address.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.49.7.1.2 (relayConfigDhcpServerAddress)</p>

remote_id_source	Defines how the switch is identified when DHCP option 82 is used. (Suboption2)	
	Values	
	HOSTNAME	Hostname of this switch
	MAC_ADDRESS	MAC address of this switch
	SYS_NAME	SNMP sysName of this switch
	USER_DEFINED	A user defined string as defined in 'custom_remote_id' is used
	PORT_ALIAS	The 'port.config.alias' value of the incoming port is used
	OID	1.3.6.1.4.1.3181.10.6.2.49.7.1.3 (relayConfigRemoteIdSource)
custom_remote_id	This remote id is used for option 82 when 'remote_id_source' is set to USER_DEFINED.	
	Value	String, max. 128 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.49.7.1.4 (relayConfigCustomRemoteId)
circuit_id_source	Defines how the ports are identified when option 82 is used. (Suboption1)	
	Values	
	SNMP_PORT_ID	Port id in 101,102 style as used with SNMP
	SLOT_PORT_ID	Port id in slot/port style
	PORT_ALIAS	The 'port.config.alias' value of the incoming port is used
	IP_SLOT_PORT_VLAN	(Agent-IP) eth (Slot/Port):(VLAN-ID) is used
	OID	1.3.6.1.4.1.3181.10.6.2.49.7.1.5 (relayConfigCircuitIdSource)
Group	pppoe_config	
Path	Protocol.DHCP.pppoe_config	
Description	This table defines the general parameter for PPPoE Intermediate Agent feature.	
vendor_id	Vendor identification that this device adds to a PPPoE request before forwarding it to the server.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.2.49.10.1.2 (pppoeConfigVendorId)

remote_id_source	The remote id identifies the client that requests a PPPoE connection.		
	Values	HOSTNAME	Hostname of this switch
		MAC_ADDRESS	MAC address of this switch
		SYS_NAME	SNMP sysName of this switch
		USER_DEFINED	A user defined string as defined in 'custom_remote_id' is used
		PORT_ALIAS	The 'port.config.alias' value of the incoming port is used
	OID	1.3.6.1.4.1.3181.10.6.2.49.10.1.3 (pppoeConfigRemoteIdSource)	
custom_remote_id	This field is only used in a PPPoE request when the remote_id_source is set to USER_DEFINED.		
	Value	String, max. 63 characters.	
	OID	1.3.6.1.4.1.3181.10.6.2.49.10.1.4 (pppoeConfigCustomRemoteId)	
circuit_id_source	This field defines how the port on which a PPPoE request comes in is identified.		
	Values	SNMP_PORT_ID	Port id in 101,102 style as used with SNMP
		SLOT_PORT_ID	Port id in slot/port style
		PORT_ALIAS	The 'port.config.alias' value of the incoming port is used
		IP_SLOT_PORT_VLAN	(Agent-IP) eth (Slot/Port):(VLAN-ID) is used
	OID	1.3.6.1.4.1.3181.10.6.2.49.10.1.5 (pppoeConfigCircuitIdSource)	
Group	radius_controlled_dhcp		
Path	Protocol.DHCP.radius_controlled_dhcp		
Description	This feature permits a local DHCP server per port which takes the IP data to serve via a RADIUS session from a common server. The Framed-IP-Address attribute is expected.		
enable_radius_dhcp	Generally enables RADIUS controlled DHCP server feature. Only ports are affected for which PACC is enabled and set to 802.1X or MAC_VIA_RADIUS controlled.		
	Values	enabled, disabled	
	OID	1.3.6.1.4.1.3181.10.6.2.49.13.1.2 (radiusControlledDhcpEnableRadiusDhcp)	
lease_time	Lease time in seconds.		
	Value	Number in range 0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.2.49.13.1.3 (radiusControlledDhcpLeaseTime)	

default_subnet_mask	<p>This subnet mask is used in the DHCP reply when the RADIUS attribute Framed-IP-Netmask is not received.</p> <p>Format IPv4 Address <i>ddd.ddd.ddd.ddd</i> (<i>ddd</i> = decimal number between 000 to 255)</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.49.13.1.4 (radiusControlledDhcpDefaultSubnetMask)</p>
<hr/>	
gateway	<p>This gateway IP address is used in the DHCP reply. The value is not received via RADIUS. When the field is left blank no gateway information is send.</p> <p>Format IPv4 Address <i>ddd.ddd.ddd.ddd</i> (<i>ddd</i> = decimal number between 000 to 255)</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.49.13.1.5 (radiusControlledDhcpGateway)</p>
<hr/>	
dns_server	<p>This domain name server IP address is used in the DHCP reply. The value is not received via RADIUS. When the field is left blank no gateway information is send.</p> <p>Format IPv4 Address <i>ddd.ddd.ddd.ddd</i> (<i>ddd</i> = decimal number between 000 to 255)</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.49.13.1.6 (radiusControlledDhcpDnsServer)</p>

31.5 DHCP Status Parameters

Group	snooping_statistics , for all ports[0..31]	
Path	Protocol.DHCP.snooping_statistics[port]	
Description	Statistics indicating activity of DHCP snooping.	
trust_mode	Reflects the determined trust mode.	
	Values	<i>UNDECIDED</i> Value not yet determined <i>UNTRUSTED</i> This port is untrusted and DHCP filtering applies <i>TRUSTED</i> This port is trusted and no filtering occurs.
	OID	1.3.6.1.4.1.3181.10.6.2.49.100.1.2 (snoopingStatisticsTrustMode)
number_of_dhcp_processed	Counts the number of DHCP messages processed.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.2.49.100.1.3 (snoopingStatisticsNumberOfDhcpProcessed)
number_of_dhcp_dropped	Counts the number of DHCP messages dropped.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.2.49.100.1.4 (snoopingStatisticsNumberOfDhcpDropped)
last_drop_reason		
	Values	<i>OK</i> <i>ILLEGAL_DHCP_SERVER</i> Forbidden DHCP message on untrusted port <i>DHCP_SERVER_SPOOFED</i> source MAC and DHCP client MAC did not match <i>ILLEGAL_RELAY_AGENT</i> <i>BINDING_MISMATCH</i> DHCPRELEASE or DHCPDECLINE interface information did not match the binding table information <i>FLOODING</i> Too many DHCP messages which appears to be an attack.
	OID	1.3.6.1.4.1.3181.10.6.2.49.100.1.5 (snoopingStatisticsLastDropReason)

32 Link Layer Discovery Protocol (LLDP)

32.1 Key Features

LLDP reception

Receive LLDP information from neighboring devices per port. Display retrieved information via all NMS interfaces. This includes geographical coordinates and civic location information.

Permits building of network topology map.

LLDP transmission

Geographical coordinates and civic location information can be specified for transmission to neighboring devices.

Permit precise location of the device. This is important in large installations.

LLDP-MED

Media Endpoint Discovery for the auto-discovery of LAN policies. Support of VLAN advertising and PoE+ control.

Permits autoconfiguration of compliant VoIP telephones.

LLDP/CDP preference

Device will prefer standards based LLDP but will automatically accept CDP if present.

Eases integration in multi vendor networks

CDP operation

Support for Cisco Discovery Protocol CDP v1, v2 for automatic detection of capabilities of neighbor CDP enabled devices.

Permits building of network topology map in Cisco environment.

CDP Voice VLAN

Support of Voice VLAN for configuration of connected Cisco VoIP-phone.

Permits autoconfiguration of Cisco VoIP telephones.

32.2 Functional Description

32.2.1 LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a vendor-neutral Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also

defines how to store and maintain information gathered about the neighboring network nodes it discovers.

32.2.2 Basic Type Length Values (TVLs)

The following parameters are included in the LLDP information block:

Management Address

The management address protocol packet includes the IPv4 address of the switch.

Port Description

The port description is taken from the ifDescr object in RFC 2863, which includes information about the manufacturer, the product name, and the version of the interface hardware/software.

System Capabilities

The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.

System Description

The system description is taken from the sysDescr object in RFC 3418, which includes the full name and version identification of the system's hardware type, software operating system, and networking software.

System Name

The system name is taken from the sysName object in RFC 3418, which contains the system's administratively assigned name.

32.2.3 IEEE 802.1 Organizationally Specific TLVs

VLAN ID

The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated

32.2.4 Media Endpoint Discovery(LLDP-MED)

Media Endpoint Discovery is an enhancement of LLDP, formally approved and published by the Telecommunications Industry Association (TIA), known as LLDP-MED. It provides the following capabilities:

- Auto-Discovery of LAN policies (such as VLAN, Layer 2 Priority and Differentiated Services (DiffServ) settings) enabling plug and play networking.
- Device location discovery to allow creation of location databases and, in the case of Voice over Internet Protocol (VoIP), Enhanced 911 services.
- Extended and automated power management of Power over Ethernet (PoE) end points.
- Inventory management, facilitating the administration of network devices including specific information like manufacturer, software and hardware versions, article and serial number.

32.3 LLDP CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Protocol.	lldp.	config.				Link Layer Discovery Protocol (LLDP)
						General settings for LLDP (link layer discovery protocol). This protocol is used to identify the directly attached neighbor devices. This is useful to build a network topology. It is also used to identify voip telephones and to set them up.
			enable_lldp		R/W	This generally enables the link layer discovery protocol (LLDP).
			enable_cdp		R/W	This enables Cisco discovery protocol. Check cdp_version parameter to select CDP version.
			lldp_enabled_ports		R/W	This parameter permits port selective LLDP enabling. When empty all ports are enabled! Syntax: slot/port, slot/port or use hex value for quick setup. Example = 0x7 defines ports 1-3.
			receive_only		R/W	This enables receive only mode. LLDP will not send any frames. It will only listen to its neighbors.
			forward_to_link		R/W	This mode forwards all received LLDP packets to the uplink port. In combination with receive_only option enabled this unit keeps quiet and all LLDP handling should be taken care off by the upstream device.
			advertized_med_class		R/W	Enables emission of LLDP-MED frames of a certain class.
			disable_med_inventory		R/W	Disable LLDP-MED inventory TLV transmission.
			disable_voice_vlan_tlv		R/W	Disable voice vlan indication TLV transmission.
			cdp_version		R/W	Determines which version CDP messages are used.
			voice_vlan_prio		R/W	Layer 2 priority used for voice vlan in voip application.
			voice_vlan_signal_prio		R/W	Layer 2 priority used for voice vlan signaling in voip application.
			voice_dscp		R/W	DiffServ codepoint (0-63) for voip application
			signaling_dscp		R/W	DiffServ codepoint (0-63) for voip signaling

time_to_live	R/W	The time to live value defines the time for which the lldp transmitted details are valid and can be displayed in the status.
tx_delay	R/W	Transmission delay in seconds between successive LLDP frame transmissions initiated by changes in the LLDP local configuration.
msg_tx_interval	R/W	The interval at which LLDP frames are transmitted on behalf of this LLDP agent.
force_lldp_transmission	R/W	Force to send LLDP packets even when there is no LLDP peer detected.
lldp_response_preferred	R/W	When enabled LLDP responses takes precedence over CDP protocol responses.
local_coordinates.		Detailed GPS information about the physical location of this device may be entered here.
latitude	R/W	A value in degrees such as: 50,123
lat_resolution	R/W	A value in bits. Higher value is more accurate.
longitude	R/W	A value in degrees such as: 50,123
long_resolution	R/W	A value in bits. Higher value is more accurate.
altitude	R/W	A value in meters.
alt_resolution	R/W	A value in bits. Higher value is more accurate.
alt_type	R/W	Defines in which way the altitude is interpreted.
datum	R/W	Name of the map the given coordinates are based upon.
local_civic_location.		Detailed address information about the physical location of this device may be entered here. These data are forwarded using the LLDP-MED protocol.
country_code	R/W	Two-letter ISO 3166 country code in capital ASCII letters. Use DE for Germany, etc.
language	R/W	ISO 639 language code used for presenting the address information.
national_subdivision	R/W	National subdivision: state, canton, region, province, or prefecture. Example: Hessen
county	R/W	County / parish / district. Example: Landkreis Darmstadt
town	R/W	City / township. Example: Frankfurt
district	R/W	City district / division / borough / ward.
block	R/W	Neighborhood / block.
street	R/W	Name of the street without house number.
leading_street_direction	R/W	Use any of these values or leave blank: N,E,W,S,NE,NW,SE,SW.

trailing_street_suffix	R/W	Use any of these values or leave blank: N,E,W,S,NE,NW,SE,SW.
street_suffix	R/W	Street suffix such as place or avenue.
house_number	R/W	House number without a possible suffix.
house_number_suffix	R/W	A modifier to the house number. It does not include parts of the house number. Example: a
landmark	R/W	Landmark or vanity address for easier reference. Example: Airport Frankfurt
additional_info	R/W	Additional location information without specified format.
name	R/W	Identifies the person or organization associated with the address. Example: Sunshine Airline Office
zip_code	R/W	Postal zip code for the address.
building	R/W	The name of the building if this exists. Example: Terminal Building East
unit	R/W	Unit / apartment / suite.
floor	R/W	Floor value. Example: 1 for first floor
room	R/W	Room number or name.
place_type	R/W	Place type. Example: Office
script	R/W	The script (from ISO 15924 [14]) used to encode the address information. Default: Latn
elin_number	R/W	Emergency Call Services (ECS) Emergency Location Identification Number (ELIN).

received_overview[PORT].

sys_name	R	System name.
sys_desc	R	System description.
chassis_id_subtype	R	Type of chassis id.
chassis_id	R	Chassis id of received frame.
mgmt_ip	R	Management IP address.
mgmt_oid	R	Management start OID for SNMP access.
capabilities	R	LLDP capabilities supported.
capabilities_enabled	R	LLDP capabilities enabled.
med_capabilities	R	LLDP_MED capabilities.
port_id_subtype	R	Type of port id.
port_identification	R	Port id.
port_description	R	Port description.
port_vlan	R	Port vlan identifier. Related to port_default_vlan_id.

received_coordinates[PORT].

Detailed GPS information about the physical location of the attached device for each port are visible here if provided through the LLDP-MED protocol.		
latitude	R	A value in degrees such as: 50,123

lat_resolution	R	A value in bits. Higher value is more accurate.
longitude	R	A value in degrees such as: 50,123
long_resolution	R	A value in bits. Higher value is more accurate.
altitude	R	A value in meters or the floor level depending on definition.
alt_resolution	R	A value in bits. Higher value is more accurate.
alt_unit	R	Defines in which way the altitude is interpreted.
datum	R	Name of the map the given coordinates are based upon.
received_civic_locations[PORT].		Detailed address information about the physical location of the attached device for each port are visible here if provided through the LLDP-MED protocol.
country_code	R	Two-letter ISO 3166 country code in capital ASCII letters. Use DE for Germany, etc.
language	R	ISO 639 language code used for presenting the address information.
national_subdivision	R	National subdivision: state, canton, region, province, or prefecture. Example: Hessen.
county	R	County / parish / district. Example: Landkreis Darmstadt
town	R	City / township. Example: Frankfurt
district	R	City district / division / borough / ward.
block	R	Neighborhood / block.
street	R	Name of the street without house number.
leading_street_direction	R	Use any of these values or leave blank: N,E,W,S,NE,NW,SE,SW.
trailing_street_suffix	R	Use any of these values or leave blank: N,E,W,S,NE,NW,SE,SW.
street_suffix	R	Street suffix such as place or avenue.
house_number	R	House number without a possible suffix.
house_number_suffix	R	A modifier to the house number. It does not include parts of the house number. Example: a
landmark	R	Landmark or vanity address for easier reference. Example: Airport Frankfurt
additional_info	R	Additional location information without specified format.
name	R	Identifies the person or organization associated with the address. Example: Sunshine Airline Office
zip_code	R	Postal zip code for the address.

building	R	The name of the building if this exists. Example: Terminal Building East
unit	R	Unit / apartment / suite.
floor	R	Floor value. Example: 1 for first floor.
room	R	Room number or name.
place_type	R	Place type. Example: Office.
script	R	The script (from ISO 15924 [14]) used to encode the address information. Default: Latn
elin_number	R	Emergency Call Services (ECS) Emergency Location Identification Number (ELIN).
received_policies[PORT].		Detailed information about the attached applications.
application_type	R	Valid application types.
policy_defined	R	False indicates policy is unknown. True indicates policy is defined.
tagged_vlan	R	When set VLAN tagging is used.
vlan_id	R	0 - only the priority level is significant. / IEEE 802.1q VLAN ID (VID) value. Related to voice vlan.
layer_2_priority	R	IEEE 802.1d / IEEE 802.1p Layer 2 Priority.
dscp	R	DiffServ/Differentiated Services Code Point (DSCP) value as defined in IETF RFC 2474 for the specified application type.
received_inventory_infos[PORT].		This table lists general inventory data of the attached equipment.
hardware_revision	R	Hardware version
firmware_revision	R	Firmware version
software_revision	R	Software version
serial_number	R	Serial number
manufacturer	R	Manufacturer name
model_name	R	Vendor-specific model name
asset_id	R	Vendor-specific asset tracking identifier
received_poe_infos[PORT].		Detailed PoE information about the attached applications.
type	R	Type of PoE equipment.
source	R	Describes the power source.
priority	R	Indicates priority of this device.
value	R	Indicates the power available from the PSE via this port expressed in units of 0.1 watts on the remote device.
received_poe_control[PORT].		
type	R	Indicates device type.
poe_power_supported	R	Indicates if PoE is supported by the interface.
poe_power_enabled	R	Indicates if PoE is enabled for this interface.

pair_control	R	Indicates if the pair selection can be controlled on the given port
power_pairs	R	Indicates which pins of the plug are used for power.
power_class	R	Required PoE class.
device_type	R	Type of PoE equipment.
source	R	Indicates the power source.
priority	R	Priority of the attached port.
pd_requested_power	R	PD requested power value in multiple of 0.1W
pse_allocated_power	R	PSE allocated power value in multiple of 0.1W

32.4 LLDP Configuration Parameters

Group Path Description	config										
	Protocol.LLDP.config General settings for LLDP (link layer discovery protocol). This protocol is used to identify the directly attached neighbor devices. This is useful to build a network topology. It is also used to identify voip telephones and to set them up.										
enable_lldp	This generally enables the link layer discovery protocol (LLDP). Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.2.43.1.1.2 (configEnableLldp)										
enable_cdp	This enables Cisco discovery protocol. Check cdp_version parameter to select CDP version. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.2.43.1.1.3 (configEnableCdp)										
lldp_enabled_ports	This parameter permits port selective LLDP enabling. When empty all ports are enabled! Syntax: slot/port, slot/port or use hex value for quick setup. Example = 0x7 defines ports 1-3. Value PORTMASK0-0xFFFFFFFF OID 1.3.6.1.4.1.3181.10.6.2.43.1.1.4 (configLldpEnabledPorts)										
receive_only	This enables receive only mode. LLDP will not send any frames. It will only listen to its neighbors. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.2.43.1.1.5 (configReceiveOnly)										
forward_to_link	This mode forwards all received LLDP packets to the uplink port. In combination with receive_only option enabled this unit keeps quiet and all LLDP handling should be taken care off by the upstream device. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.2.43.1.1.6 (configForwardToLink)										
advertized_med_class	Enables emission of LLDP-MED frames of a certain class. Values <table> <tr> <td><i>DISABLE_MED</i></td> <td>Disables MED class</td> </tr> <tr> <td><i>GENERIC_ENDPOINT</i></td> <td>Enables generic_endpoint</td> </tr> <tr> <td><i>MEDIA_ENDPOINT</i></td> <td>Enables media_endpoint</td> </tr> <tr> <td><i>COMMUNICATION_ENDPOINT</i></td> <td>Enables communication_endpoint</td> </tr> <tr> <td><i>NETWORK_DEVICE</i></td> <td>Enables networkconnectivity_device</td> </tr> </table> OID 1.3.6.1.4.1.3181.10.6.2.43.1.1.7 (configAdvertizedMedClass)	<i>DISABLE_MED</i>	Disables MED class	<i>GENERIC_ENDPOINT</i>	Enables generic_endpoint	<i>MEDIA_ENDPOINT</i>	Enables media_endpoint	<i>COMMUNICATION_ENDPOINT</i>	Enables communication_endpoint	<i>NETWORK_DEVICE</i>	Enables networkconnectivity_device
<i>DISABLE_MED</i>	Disables MED class										
<i>GENERIC_ENDPOINT</i>	Enables generic_endpoint										
<i>MEDIA_ENDPOINT</i>	Enables media_endpoint										
<i>COMMUNICATION_ENDPOINT</i>	Enables communication_endpoint										
<i>NETWORK_DEVICE</i>	Enables networkconnectivity_device										

disable_med_inventory	Disable LLDP-MED inventory TLV transmission.	
	Values	enabled, disabled
	OID	1.3.6.1.4.1.3181.10.6.2.43.1.1.8 (configDisableMedInventory)
disable_voice_vlan_tlv	Disable voice vlan indication TLV transmission.	
	Values	enabled, disabled
	OID	1.3.6.1.4.1.3181.10.6.2.43.1.1.9 (configDisableVoiceVlanTlv)
cdp_version	Determines which version CDP messages are used.	
	Values	V1_AND_V2 Usually both version may coexist
	V1	Use only version 1
	V2	Use only version 2
	OID	1.3.6.1.4.1.3181.10.6.2.43.1.1.10 (configCdpVersion)
voice_vlan_prio	Layer 2 priority used for voice vlan in voip application.	
	Value	Number in range 0-7
	OID	1.3.6.1.4.1.3181.10.6.2.43.1.1.11 (configVoiceVlanPrio)
voice_vlan_signal_prio	Layer 2 priority used for voice vlan signaling in voip application.	
	Value	Number in range 0-7
	OID	1.3.6.1.4.1.3181.10.6.2.43.1.1.12 (configVoiceVlanSignalPrio)
voice_dscp	DiffServ codepoint (0-63) for voip application	
	Value	Number in range 0-63
	OID	1.3.6.1.4.1.3181.10.6.2.43.1.1.13 (configVoiceDscp)
signaling_dscp	DiffServ codepoint (0-63) for voip signaling	
	Value	Number in range 0-63
	OID	1.3.6.1.4.1.3181.10.6.2.43.1.1.14 (configSignalingDscp)
time_to_live	The time to live value defines the time for which the lldp transmitted details are valid and can be displayed in the status.	
	Value	Number in range 0-255
	OID	1.3.6.1.4.1.3181.10.6.2.43.1.1.15 (configTimeToLive)
tx_delay	Transmission delay in seconds between successive LLDP frame transmissions initiated by changes in the LLDP local configuration.	
	Value	Number in range 1-250
	OID	1.3.6.1.4.1.3181.10.6.2.43.1.1.16 (configTxDelay) 1.0.8802.1.1.2.1.1.4 (lldpTxDelay)

msg_tx_interval	<p>The interval at which LLDP frames are transmitted on behalf of this LLDP agent.</p> <p>Value Number in range 5-32767</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.43.1.1.17 (configMsgTxInterval) 1.0.8802.1.1.2.1.1.1 (lldpMessageTxInterval)</p>
force_lldp_transmission	<p>Force to send LLDP packets even when there is no LLDP peer detected.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.43.1.1.18 (configForceLldpTransmission)</p>
lldp_response_preferred	<p>When enabled LLDP responses takes precedence over CDP protocol responses.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.43.1.1.19 (configLldpResponsePreferred)</p>
Group Path Description	<p>local_coordinates</p> <p>Protocol.LLDP.local_coordinates</p> <p>Detailed GPS information about the physical location of this device may be entered here.</p>
latitude	<p>A value in degrees such as: 50,123</p> <p>Value String, max. 16 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.43.2.1.2 (localCoordinatesLatitude)</p>
lat_resolution	<p>A value in bits. Higher value is more accurate.</p> <p>Value Number in range 0-34</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.43.2.1.3 (localCoordinatesLatResolution)</p>
longitude	<p>A value in degrees such as: 50,123</p> <p>Value String, max. 16 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.43.2.1.4 (localCoordinatesLongitude)</p>
long_resolution	<p>A value in bits. Higher value is more accurate.</p> <p>Value Number in range 0-34</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.43.2.1.5 (localCoordinatesLongResolution)</p>
altitude	<p>A value in meters.</p> <p>Value String, max. 16 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.43.2.1.6 (localCoordinatesAltitude)</p>

alt_resolution	A value in bits. Higher value is more accurate. Value Number in range 0-30 OID 1.3.6.1.4.1.3181.10.6.2.43.2.1.7 (localCoordinatesAltResolution)
alt_type	Defines in which way the altitude is interpreted. Values <i>METER</i> <i>FLOOR</i> OID 1.3.6.1.4.1.3181.10.6.2.43.2.1.8 (localCoordinatesAltType)
datum	Name of the map the given coordinates are based upon. Value String, max. 16 characters. OID 1.3.6.1.4.1.3181.10.6.2.43.2.1.9 (localCoordinatesDatum)
Group Path Description	local_civic_location Protocol.LLDP.local_civic_location Detailed address information about the physical location of this device may be entered here. These data are forwarded using the LLDP-MED protocol.
country_code	Two-letter ISO 3166 country code in capital ASCII letters. Use DE for Germany, etc. Value String, max. 4 characters. OID 1.3.6.1.4.1.3181.10.6.2.43.3.1.2 (localCivicLocationCountryCode)
language	ISO 639 language code used for presenting the address information. Value String, max. 8 characters. OID 1.3.6.1.4.1.3181.10.6.2.43.3.1.3 (localCivicLocationLanguage)
national_subdivision	National subdivision: state, canton, region, province, or prefecture. Example: Hessen Value String, max. 16 characters. OID 1.3.6.1.4.1.3181.10.6.2.43.3.1.4 (localCivicLocationNationalSubdivision)
county	County / parish / district. Example: Landkreis Darmstadt Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.2.43.3.1.5 (localCivicLocationCounty)

town	City / township. Example: Frankfurt
	Value String, max. 32 characters.
	OID 1.3.6.1.4.1.3181.10.6.2.43.3.1.6 (localCivicLocationTown)
district	City district / division / borough / ward.
	Value String, max. 32 characters.
	OID 1.3.6.1.4.1.3181.10.6.2.43.3.1.7 (localCivicLocationDistrict)
block	Neighborhood / block.
	Value String, max. 16 characters.
	OID 1.3.6.1.4.1.3181.10.6.2.43.3.1.8 (localCivicLocationBlock)
street	Name of the street without house number.
	Value String, max. 32 characters.
	OID 1.3.6.1.4.1.3181.10.6.2.43.3.1.9 (localCivicLocationStreet)
leading_street_direction	Use any of these values or leave blank: N,E,W,S,NE,NW,SE,SW.
	Value String, max. 4 characters.
	OID 1.3.6.1.4.1.3181.10.6.2.43.3.1.10 (localCivicLocationLeadingStreetDirection)
trailing_street_suffix	Use any of these values or leave blank: N,E,W,S,NE,NW,SE,SW.
	Value String, max. 4 characters.
	OID 1.3.6.1.4.1.3181.10.6.2.43.3.1.11 (localCivicLocationTrailingStreetSuffix)
street_suffix	Street suffix such as place or avenue.
	Value String, max. 8 characters.
	OID 1.3.6.1.4.1.3181.10.6.2.43.3.1.12 (localCivicLocationStreetSuffix)
house_number	House number without a possible suffix.
	Value String, max. 8 characters.
	OID 1.3.6.1.4.1.3181.10.6.2.43.3.1.13 (localCivicLocationHouseNumber)
house_number_suffix	A modifier to the house number. It does not include parts of the house number. Example: a
	Value String, max. 8 characters.
	OID 1.3.6.1.4.1.3181.10.6.2.43.3.1.14 (localCivicLocationHouseNumberSuffix)

landmark	Landmark or vanity address for easier reference. Example: Airport Frankfurt	
	Value	String, max. 128 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.3.1.15 (localCivicLocationLandmark)
additional_info	Additional location information without specified format.	
	Value	String, max. 128 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.3.1.16 (localCivicLocationAdditionalInfo)
name	Identifies the person or organization associated with the address. Example: Sunshine Airline Office	
	Value	String, max. 128 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.3.1.17 (localCivicLocationName)
zip_code	Postal zip code for the address.	
	Value	String, max. 16 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.3.1.18 (localCivicLocationZipCode)
building	The name of the building if this exists. Example: Terminal Building East	
	Value	String, max. 128 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.3.1.19 (localCivicLocationBuilding)
unit	Unit / apartment / suite.	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.3.1.20 (localCivicLocationUnit)
floor	Floor value. Example: 1 for first floor	
	Value	String, max. 8 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.3.1.21 (localCivicLocationFloor)
room	Room number or name.	
	Value	String, max. 16 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.3.1.22 (localCivicLocationRoom)
place_type	Place type. Example: Office	
	Value	String, max. 16 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.3.1.23 (localCivicLocationPlaceType)
script	The script (from ISO 15924 [14]) used to encode the address information. Default: Latn	
	Value	String, max. 16 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.3.1.24 (localCivicLocationScript)

elin_number	Emergency Call Services (ECS) Emergency Location Identification Number (ELIN).
Value	String, max. 32 characters.
OID	1.3.6.1.4.1.3181.10.6.2.43.3.1.25 (localCivicLocationElinNumber)

32.5 LLDP Status Parameters

Group	received_overview , for all ports[0..31]	
Path	Protocol.LLDP.received_overview[port]	
Description		
sys_name	System name.	
	Value	String, max. 128 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.100.1.2 (receivedOverviewSysName) 1.0.8802.1.1.2.1.4.1.1.9.0 (lldpRemSysName)
sys_desc	System description.	
	Value	String, max. 128 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.100.1.3 (receivedOverviewSysDesc) 1.0.8802.1.1.2.1.4.1.1.10.0 (lldpRemSysDesc)
chassis_id_subtype	Type of chassis id.	
	Values	UNKNOWN CHASSIS_COMPONENT INTERFACE_ALIAS PORT_COMPONENT MAC_ADDRESS NETWORK_ADDRESS INTERFACE_NAME LOCAL
	OID	1.3.6.1.4.1.3181.10.6.2.43.100.1.4 (receivedOverviewChassisIdSubtype) 1.0.8802.1.1.2.1.4.1.1.4.0 (lldpRemChassisIdSubType)
chassis_id	Chassis id of received frame.	
	Value	String, max. 128 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.100.1.5 (receivedOverviewChassisId) 1.0.8802.1.1.2.1.4.1.1.5.0 (lldpRemChassisId)
mgmt_ip	Management IP address.	
	Value	String, max. 128 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.100.1.6 (receivedOverviewMgmtIp) 1.0.8802.1.1.2.1.4.2.1.2.0 (lldpRemManAddr)

mgmt_oid	Management start OID for SNMP access.		
	Value	String, max. 128 characters.	
	OID	1.3.6.1.4.1.3181.10.6.2.43.100.1.7 (receivedOverviewMgmtOid) 1.0.8802.1.1.2.1.4.2.1.5.0 (lldpRemManAddrOID)	
capabilities	LLDP capabilities supported.		
	Values	OTHER	Other capabilities
		REPEATER	Repeater capabilities
		BRIDGE	Bridge capabilities
		WLAN	WLAN capabilities
		ROUTER	Router capabilities
		TELEPHONE	Telephone capabilities
		DOCSIS	DOCSIS capabilities
		STATION	Station capabilities
	OID	1.3.6.1.4.1.3181.10.6.2.43.100.1.8 (receivedOverviewCapabilities) 1.0.8802.1.1.2.1.4.1.1.11.0 (lldpRemSysCapSupported)	
capabilities_enabled	LLDP capabilities enabled.		
	Values	OTHER	Other capabilities
		REPEATER	Repeater capabilities
		BRIDGE	Bridge capabilities
		WLAN	WLAN capabilities
		ROUTER	Router capabilities
		TELEPHONE	Telephone capabilities
		DOCSIS	DOCSIS capabilities
		STATION	Station capabilities
	OID	1.3.6.1.4.1.3181.10.6.2.43.100.1.9 (receivedOverviewCapabilitiesEnabled) 1.0.8802.1.1.2.1.4.1.1.12.0 (lldpRemSysCapEnabled)	
med_capabilities	LLDP_MED capabilities.		
	Values	CAPABILITY	
		POLICY	Policy capabilities
		LOCATION	Location capabilities
		MDI_PSE	MDI/PSE capabilities
		MDI_PD	MDI/PD capabilities
		INVENTORY	Inventory capabilities
	OID	1.3.6.1.4.1.3181.10.6.2.43.100.1.10 (receivedOverviewMedCapabilities) 1.0.8802.1.1.2.1.5.4795.1.1.2.1.1 (lldpXMedPortCapSupported)	

port_id_subtype	Type of port id.	
	Values	UNKNOWN INTERFACE_ALIAS PORT_COMPONENT MAC_ADDRESS NETWORK_ADDRESS INTERFACE_NAME AGENT_CIRCUIT_ID LOCAL
	OID	1.3.6.1.4.1.3181.10.6.2.43.100.1.11 (receivedOverviewPortIdSubtype) 1.0.8802.1.1.2.1.4.1.1.6.0 (lldpRemPortIdSubType)
port_identification	Port id.	
	Value	String, max. 128 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.100.1.12 (receivedOverviewPortIdentification) 1.0.8802.1.1.2.1.4.1.1.7.0 (lldpRemPortId)
port_description	Port description.	
	Value	String, max. 128 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.100.1.13 (receivedOverviewPortDescription) 1.0.8802.1.1.2.1.4.1.1.8.0 (lldpRemPortDesc)
port_vlan	Port vlan identifier. Related to port_default_vlan_id.	
	Value	Number in range 0-65535
	OID	1.3.6.1.4.1.3181.10.6.2.43.100.1.14 (receivedOverviewPortVlan)
Group	received_coordinates , for all ports[0..31]	
Path	Protocol.LLDP.received_coordinates[port]	
Description	Detailed GPS information about the physical location of the attached device for each port are visible here if provided through the LLDP-MED protocol.	
latitude	A value in degrees such as: 50,123	
	Value	String, max. 8 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.101.1.2 (receivedCoordinatesLatitude)

lat_resolution	A value in bits. Higher value is more accurate.
Value	Number in range 0-255
OID	1.3.6.1.4.1.3181.10.6.2.43.101.1.3 (receivedCoordinatesLatResolution)
longitude	A value in degrees such as: 50,123
Value	String, max. 8 characters.
OID	1.3.6.1.4.1.3181.10.6.2.43.101.1.4 (receivedCoordinatesLongitude)
long_resolution	A value in bits. Higher value is more accurate.
Value	Number in range 0-255
OID	1.3.6.1.4.1.3181.10.6.2.43.101.1.5 (receivedCoordinatesLongResolution)
altitude	A value in meters or the floor level depending on definition.
Value	String, max. 8 characters.
OID	1.3.6.1.4.1.3181.10.6.2.43.101.1.6 (receivedCoordinatesAltitude)
alt_resolution	A value in bits. Higher value is more accurate.
Value	Number in range 0-255
OID	1.3.6.1.4.1.3181.10.6.2.43.101.1.7 (receivedCoordinatesAltResolution)
alt_unit	Defines in which way the altitude is interpreted.
Values	<i>METER</i> Altitude value is defined in meters <i>FLOOR</i> Altitude value defines the building floor
OID	1.3.6.1.4.1.3181.10.6.2.43.101.1.8 (receivedCoordinatesAltUnit)
datum	Name of the map the given coordinates are based upon.
Value	String, max. 16 characters.
OID	1.3.6.1.4.1.3181.10.6.2.43.101.1.9 (receivedCoordinatesDatum)

Group
Path
Description

received_civic_locations, for all ports[0..31]
Protocol.LLDP.received_civic_locations[port]
Detailed address information about the physical location of the attached device for each port are visible here if provided through the LLDP-MED protocol.

country_code	Two-letter ISO 3166 country code in capital ASCII letters. Use DE for Germany, etc. Value String, max. 4 characters. OID 1.3.6.1.4.1.3181.10.6.2.43.102.1.2 (receivedCivicLocationsCountryCode)
language	ISO 639 language code used for presenting the address information. Value String, max. 8 characters. OID 1.3.6.1.4.1.3181.10.6.2.43.102.1.3 (receivedCivicLocationsLanguage)
national_subdivision	National subdivision: state, canton, region, province, or prefecture. Example: Hessen. Value String, max. 16 characters. OID 1.3.6.1.4.1.3181.10.6.2.43.102.1.4 (receivedCivicLocationsNationalSubdivision)
county	County / parish / district. Example: Landkreis Darmstadt Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.2.43.102.1.5 (receivedCivicLocationsCounty)
town	City / township. Example: Frankfurt Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.2.43.102.1.6 (receivedCivicLocationsTown)
district	City district / division / borough / ward. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.2.43.102.1.7 (receivedCivicLocationsDistrict)
block	Neighborhood / block. Value String, max. 16 characters. OID 1.3.6.1.4.1.3181.10.6.2.43.102.1.8 (receivedCivicLocationsBlock)
street	Name of the street without house number. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.2.43.102.1.9 (receivedCivicLocationsStreet)
leading_street_direction	Use any of these values or leave blank: N,E,W,S,NE,NW,SE,SW. Value String, max. 4 characters. OID 1.3.6.1.4.1.3181.10.6.2.43.102.1.10 (receivedCivicLocationsLeadingStreetDirection)

trailing_street_suffix	<p>Use any of these values or leave blank: N,E,W,S,NE,NW,SE,SW.</p> <p>Value String, max. 4 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.43.102.1.11 (receivedCivicLocationsTrailingStreetSuffix)</p>
street_suffix	<p>Street suffix such as place or avenue.</p> <p>Value String, max. 8 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.43.102.1.12 (receivedCivicLocationsStreetSuffix)</p>
house_number	<p>House number without a possible suffix.</p> <p>Value String, max. 8 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.43.102.1.13 (receivedCivicLocationsHouseNumber)</p>
house_number_suffix	<p>A modifier to the house number. It does not include parts of the house number. Example: a</p> <p>Value String, max. 8 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.43.102.1.14 (receivedCivicLocationsHouseNumberSuffix)</p>
landmark	<p>Landmark or vanity address for easier reference. Example: Airport Frankfurt</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.43.102.1.15 (receivedCivicLocationsLandmark)</p>
additional_info	<p>Additional location information without specified format.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.43.102.1.16 (receivedCivicLocationsAdditionalInfo)</p>
name	<p>Identifies the person or organization associated with the address. Example: Sunshine Airline Office</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.43.102.1.17 (receivedCivicLocationsName)</p>
zip_code	<p>Postal zip code for the address.</p> <p>Value String, max. 16 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.43.102.1.18 (receivedCivicLocationsZipCode)</p>
building	<p>The name of the building if this exists. Example: Terminal Building East</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.43.102.1.19 (receivedCivicLocationsBuilding)</p>

unit	Unit / apartment / suite.	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.102.1.20 (receivedCivicLocationsUnit)
floor	Floor value. Example: 1 for first floor.	
	Value	String, max. 8 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.102.1.21 (receivedCivicLocationsFloor)
room	Room number or name.	
	Value	String, max. 16 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.102.1.22 (receivedCivicLocationsRoom)
place_type	Place type. Example: Office.	
	Value	String, max. 16 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.102.1.23 (receivedCivicLocationsPlaceType)
script	The script (from ISO 15924 [14]) used to encode the address information. Default: Latn	
	Value	String, max. 16 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.102.1.24 (receivedCivicLocationsScript)
elin_number	Emergency Call Services (ECS) Emergency Location Identification Number (ELIN).	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.102.1.25 (receivedCivicLocationsElinNumber)

Group	received_policies , for all ports[0..31]
Path	Protocol.LLDP.received_policies[port]
Description	Detailed information about the attached applications.

application_type	Valid application types.		
	Values	UNKNOWN	Unspecified application
		VOICE	Used by dedicated IP phone handsets and other similar devices supporting interactive voice services
		VOICE_SIGNALING	Defines a separate policy for the command and control signaling that supports voice applications
		GUEST_VOICE	Limited feature-set voice service for guest users
		GUEST_VOICE_SIGNALING	Defines a separate policy for the command and control signaling that supports guest voice applications
		SOFTPHONE_VOICE	Used by softphone applications that operate on devices, such as PCs or laptop computers
		VIDEO_CONFERENCING	Used by video conferencing applications
		STREAMING_VIDEO	Used for streaming video applications
		VIDEO_SIGNALING	Defines a separate policy for the command and control of video applications
	OID	1.3.6.1.4.1.3181.10.6.2.43.103.1.2 (receivedPoliciesApplicationType) 1.0.8802.1.1.2.1.5.4795.1.3.2.1.1 (IldpXMedRemMediaPolicyAppType)	

policy_defined	False indicates policy is unknown. True indicates policy is defined.		
	Values	true, false	
	OID	1.3.6.1.4.1.3181.10.6.2.43.103.1.3 (receivedPoliciesPolicyDefined) 1.0.8802.1.1.2.1.5.4795.1.3.2.1.5 (IldpXMedRemMediaPolicyUnknown)	

tagged_vlan	When set VLAN tagging is used.		
	Values	true, false	
	OID	1.3.6.1.4.1.3181.10.6.2.43.103.1.4 (receivedPoliciesTaggedVlan) 1.0.8802.1.1.2.1.5.4795.1.3.2.1.6 (IldpXMedRemMediaPolicyTagged)	

vlan_id	0 - only the priority level is significant. / IEEE 802.1q VLAN ID (VID) value. Related to voice vlan.		
	Value	Number in range 0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.2.43.103.1.5 (receivedPoliciesVlanId) 1.0.8802.1.1.2.1.5.4795.1.3.2.1.2 (IldpXMedRemMediaPolicyVlanID)	

layer_2_priority	IEEE 802.1d / IEEE 802.1p Layer 2 Priority.	
	Values UNKNOWN BACKGROUND SPARE BEST_EFFORT Default EXCELLENT_EFFORT CONTROLLED_LOAD VIDEO VOICE NETWORK_CONTROL	
	OID 1.3.6.1.4.1.3181.10.6.2.43.103.1.6 (receivedPoliciesLayer2Priority) 1.0.8802.1.1.2.1.5.4795.1.3.2.1.3 (IldpXMedRemMediaPolicyPriority)	
dscp	DiffServ/Differentiated Services Code Point (DSCP) value as defined in IETF RFC 2474 for the specified application type.	
	Value Number in range 0-255	
	OID 1.3.6.1.4.1.3181.10.6.2.43.103.1.7 (receivedPoliciesDscp) 1.0.8802.1.1.2.1.5.4795.1.3.2.1.4 (IldpXMedRemMediaPolicyDscp)	
Group	received_inventory_infos , for all ports[0..31]	
Path	Protocol.LLDP.received_inventory_infos[port]	
Description	This table lists general inventory data of the attached equipment.	
hardware_revision	Hardware version	
	Value String, max. 32 characters.	
	OID 1.3.6.1.4.1.3181.10.6.2.43.104.1.2 (receivedInventoryInfosHardwareRevision) 1.0.8802.1.1.2.1.5.4795.1.3.3.1.1.0 (IldpXMedRemHardwareRev)	
firmware_revision	Firmware version	
	Value String, max. 32 characters.	
	OID 1.3.6.1.4.1.3181.10.6.2.43.104.1.3 (receivedInventoryInfosFirmwareRevision) 1.0.8802.1.1.2.1.5.4795.1.3.3.1.2.0 (IldpXMedRemFirmwareRev)	

software_revision	Software version	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.104.1.4 (receivedInventoryInfosSoftwareRevision) 1.0.8802.1.1.2.1.5.4795.1.3.3.1.3.0 (IldpXMedRemSoftwareRev)
serial_number	Serial number	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.104.1.5 (receivedInventoryInfosSerialNumber) 1.0.8802.1.1.2.1.5.4795.1.3.3.1.4.0 (IldpXMedRemSerialNum)
manufacturer	Manufacturer name	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.104.1.6 (receivedInventoryInfosManufacturer) 1.0.8802.1.1.2.1.5.4795.1.3.3.1.5.0 (IldpXMedRemMfgName)
model_name	Vendor-specific model name	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.104.1.7 (receivedInventoryInfosModelName) 1.0.8802.1.1.2.1.5.4795.1.3.3.1.6.0 (IldpXMedRemModelName)
asset_id	Vendor-specific asset tracking identifier	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.43.104.1.8 (receivedInventoryInfosAssetId) 1.0.8802.1.1.2.1.5.4795.1.3.3.1.7.0 (IldpXMedRemAssetID)
Group	received_poe_infos , for all ports[0..31]	
Path	Protocol.LLDP.received_poe_infos[port]	
Description	Detailed PoE information about the attached applications.	
type	Type of PoE equipment.	
	Values	<i>UNKNOWN</i> No information received <i>PSE</i> Power Sourcing Equipment <i>PD</i> Powered Device <i>NO_POE</i> The device does not support PoE
	OID	1.3.6.1.4.1.3181.10.6.2.43.105.1.2 (receivedPoeInfosType) 1.0.8802.1.1.2.1.5.4795.1.3.5.1.1 (IldpXMedRemXPoEDeviceType)

source	Describes the power source.		
	Values	UNKNOWN	No information received
		PD_PSE_PRIMARY	For type PD: Power source is the PSE. For type PSE: Power source is the primary power source
		PD_LOCAL_BACKUP	For type PD: Power source is a local source. For type PSE: Power source is the backup power source
		PD_PSE_LOCAL	For type PD: The power source is both the PSE and a local source. For type PSE: this value should not occur
OID	1.3.6.1.4.1.3181.10.6.2.43.105.1.3 (receivedPoeInfosSource) 1.0.8802.1.1.2.1.5.4795.1.3.6.1.2 (IldpXMedRemXPoEPSEPowerSource)		

priority	Indicates priority of this device.		
	Values	UNKNOWN	No information received
		CRITICAL	Critical priority
		HIGH	High priority
		LOW	Low priority
OID	1.3.6.1.4.1.3181.10.6.2.43.105.1.4 (receivedPoeInfosPriority) 1.0.8802.1.1.2.1.5.4795.1.3.6.1.3 (IldpXMedRemXPoEPSEPowerPriority)		

value	Indicates the power available from the PSE via this port expressed in units of 0.1 watts on the remote device.		
	Value	Number in range 0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.2.43.105.1.5 (receivedPoeInfosValue) 1.0.8802.1.1.2.1.5.4795.1.3.6.1.1 (IldpXMedRemXPoEPSEPowerAv)	

Group	received_poe_control, for all ports[0..31]
Path	Protocol.LLDP.received_poe_control[port]
Description	

type	Indicates device type.		
	Values	UNKNOWN	No information received
		PSE	Power Sourcing Equipment
		PD	Powered Device
		NO_POE	The device does not support PoE
OID	1.3.6.1.4.1.3181.10.6.2.43.106.1.2 (receivedPoeControlType) 1.3.111.2.802.3.1.5.1.3.2.1.1 (IldpV2Xdot3RemPowerPortClass)		

poe_power_supported	Indicates if PoE is supported by the interface.
	Values true, false OID 1.3.6.1.4.1.3181.10.6.2.43.106.1.3 (receivedPoeControlPoePowerSupported) 1.3.111.2.802.3.1.5.1.3.2.1.2 (IldpV2Xdot3RemPowerMDISupported)
poe_power_enabled	Indicates if PoE is enabled for this interface.
	Values true, false OID 1.3.6.1.4.1.3181.10.6.2.43.106.1.4 (receivedPoeControlPoePowerEnabled) 1.3.111.2.802.3.1.5.1.3.2.1.3 (IldpV2Xdot3RemPowerMDIEnabled)
pair_control	Indicates if the pair selection can be controlled on the given port
	Values true, false OID 1.3.6.1.4.1.3181.10.6.2.43.106.1.5 (receivedPoeControlPairControl) 1.3.111.2.802.3.1.5.1.3.2.1.4 (IldpV2Xdot3RemPowerPairControlable)
power_pairs	Indicates which pins of the plug are used for power.
	Values <i>SIGNAL</i> The signal pairs only are in use <i>SPARE</i> The spare pairs only are in use OID 1.3.6.1.4.1.3181.10.6.2.43.106.1.6 (receivedPoeControlPowerPairs) 1.3.111.2.802.3.1.5.1.3.2.1.5 (IldpV2Xdot3RemPowerPairs)
power_class	Required PoE class.
	Values <i>NO_CLASS</i> <i>CLASS_0</i> <i>CLASS_1</i> <i>CLASS_2</i> <i>CLASS_3</i> <i>CLASS_4</i> OID 1.3.6.1.4.1.3181.10.6.2.43.106.1.7 (receivedPoeControlPowerClass) 1.3.111.2.802.3.1.5.1.3.2.1.6 (IldpV2Xdot3RemPowerClass)
device_type	Type of PoE equipment.
	Value Number in range 0-255 OID 1.3.6.1.4.1.3181.10.6.2.43.106.1.8 (receivedPoeControlDeviceType) 1.3.111.2.802.3.1.5.1.3.2.1.7 (IldpV2Xdot3RemPowerType)

source	Indicates the power source.		
	Values	UNKNOWN	No information received
		PD_PSE_PRIMARY	For type PD: Power source is the PSE. For type PSE: Power source is the primary power source
		PD_LOCAL_BACKUP	For type PD: Power source is a local source. For type PSE: Power source is the backup power source
		PD_PSE_LOCAL	For type PD: The power source is both the PSE and a local source. For type PSE: this value should not occur
	OID	1.3.6.1.4.1.3181.10.6.2.43.106.1.9 (receivedPoeControlSource) 1.3.111.2.802.3.1.5.1.3.2.1.8 (IldpV2Xdot3RemPowerSource)	

priority	Priority of the attached port.		
	Values	UNKNOWN	No information received
		CRITICAL	Critical priority
		HIGH	High priority
		LOW	Low priority
	OID	1.3.6.1.4.1.3181.10.6.2.43.106.1.10 (receivedPoeControlPriority) 1.3.111.2.802.3.1.5.1.3.2.1.9 (IldpV2Xdot3RemPowerPriority)	

pd_requested_power	PD requested power value in multiple of 0.1W		
	Value	Number in range 0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.2.43.106.1.11 (receivedPoeControlPdRequestedPower) 1.3.111.2.802.3.1.5.1.3.2.1.10 (IldpV2Xdot3RemPDRRequestedPowerValue)	

pse_allocated_power	PSE allocated power value in multiple of 0.1W		
	Value	Number in range 0-0xFFFFFFFF	
	OID	1.3.6.1.4.1.3181.10.6.2.43.106.1.12 (receivedPoeControlPseAllocatedPower) 1.3.111.2.802.3.1.5.1.3.2.1.11 (IldpV2Xdot3RemPSEAllocatedPowerValue)	

33 Link Aggregation Control Protocol (LACP)

33.1 Key Features

Static Link Aggregation

Multiplies available bandwidth between two end points. The setup is manually. Up to 16 groups of any number of ports per group.

Bandwidth is shared to increase link throughput.

Dynamic Link Aggregation

Multiplies available bandwidth between two end points. The setup is dynamic within a predefined group of ports.

The protocol negotiates a slower link to automatically continue operation in the event of a (sub)link failure.

Load Balancing and Trunking

Load balancing between ports that have the same path increases throughput and provides a backup link upon failure. Also known as EtherChannel (in LACP mode).

Increased uplink throughput and improved resilience against link failures.

IEEE 802.1X Supplicant should authenticate on every port of a LACP trunk

If the uplink interface of the device is an aggregated LACP trunk, it is possible to use the IEEE 802.1X Supplicant to authenticate on the upstream switch port. To use this feature just configure the Supplicant port as one of the ports of the LACP trunk.

33.2 Functional Description

Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel for the purpose of providing fault-tolerance and high-speed links between switches, routers and servers.

LACP works by sending frames (LACPDUs) down all links that have the protocol enabled. If it finds a device on the other end of the link that also has LACP enabled, it will also independently send frames along the same links enabling the two units to detect multiple links between themselves and then combine them into a single logical link.

LACP can be configured in one of two modes: active or passive. In active mode it will always send frames along the configured links. In passive mode however, it acts as "speak when spoken to", and therefore can be used as a way of controlling accidental loops (as long as the other device is in active mode).

Example

For LACP the aggregation type must be set to dynamic (default value):

```
Protocol.LACP.config.link_aggregation = DYNAMIC
```

The LACP mode can be set to active (default value) or passive. In active mode, each port actively sends LACP packets. In passive mode, each port will only respond to received LACP packets:

```
Protocol.LACP.config.mode = ACTIVE
```

The LACP implementation supports a maximum of 16 aggregation groups (channels) with the channel id ranging from 1 to 16. Before using LACP, at least one group must be defined:

```
Protocol.LACP.trunk_config[1].trunk_enable = Enabled
```

This enables the aggregation group with id#1.

Now this channel can be assigned to the member ports:

```
Protocol.LACP.port_config[2/1].trunk_id = 1  
Protocol.LACP.port_config[2/2].trunk_id = 1  
Protocol.LACP.port_config[2/3].trunk_id = 1  
Protocol.LACP.port_config[2/4].trunk_id = 1
```

This assigns ports 2/1 to 2/4 as member of the LACP channel with id#1. Please note that the default trunk_id value is 0 which means no channel.

Now LACP works on the configured ports.

33.3 LACP CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Protocol.	lACP.					Link Aggregation Control Protocol (LACP)
			enable_lACP	R/W		General enable of LACP function.
	config.		link_aggregation	R/W		With static setting the link aggregation operates exactly on the ports defined via trunk configuration. Dynamic uses protocol between both endpoints to dynamically use as many or little links as currently available.
			system_priority	R/W		Priority associated with the system.
			mode	R/W		Determines active or passive operational mode.
			transmit_interval	R/W		Determine LACP PDU interval.
			port_config[PORT].			Configuration parameter concerning the port specific LACP settings
			trunk_id	R/W		All ports with the same trunk_id form a common trunk. Use trunk_id 0 for ports that do not belong to any LACP trunk. The trunk_id corresponds to the trunk_config[index].
		trunk_config[16].				Each trunk is referenced by its index number.
			name	R/W		Unique name used to identify the trunk Interface.
			trunk_enable	R/W		Enables the trunk for operation. When disabled, trunk is brought down.
		port_status[PORT].				Displays the negotiated and active settings of LACP parameters.
			trunk_name	R		Name of the trunk to which port is associated.
			trunk_id	R		interface index value of the trunk to which port is attached.
			activity_mode	R		
			synchronized	R		True when trunk is synchronized.
			aggregation_possible	R		Indicates link is aggregable or not.
			collection	R		Collection of incoming frames on this link is enabled or disabled.
			distribution	R		Distribution of outgoing frames on this link is enabled or disabled.

expired_state	R	True indicates that the actor is in the EXPIRED state
defaulted_state	R	When true default configured operational partner information are used. If false the partner information in use has been received in a LACP PDU.
actor_status[PORT].		Actor specific status values.
system_priority	R	Priority associated with the system
system_id	R	Mac address of the switch
port	R	Port number assigned by LACP which is local to LACP.
priority	R	Priority assigned to the port.
admin_key	R	current administration key value of the port.
oper_key	R	current operational key value of the port.
transmit_interval	R	Indicates the link partners transmit interval.
partner_status[PORT].		Partner specific status values.
system_priority	R	Priority associated with the system
system_id	R	Mac address of the switch
port	R	Port number assigned by LACP which is local to LACP.
priority	R	Priority assigned to the port.
admin_key	R	current administration key value of the port.
oper_key	R	current operational key value of the port.
receive_interval	R	Partner requesting transmission interval from actor. TRUE send PDUs for every 1 sec, FALSE every 30 secs.
activity_mode	R	
synchronized	R	True when trunk is synchronized.
aggregation_possible	R	Indicates link is aggregable or not.
collection	R	Collection of incoming frames on this link is enabled or disabled.
distribution	R	Distribution of outgoing frames on this link is enabled or disabled.
expired_state	R	True indicates that the actor is in the EXPIRED state
defaulted_state	R	When true default configured operational partner information are used. If false the partner information in use has been received in a LACP PDU.

33.4 LACP Configuration Parameters

Group Path	General Parameters Protocol.LACP
enable_lacp	<p>General enable of LACP function.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.54.1 (lacpEnableLacp)</p>
Group Path Description	port_config , for each port[0..24] Protocol.LACP.port_config[port] Configuration parameter concerning the port specific LACP settings
trunk_id	<p>All ports with the same trunk_id form a common trunk. Use trunk_id 0 for ports that do not belong to any LACP trunk. The trunk_id corresponds to the trunk_config[index].</p> <p>Value Number in range 0-16</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.54.3.1.2 (portConfigTrunkId)</p>
Group Path Description	config Protocol.LACP.config
link_aggregation	<p>With static setting the link aggregation operates exactly on the ports defined via trunk configuration. Dynamic uses protocol between both endpoints to dynamically use as many or little links as currently available.</p> <p>Values <i>STATIC</i> Only respond to received LACP PDU <i>DYNAMIC</i> Actively send LACP PDUs every 30s</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.54.2.1.2 (configLinkAggregation)</p>
system_priority	<p>Priority associated with the system.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.54.2.1.3 (configSystemPriority)</p>

mode	Determines active or passive operational mode.
Values	<i>PASSIVE</i> Only respond to received LACP PDU <i>ACTIVE</i> Actively send LACP PDUs every 30s
OID	1.3.6.1.4.1.3181.10.6.2.54.2.1.4 (configMode)

transmit_interval	Determine LACP PDU interval.
Values	<i>SLOW</i> Request partner to send LACP PDUs every 30 sec <i>FAST</i> Request partner to send LACP PDUs every 1 sec
OID	1.3.6.1.4.1.3181.10.6.2.54.2.1.5 (configTransmitInterval)

33.5 LACP Status Parameters

Group	port_status , for each port[0..24]	
Path	Protocol.LACP.port_status[port]	
Description	Displays the negotiated and active settings of LACP parameters.	
trunk_name	Name of the trunk to which port is associated.	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.54.100.1.2 (portStatusTrunkName)
trunk_id	interface index value of the trunk to which port is attached.	
	Value	Number in range 0-255
	OID	1.3.6.1.4.1.3181.10.6.2.54.100.1.3 (portStatusTrunkId)
activity_mode		
	Values	<i>PASSIVE</i> Only respond to received LACP PDU <i>ACTIVE</i> Actively send LACP PDUs every 30s
	OID	1.3.6.1.4.1.3181.10.6.2.54.100.1.4 (portStatusActivityMode)
synchronized	True when trunk is synchronized.	
	Values	true, false
	OID	1.3.6.1.4.1.3181.10.6.2.54.100.1.5 (portStatusSynchronized)
aggregation_possible	Indicates link is aggregable or not.	
	Values	true, false
	OID	1.3.6.1.4.1.3181.10.6.2.54.100.1.6 (portStatusAggregationPossible)
collection	Collection of incoming frames on this link is enabled or disabled.	
	Values	true, false
	OID	1.3.6.1.4.1.3181.10.6.2.54.100.1.7 (portStatusCollection)
distribution	Distribution of outgoing frames on this link is enabled or disabled.	
	Values	true, false
	OID	1.3.6.1.4.1.3181.10.6.2.54.100.1.8 (portStatusDistribution)
expired_state	True indicates that the actor is in the EXPIRED state	
	Values	true, false
	OID	1.3.6.1.4.1.3181.10.6.2.54.100.1.9 (portStatusExpiredState)

defaulted_state	When true default configured operational partner information are used. If false the partner information in use has been received in a LACP PDU. Values true, false OID 1.3.6.1.4.1.3181.10.6.2.54.100.1.10 (portStatusDefaultedState)
Group Path Description	actor_status , for each port[0..24] Protocol.LACP.actor_status[port] Actor specific status values.
system_priority	Priority associated with the system Value Number in range 0-65535 OID 1.3.6.1.4.1.3181.10.6.2.54.101.1.2 (actorStatusSystemPriority)
system_id	Mac address of the switch Format MAC Address <i>hh-hh-hh-hh-hh-hh</i> (hh = hexadecimal number between 00 to ff) OID 1.3.6.1.4.1.3181.10.6.2.54.101.1.3 (actorStatusSystemId)
port	Port number assigned by LACP which is local to LACP. Value Number in range 0-65535 OID 1.3.6.1.4.1.3181.10.6.2.54.101.1.4 (actorStatusPort)
priority	Priority assigned to the port. Value Number in range 0-65535 OID 1.3.6.1.4.1.3181.10.6.2.54.101.1.5 (actorStatusPriority)
admin_key	current administration key value of the port. Value Number in range 0-65535 OID 1.3.6.1.4.1.3181.10.6.2.54.101.1.6 (actorStatusAdminKey)
oper_key	current operational key value of the port. Value Number in range 0-65535 OID 1.3.6.1.4.1.3181.10.6.2.54.101.1.7 (actorStatusOperKey)
transmit_interval	Indicates the link partners transmit interval. Values <i>SLOW</i> Partner is sending LACP PDUs every 30 sec <i>FAST</i> Partner is sending LACP PDUs every 1 sec OID 1.3.6.1.4.1.3181.10.6.2.54.101.1.8 (actorStatusTransmitInterval)

Group	partner_status , for each port[0..24]
Path	Protocol.LACP.partner_status[port]
Description	Partner specific status values.
system_priority	<p>Priority associated with the system</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.54.102.1.2 (partnerStatusSystemPriority)</p>
system_id	<p>Mac address of the switch</p> <p>Format MAC Address <i>hh-hh-hh-hh-hh-hh</i> (<i>hh</i> = hexadecimal number between 00 to ff)</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.54.102.1.3 (partnerStatusSystemId)</p>
port	<p>Port number assigned by LACP which is local to LACP.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.54.102.1.4 (partnerStatusPort)</p>
priority	<p>Priority assigned to the port.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.54.102.1.5 (partnerStatusPriority)</p>
admin_key	<p>current administration key value of the port.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.54.102.1.6 (partnerStatusAdminKey)</p>
oper_key	<p>current operational key value of the port.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.54.102.1.7 (partnerStatusOperKey)</p>
receive_interval	<p>Partner requesting transmission interval from actor. TRUE send PDUs for every 1 sec, FALSE every 30 secs.</p> <p>Values <i>SLOW</i> Partner is sending LACP PDUs every 30 sec <i>FAST</i> Partner is sending LACP PDUs every 1 sec</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.54.102.1.8 (partnerStatusReceiveInterval)</p>

activity_mode		
	Values	<i>PASSIVE</i> Only respond to received LACP PDU <i>ACTIVE</i> Actively send LACP PDUs every 30s
	OID	1.3.6.1.4.1.3181.10.6.2.54.102.1.9 (partnerStatusActivityMode)
synchronized		True when trunk is synchronized.
	Values	true, false
	OID	1.3.6.1.4.1.3181.10.6.2.54.102.1.10 (partnerStatusSynchronized)
aggregation_possible		Indicates link is aggregable or not.
	Values	true, false
	OID	1.3.6.1.4.1.3181.10.6.2.54.102.1.11 (partnerStatusAggregationPossible)
collection		Collection of incoming frames on this link is enabled or disabled.
	Values	true, false
	OID	1.3.6.1.4.1.3181.10.6.2.54.102.1.12 (partnerStatusCollection)
distribution		Distribution of outgoing frames on this link is enabled or disabled.
	Values	true, false
	OID	1.3.6.1.4.1.3181.10.6.2.54.102.1.13 (partnerStatusDistribution)
expired_state		True indicates that the actor is in the EXPIRED state
	Values	true, false
	OID	1.3.6.1.4.1.3181.10.6.2.54.102.1.14 (partnerStatusExpiredState)
defaulted_state		When true default configured operational partner information are used. If false the partner information in use has been received in a LACP PDU.
	Values	true, false
	OID	1.3.6.1.4.1.3181.10.6.2.54.102.1.15 (partnerStatusDefaultedState)

34 Ring

34.1 Key Features

MICROSENS Ring Protocol

MICROSENS ring redundancy protocol. Up to 2 independent rings can be handled by a single device simultaneously. Typical 50ms ring recovery upon break of a ring is provided. The previous generation G5 and the G6 Ring protocols are compatible and interwork.

MICROSENS ring protocol does not require any third party license costs.

34.2 Functional Description

The Ring protocol is designed to automatically switchover data traffic in a ring network, should a failure in one of the ports or cables occur. In case of failure of a node or segment, the ring master automatically reconfigures the remaining switches for continued data flow.

Up to two independent rings can be handled by the switch simultaneously. Each ring may typical have 10- 20 other switches as members.

34.3 Ring CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Protocol.	ring.		Proprietary redundant ring and MRP ring related settings and status values.			
	config[2].		This section is used to configure the MICROSENS ring protocol which provides fast network redundancy.			
			name		R/W	User defined ring name is purely informational.
			enable_ring		R/W	Used to enable the redundant ring function.
			ring_master		R/W	When enabled this unit is designated as ring master. There can only be one master in a ring.
			number		R/W	Ring number must be set identical for each member of a ring. When left unassigned the default setting 1 for index 1 and 2 for index 2 is used.
			port_a		R/W	Port number for ring side A
			port_b		R/W	Port number for ring side B. Ring master blocks B when ring is ok
	mrp_config.		This section is used to configure the MRP ring protocol.			
			enable_mrp		R/W	Used to enable the MRP ring function. Only enable when all MRP and VLAN settings have been set. Only close cable connections of the ring when all nodes have been enabled.
			domain_name		R/W	User defined ring name is purely informational. When specified, the name will be inserted in all MRP related events. When left blank, the UUID of the MRP ring is inserted instead.
			expected_role		R/W	Determines role of this node in the ring. Configure only one master per ring.

react_on_link_change	R/W	When enabled the manager reacts to link change messages from a client. Disable this feature only when any member of the ring does not support react on link change feature. Also known as Advanced Mode. Only applies to manager role.
recovery_time	R/W	Specifies the guaranteed maximum recovery time (i.e. Time from the fault event to the time when the network regains its required communication function). Only applies to manager role.
port_1	R/W	Port number for ring side 1
port_2	R/W	Port number for ring side 2. Ring master blocks B when ring is ok
vlan_id	R/W	When using a VLAN ensure that the rings ports are configured as member of the VLAN in the vlan settings. Leave this field blank or set to 0 when no VLAN is used.
reset_round_trip_delays	X	When executed the min_round_trip_delay and max_round_trip_delay values are reset to 0. This has no service implications.
reset_statistics	X	When executed statistics related to this MRP ring are cleared. This has no service implications.
status[2].		Status values display the current condition of the ring network.
state	R	
last_state_change	R	Time and date string indication when the state of the ring protocol has last changed to the state now indicated.
ring_interrupt	R	
global_ring_alarm	R	
error_detected	R	
ring_port_a_interrupted	R	
ring_port_b_interrupted	R	
statistics[2].		Statistics of the ring network performance.
number_of_backups	R	Counts the number of backups engaged since the last power up.
current_backup_duration	R	Indicates since how long a currently active backup is established. When no backup is active a 0 is displayed.
last_backup_duration	R	Indicates since how long the last backup was established. Indicates 0 if there was no backup since last reboot.
total_backup_duration	R	Total time the ring was in backup since last reboot.
coupling_status.		Indicates status of ring coupling function.

controller_state	R	Data transmission state.
cport_link	R	Coupling port is in linkup condition.
cport_forward	R	Coupling port is in forwarding state.
cport_timeout	R	Indicates that no ring coupling frames were received within defined period.
connection_valid	R	Indicates that source ip address of received frame matches configured partner ip.
valid_partner_ip	R	Indicates that received ring number matches expected locally configured ring number.
valid_partner_id	R	
mrp_status.		Status common to manager and client
operation	R	Indicates if MRP function is enabled.
admin_role	R	Mirrors expected role configuration.
operational_role	R	real_role ??
port_1_state	R	
port_2_state	R	
domain_id	R	When left blank the default id of all bits 1 is used.
domain_error	R	
mrp_manager_status.		Status that applies to manager only. Invalid when in client mode.
ring_state	R	Indicates of MRP is enabled on this device.
manager_priority	R	The priority of this MRP entity.
ring_open_count	R	Counts how many times was the ring broken.
time_since_last_ring_open	R	Seconds since the ring was last opened.
max_round_trip_delay	R	The longest round trip delay that was measured since value reset. Value in microseconds
min_round_trip_delay	R	The shortest round trip delay that was measured since value reset. Value in microseconds
topology_change_interval	R	Interval for sending of MRP_TopologyChange messages
topo_change_repeat_count	R	Topology change repeat count for repeated transmission of MRP_TopologyChange messages
short_test_interval	R	Short interval for sending of MRP_Test messages after link changes on the ring
default_test_interval	R	Default interval for sending of MRP_Test messages on the ring
test_monitor_count	R	Count for monitoring the reception of MRP_Test messages

test_monitor_ext_count	R	The extended interval count for monitoring the reception of MRP_Test messages
nonblocking_support	R	False indicates that the manager requires ring clients that support port blocking. This is standard behavior of any modern switch.
mrp_client_status.		Status that applies to client only. Invalid when in manager mode.
link_down_timer	R	The interval for sending of MRP_linkDown messages
link_up_timer	R	The interval for sending of MRP_linkUp messages
link_change_count	R	The count for repeated transmission of MRP_LinkChange messages
blocked_support	R	True indicates that this client supports port blocking. The value is always true.

34.4 Ring Configuration Parameters

Group	config , for all ring indices [1..2]
Path	Protocol.Ring.config[index]
Description	This section is used to configure the MICROSENS ring protocol which provides fast network redundancy.
name	User defined ring name is purely informational. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.2.45.1.1.2 (configName)
enable_ring	Used to enable the redundant ring function. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.2.45.1.1.3 (configEnableRing)
ring_master	When enabled this unit is designated as ring master. There can only be one master in a ring. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.2.45.1.1.4 (configRingMaster)
number	Ring number must be set identical for each member of a ring. When left unassigned the default setting 1 for index 1 and 2 for index 2 is used. Value Number in range 0-255 OID 1.3.6.1.4.1.3181.10.6.2.45.1.1.5 (configNumber)
port_a	Port number for ring side A Value PORT0-255 OID 1.3.6.1.4.1.3181.10.6.2.45.1.1.6 (configPortA)
port_b	Port number for ring side B. Ring master blocks B when ring is ok Value PORT0-255 OID 1.3.6.1.4.1.3181.10.6.2.45.1.1.7 (configPortB)
Group	mrp_config
Path	Protocol.Ring.mrp_config
Description	This section is used to configure the MRP ring protocol.

enable_mrp	<p>Used to enable the MRP ring function. Only enable when all MRP and VLAN settings have been set. Only close cable connections of the ring when all nodes have been enabled. ATTENTION: Not implemented.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.2.1.2 (mrpConfigEnableMrp)</p>
domain_name	<p>User defined ring name is purely informational. When specified, the name will be inserted in all MRP related events. When left blank, the UUID of the MRP ring is inserted instead. ATTENTION: Not implemented.</p> <p>Value String, max. 240 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.2.1.3 (mrpConfigDomainName) 1.0.62439.1.1.1.3 (mrpDomainName)</p>
expected_role	<p>Determines role of this node in the ring. Configure only one master per ring. ATTENTION: Not implemented.</p> <p>Values <i>CLIENT</i> Normal ring node <i>MANAGER</i> Master ring node</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.2.1.4 (mrpConfigExpectedRole)</p>
react_on_link_change	<p>When enabled the manager reacts to link change messages from a client. Disable this feature only when any member of the ring does not support react on link change feature. Also known as Advanced Mode. Only applies to manager role. ATTENTION: Not implemented.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.2.1.5 (mrpConfigReactOnLinkChange) 1.0.62439.1.1.1.20 (mrpDomainMRMReactOnLinkChange)</p>
recovery_time	<p>Specifies the guaranteed maximum recovery time (i.e. Time from the fault event to the time when the network regains its required communication function). Only applies to manager role. ATTENTION: Not implemented.</p> <p>Values <i>RECOVERY_TIME_500_MS</i> Worst ring recovery time is 500ms <i>RECOVERY_TIME_200_MS</i> Worst ring recovery time is 200ms</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.2.1.6 (mrpConfigRecoveryTime)</p>
port_1	<p>Port number for ring side 1 ATTENTION: Not implemented.</p> <p>Value PORT0-255</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.2.1.7 (mrpConfigPort1) 1.0.62439.1.1.1.6 (mrpDomainRingPort1)</p>

port_2	<p>Port number for ring side 2. Ring master blocks B when ring is ok ATTENTION: Not implemented.</p>
	<p>Value PORT0-255</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.2.1.8 (mrpConfigPort2) 1.0.62439.1.1.1.8 (mrpDomainRingPort2)</p>
vlan_id	<p>When using a VLAN ensure that the rings ports are configured as member of the VLAN in the vlan settings. Leave this field blank or set to 0 when no VLAN is used. ATTENTION: Not implemented.</p>
	<p>Value Number in range 0-4095</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.2.1.9 (mrpConfigVlanId) 1.0.62439.1.1.1.13 (mrpDomainVlanId)</p>
reset_round_trip_delays	<p>When executed the min_round_trip_delay and max_round_trip_delay values are reset to 0. This has no service implications. ATTENTION: Not implemented.</p>
	<p>Action Excecute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.2.1.10 (mrpConfigResetRoundTripDelays) 1.0.62439.1.1.1.19 (mrpDomainResetRoundTripDelays)</p>
reset_statistics	<p>When executed statistics related to this MRP ring are cleared. This has no service implications. ATTENTION: Not implemented.</p>
	<p>Action Excecute command.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.2.1.11 (mrpConfigResetStatistics)</p>

34.5 Ring Status Parameters

Group	status, for all ring indices [1..2]		
Path	Protocol.Ring.status[index]		
Description	Status values display the current condition of the ring network.		
state	Values	UNUSED	Ring function is not enabled
		NORMAL	Normal condition with no errors detected
		BACKUP	A single error in the ring has occurred and is healed by the ring protection function. Communication continues
		ERROR	Errors in the ring have been detected. These cannot be recovered. Possible communication loss
		MISCONFIGURED	The overall configuration of the ring across all involved units is incorrect
	OID	1.3.6.1.4.1.3181.10.6.2.45.100.1.2 (statusState)	
last_state_change	Time and date string indication when the state of the ring protocol has last changed to the state now indicated.		
	Value	String, max. 32 characters.	
	OID	1.3.6.1.4.1.3181.10.6.2.45.100.1.3 (statusLastStateChange)	
ring_interrupt	Values	true, false	
	OID	1.3.6.1.4.1.3181.10.6.2.45.100.1.4 (statusRingInterrupt)	
global_ring_alarm	Values	true, false	
	OID	1.3.6.1.4.1.3181.10.6.2.45.100.1.5 (statusGlobalRingAlarm)	
error_detected	Values	true, false	
	OID	1.3.6.1.4.1.3181.10.6.2.45.100.1.6 (statusErrorDetected)	
ring_port_a_interrupted	Values	true, false	
	OID	1.3.6.1.4.1.3181.10.6.2.45.100.1.7 (statusRingPortAInterrupted)	

ring_port_b_interrupted

Values true, false
OID 1.3.6.1.4.1.3181.10.6.2.45.100.1.8
(statusRingPortBInterrupted)

Group	statistics , for all ring indices [1..2]
Path	Protocol.Ring.statistics[index]
Description	Statistics of the ring network performance.

number_of_backups Counts the number of backups engaged since the last power up.

Value Number in range 0-0xFFFFFFFF
OID 1.3.6.1.4.1.3181.10.6.2.45.101.1.2
(statisticsNumberOfBackups)

current_backup_duration Indicates since how long a currently active backup is established. When no backup is active a 0 is displayed.

Value PERIOD0-0xFFFFFFFF
OID 1.3.6.1.4.1.3181.10.6.2.45.101.1.3
(statisticsCurrentBackupDuration)

last_backup_duration Indicates since how long the last backup was established. Indicates 0 if there was no backup since last reboot.

Value PERIOD0-0xFFFFFFFF
OID 1.3.6.1.4.1.3181.10.6.2.45.101.1.4
(statisticsLastBackupDuration)

total_backup_duration Total time the ring was in backup since last reboot.

Value PERIOD0-0xFFFFFFFF
OID 1.3.6.1.4.1.3181.10.6.2.45.101.1.5
(statisticsTotalBackupDuration)

Group	coupling_status
Path	Protocol.Ring.coupling_status
Description	Indicates status of ring coupling function.

controller_state	Data transmission state. ATTENTION: Not implemented. Values <i>DISABLED</i> <i>BLOCKING</i> <i>LINK</i> <i>FORWARDING</i> <i>STANDBY</i> OID 1.3.6.1.4.1.3181.10.6.2.45.102.1.2 (couplingStatusControllerState)
cport_link	Coupling port is in linkup condition. ATTENTION: Not implemented. Values true, false OID 1.3.6.1.4.1.3181.10.6.2.45.102.1.3 (couplingStatusCportLink)
cport_forward	Coupling port is in forwarding state. ATTENTION: Not implemented. Values true, false OID 1.3.6.1.4.1.3181.10.6.2.45.102.1.4 (couplingStatusCportForward)
cport_timeout	Indicates that no ring coupling frames were received within defined period. ATTENTION: Not implemented. Values true, false OID 1.3.6.1.4.1.3181.10.6.2.45.102.1.5 (couplingStatusCportTimeout)
connection_valid	Indicates that source ip address of received frame matches configured partner ip. ATTENTION: Not implemented. Values true, false OID 1.3.6.1.4.1.3181.10.6.2.45.102.1.6 (couplingStatusConnectionValid)
valid_partner_ip	Indicates that received ring number matches expected locally configured ring number. ATTENTION: Not implemented. Values true, false OID 1.3.6.1.4.1.3181.10.6.2.45.102.1.7 (couplingStatusValidPartnerIp)
valid_partner_id	ATTENTION: Not implemented. Values true, false OID 1.3.6.1.4.1.3181.10.6.2.45.102.1.8 (couplingStatusValidPartnerId)

Group Path Description	mrp_status Protocol.Ring.mrp_status Status common to manager and client
operation	<p>Indicates if MRP function is enabled. ATTENTION: Not implemented.</p> <p>Values <i>DISABLED</i> MRP is disabled <i>ENABLED</i> MRP is enabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.103.1.2 (mrpStatusOperation)</p>
admin_role	<p>Mirrors expected role configuration. ATTENTION: Not implemented.</p> <p>Values <i>DISABLED</i> MRP is disabled <i>CLIENT</i> Client (slave) mode <i>MANAGER</i> Manager (master) node</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.103.1.3 (mrpStatusAdminRole) 1.0.62439.1.1.1.4 (mrpDomainAdminRole)</p>
operational_role	<p>real_role ?? ATTENTION: Not implemented.</p> <p>Values <i>DISABLED</i> MRP is disabled <i>CLIENT</i> Client (slave) mode <i>MANAGER</i> Manager (master) node</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.103.1.4 (mrpStatusOperationalRole) 1.0.62439.1.1.1.5 (mrpDomainOperRole)</p>
port_1_state	<p>ATTENTION: Not implemented.</p> <p>Values <i>UNUSED</i> MRP is disabled <i>BLOCKING</i> Port is blocked. No communication. Ethernet LED indicates yellow. <i>FORWARDING</i> Port is forwarding data <i>NOT_CONNECTED</i> Port is not connected to network</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.103.1.5 (mrpStatusPort1State) 1.0.62439.1.1.1.7 (mrpDomainRingPort1State)</p>
port_2_state	<p>ATTENTION: Not implemented.</p> <p>Values <i>UNUSED</i> MRP is disabled <i>BLOCKING</i> Port is blocked. No communication. Ethernet LED indicates yellow. <i>FORWARDING</i> Port is forwarding data <i>NOT_CONNECTED</i> Port is not connected to network</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.103.1.6 (mrpStatusPort2State) 1.0.62439.1.1.1.9 (mrpDomainRingPort2State)</p>

domain_id	When left blank the default id of all bits 1 is used. ATTENTION: Not implemented.
Value	String, max. 65 characters.
OID	1.3.6.1.4.1.3181.10.6.2.45.103.1.7 (mrpStatusDomainId) 1.0.62439.1.1.1.2 (mrpDomainID)

domain_error	ATTENTION: Not implemented.														
Values	<table> <tr> <td><i>DISABLED</i></td><td>MRP is disabled</td></tr> <tr> <td><i>NO_ERROR</i></td><td>MRP is running and redundancy is available</td></tr> <tr> <td><i>INVALID_VLAN</i></td><td>The configured VLAN is not permitted</td></tr> <tr> <td><i>INVALID</i></td><td>General error code</td></tr> <tr> <td><i>MULTI_MGR</i></td><td>Multiple managers in the ring</td></tr> <tr> <td><i>SINGLE_SIDE</i></td><td>Test frames only received on one port</td></tr> <tr> <td><i>LINK_ERROR</i></td><td>Link error</td></tr> </table>	<i>DISABLED</i>	MRP is disabled	<i>NO_ERROR</i>	MRP is running and redundancy is available	<i>INVALID_VLAN</i>	The configured VLAN is not permitted	<i>INVALID</i>	General error code	<i>MULTI_MGR</i>	Multiple managers in the ring	<i>SINGLE_SIDE</i>	Test frames only received on one port	<i>LINK_ERROR</i>	Link error
<i>DISABLED</i>	MRP is disabled														
<i>NO_ERROR</i>	MRP is running and redundancy is available														
<i>INVALID_VLAN</i>	The configured VLAN is not permitted														
<i>INVALID</i>	General error code														
<i>MULTI_MGR</i>	Multiple managers in the ring														
<i>SINGLE_SIDE</i>	Test frames only received on one port														
<i>LINK_ERROR</i>	Link error														
OID	1.3.6.1.4.1.3181.10.6.2.45.103.1.8 (mrpStatusDomainError) 1.0.62439.1.1.1.11 (mrpDomainError)														

Group	mrp_manager_status
Path	Protocol.Ring.mrp_manager_status
Description	Status that applies to manager only. Invalid when in client mode.

ring_state	Indicates if MRP is enabled on this device. ATTENTION: Not implemented.								
Values	<table> <tr> <td><i>DISABLED</i></td><td>MRP is disabled</td></tr> <tr> <td><i>RING_CLOSED</i></td><td>MRP is running and redundancy is available</td></tr> <tr> <td><i>RING_OPEN</i></td><td>Ring open. No redundancy at this time</td></tr> <tr> <td><i>UNDEFINED</i></td><td>Undefined protocol state</td></tr> </table>	<i>DISABLED</i>	MRP is disabled	<i>RING_CLOSED</i>	MRP is running and redundancy is available	<i>RING_OPEN</i>	Ring open. No redundancy at this time	<i>UNDEFINED</i>	Undefined protocol state
<i>DISABLED</i>	MRP is disabled								
<i>RING_CLOSED</i>	MRP is running and redundancy is available								
<i>RING_OPEN</i>	Ring open. No redundancy at this time								
<i>UNDEFINED</i>	Undefined protocol state								
OID	1.3.6.1.4.1.3181.10.6.2.45.104.1.2 (mrpManagerStatusRingState) 1.0.62439.1.1.1.10 (mrpDomainState)								

manager_priority	The priority of this MRP entity. ATTENTION: Not implemented.
Value	Number in range 0-0xFFFFFFFF
OID	1.3.6.1.4.1.3181.10.6.2.45.104.1.3 (mrpManagerStatusManagerPriority) 1.0.62439.1.1.1.14 (mrpDomainManagerPriority)

ring_open_count	<p>Counts how many times was the ring broken. ATTENTION: Not implemented.</p> <p>Value Number in range 0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.104.1.4 (mrpManagerStatusRingOpenCount) 1.0.62439.1.1.1.15 (mrpDomainRingOpenCount)</p>
time_since_last_ring_open	<p>Seconds since the ring was last opened. ATTENTION: Not implemented.</p> <p>Value PERIOD0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.104.1.5 (mrpManagerStatusTimeSinceLastRingOpen) 1.0.62439.1.1.1.16 (mrpDomainLastRingOpenChange)</p>
max_round_trip_delay	<p>The longest round trip delay that was measured since value reset. Value in microseconds ATTENTION: Not implemented.</p> <p>Value Number in range 0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.104.1.6 (mrpManagerStatusMaxRoundTripDelay) 1.0.62439.1.1.1.17 (mrpDomainRoundTripDelayMax)</p>
min_round_trip_delay	<p>The shortest round trip delay that was measured since value reset. Value in microseconds ATTENTION: Not implemented.</p> <p>Value Number in range 0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.104.1.7 (mrpManagerStatusMinRoundTripDelay) 1.0.62439.1.1.1.18 (mrpDomainRoundTripDelayMin)</p>
topology_change_interval	<p>Interval for sending of MRP_TopologyChange messages ATTENTION: Not implemented.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.104.1.8 (mrpManagerStatusTopologyChangeInterval)</p>
topo_change_repeat_count	<p>Topology change repeat count for repeated transmission of MRP_TopologyChange messages ATTENTION: Not implemented.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.104.1.9 (mrpManagerStatusTopoChangeRepeatCount)</p>
short_test_interval	<p>Short interval for sending of MRP_Test messages after link changes on the ring ATTENTION: Not implemented.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.104.1.10 (mrpManagerStatusShortTestInterval)</p>

default_test_interval	<p>Default interval for sending of MRP_Test messages on the ring ATTENTION: Not implemented.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.104.1.11 (mrpManagerStatusDefaultTestInterval)</p>
test_monitor_count	<p>Count for monitoring the reception of MRP_Test messages ATTENTION: Not implemented.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.104.1.12 (mrpManagerStatusTestMonitorCount)</p>
test_monitor_ext_count	<p>The extended interval count for monitoring the reception of MRP_Test messages ATTENTION: Not implemented.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.104.1.13 (mrpManagerStatusTestMonitorExtCount)</p>
nonblocking_support	<p>False indicates that the manager requires ring clients that support port blocking. This is standard behavior of any modern switch. ATTENTION: Not implemented.</p> <p>Values true, false</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.104.1.14 (mrpManagerStatusNonblockingSupport)</p>

Group	mrp_client_status
Path	Protocol.Ring.mrp_client_status
Description	Status that applies to client only. Invalid when in manager mode.
link_down_timer	<p>The interval for sending of MRP_linkDown messages ATTENTION: Not implemented.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.105.1.2 (mrpClientStatusLinkDownTimer)</p>
link_up_timer	<p>The interval for sending of MRP_linkUp messages ATTENTION: Not implemented.</p> <p>Value Number in range 0-65535</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.45.105.1.3 (mrpClientStatusLinkUpTimer)</p>

link_change_count	The count for repeated transmission of MRP_LinkChange messages ATTENTION: Not implemented.
Value	Number in range 0-65535
OID	1.3.6.1.4.1.3181.10.6.2.45.105.1.4 (mrpClientStatusLinkChangeCount)

blocked_support	True indicates that this client supports port blocking. The value is always true. ATTENTION: Not implemented.
Values	true, false
OID	1.3.6.1.4.1.3181.10.6.2.45.105.1.5 (mrpClientStatusBlockedSupport) 1.0.62439.1.1.1.12 (mrpDomainBlocked)

35 Message Queue Telemetry Transport (MQTT)

35.1 Key Features

Auto publish actor, sensor and GUI data

Any changes to sensor or actor data of the entire SmartOffice system can automatically be published. Likewise, any GUI activity can be published. Features can be enabled individually.

This enables other systems to track SmartOffice activities in a very convenient way.

Auto subscribe actor, sensor and GUI data

Any sensor or actor data of the entire SmartOffice system can automatically be accessed. Likewise, the GUI can be remote controlled. Features can be enabled individually.

This enables other systems to remote control the SmartOffice System. It also permit for automatic sensor creation to incorporate foreign data.

Topic Map

MQTT data from other systems can be subscribed to and are automatically mapped to local SmartOffice sensors. Similarly, individual actor group changes can be published to control remote devices.

While auto publish provides a simple and generic way to interconnect with others, the topic map provides a detailed precise way to do so, while keeping other data obscure.

Configuration via MQTT

MQTT may be used to access any configuration parameter. Read and write access is supported. For security the feature can be switched off or limited to read only. In addition user access rights of command level can be applied.

Configuration access via MQTT is a further step to permit full control of the system via MQTT.

Script Execution via MQTT

MicroScripts that already reside on the system can be executed via MQTT. Topic payload and extra topic elements are forwarded to the Script as parameters. The permitted scripts can precisely be defined.

Running a script via MQTT offers a flexible way to adapt a foreign system.

Local broker

Typically, a third party broker is accessed to transfer information. When such a broker is not available, a local broker can be provided.

In smaller application the embedded broker can suffice and may be used as the third party broker for other devices, saving cost for an extra device.

Data Transformation

Often data are not available in a compatible format among several devices of different vendors. Transformation rules permit on-the-fly transformation and calculations to achieve uniform data representation.

Ensure data uniformity across vendors and interfaces.

35.2 Functional Description

Preface

Message Queue Telemetry Transport (MQTT) is a recent protocol specially designed for the Internet of Things (IoT). In MQTT all data are referenced using topics. These look like directories.

For example: *'Frankfurt/MyBuilding/ground floor/room 1/lighting/desktop'*

The G6 fully supports MQTT being able to publish all SmartOffice functions and to subscribe to any kind of topic with translation to internal representation. Additionally, a broker (Server) is included to and from which other devices can connect.

Function

Small sensor devices can send updates of their values to a central broker. The broker (server) keeps a record of all received messages. Other systems can register with the broker to receive updates of certain topics. In this way there is no direct connection between the end devices. The G6 can be setup to publish precisely defined objects (and hide all others) or may be setup to publish any changes to actors, sensors or groups. Additionally, any operation on the SmartOffice GUI (web page) can be forwarded. In this way the GUI could be used to control a completely separate device.

The G6 may also subscribe to topics from other devices. Since the topic structure is only loosely defined, a look up table is used to map topics to internal sensors. Once the sensor is defined, it can be used in the SmartOffice context, just like any other sensor data. The G6 may connect to any MQTT broker or use the local broker. Which scenario is better suited depends on the overall network design.

Security

Reliability is ensured by supported by allowing all three defined quality of service levels. Security is fully supported by optional AES256 encryption including the use of certificates. The internal broker supports username controlled topic access control lists.

For simple applications, or for easier testing, security features can be switched off.

Topics

In MQTT all data are referenced using topics. When G6 is publishing it needs to create topics. This is done by combining a configurable prefix followed by the scheme *'prefix/device/instance/attribute'* for actors or sensors. For actor- or sensor groups the logic *'prefix/groupname/attribute'* is used.

To permit the deployment of several G6 devices in a SmartOffice network, while using the same configuration in each device, it is possible to use variables in the topic prefix.

Variables

These are:

Variable	Inserts
{SMO}	'SmartOffice' text
{MFG}	the manufacturer name (MICROSENS)
{MAC}	the MAC address of this device (using ':' separators)
{IP4}	the IPv4 address of this device
{IP6}	the first IPv6 address of this device (if IP V6 is enabled)
{DMN}	' <i>smartoffice.director_config.domain_name</i> '
{ART}	the article number of this device
{SER}	the serial number of this device
{LOC}	the SNMP SysLocation value
{NAM}	the SNMP SysName value

Several variables may be used in one topic like: {SMO}/{MFG}_{MAC}

This parameter expansion is available for:

- MQTT.publisher_config_topic_prefix
- MQTT.broker_access.client_id
- MQTT.topic_map.topic

Topic Wildcards

In MQTT it is possible to listen to any topic by using the wildcard '+' to do not care for a certain level such as 'floor/+/temperature' to listen to the temperature in any room of this floor.

In the G6 this wildcard is NOT supported!

The wildcard may be specified to receive all elements from the server, but in the subsequent comparison using the topic_map to map to a particular internal sensor it does not make sense anymore. If let's say 5 rooms could publish data of interest, 5 distinct entries must be made.

Tip!

When setting up the configuration the precise topics to subscribe to may be unclear. In this situation it could be useful to use MQTT wildcards in the mapping table AND enable MQTT tracing 'MQTT.broker_access.trace_mode = Enabled'.

This will display all incoming topics that match the wildcard. There will, however, be no update of any sensor. The display may be used to discover the exact topic to enter.

microScript

In general MQTT integrates into the SmartOffice system through actor and sensor emulation. This is detailed in this chapter. It may, however, also be useful to use MQTT under program control.

Through microScript it is also possible to publish and subscribe to topics. Subscribing via script has the advantage that wildcards may be used to receive an undetermined number of topics as compared to the straight 1:1 mapping of topic to sensor available via configuration. Configured and scripted MQTT operation may be used in parallel.

Further details about the microScript solution are available in a separate handbook.

35.3 MQTT CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Protocol.	mqtt.					MQTT Internet of Things protocol.
			enable_mqtt		R/W	Master enable for all MQTT related functions.
			help_topic_variables		X	Displays useful information about topic expansion using curly brackets. Note that help is only displayed when MQTT is generally enabled.
	publisher_config.					This section defines outgoing messages published by this system to the outside world.
			enable_publishing		R/W	Master enable for publishing function. When enabled outgoing MQTT messages indicating the changes according to the selected smart office elements will be generated.
			topic_prefix		R/W	This prefix is prepended to all outgoing topics. Any valid string may be used. Trailing slash is optional. Any number of levels may be specified. The system will append in the following logic: prefix/device/instance/attribute for individual actor/sensors and in this format for groups: prefix/groupname/attribute or prefix/gui/gui_element. Topic variable expansion is available. Additional information available with mqtt.help_topic_variables command. Variables may be used like location/{MAC}/subtopic.
			quality_of_service		R/W	This defines the QoS with which the publish_all.. elements are published. Actors published through the topic_map use their own local QoS setting.
			publish_all_actorgroups		R/W	When enabled any changes to any actor_group are reported.
			publish_all_sensorgroups		R/W	When enabled any changes to any sensor_group are reported.
			publish_all_actors		R/W	When enabled any changes to any actor are reported. This can create a significant amount of traffic. Usually it is preferred to only publish actorgroup changes.

publish_all_sensors	R/W	When enabled any changes from any sensor are reported. This can create a significant amount of traffic. Usually it is preferred to only publish sensorgroup changes.
publish_gui_elements	R/W	When enabled any GUI activity of elements for which the parameter remote_accessible is enabled is reported. NOTE: For now the remote_accessible is ignored and all activities are reported.
subscriber_config.		This section defines reaction to incoming messages not defined in the topic map.
enable_subscription	R/W	Master enable for subscription function. When enabled incoming MQTT messages matching the following topics will be accepted. This is independent from specific definitions defined by the topic map. It is intended when the system is generally MQTT controlled to avoid the requirement for a very large topic map.
match_topic_prefix	R/W	When a topic starting with the defined prefix is received, then the next keyword is used to select actor, actorgroup, sensor or gui. For additional syntax check the individual subscription enable text. The wildcard + is permitted in the match topic. Topic variable expansion is available. Additional information available with mqtt.help_topic_variables command. Variables may be used like location/{MAC}/subtopic.
quality_of_service	R/W	This QoS defines with which level the match_topic is subscribed.
subscribe_all_actorgroups	R/W	When enabled actor groups can be set via MQTT. Format: match_topic_prefix/actorgroup/groupname (using default priority 10) or match_topic_prefix/actorgroup/groupname/attribute/priority. Only use priority format if fully understood. Send empty double quotes to release a priority level. 1 is highest, 32 lowest priority. Standard is 10.
subscribe_all_actors	R/W	When enabled individual actors can be set via MQTT provided they are not part of any actor group. Format: match_topic_prefix/actor/device/instance/attribute.
permit_actor_creation	R/W	When enabled, incoming actor_topics that specify an actor that does not already exist in the system will automatically be created. This simplifies adding new external data sources but also implies the danger that too many actors (due to incorrect or rouge data) could be created filling up the actor table.

subscribe_gui_elements	R/W	When enabled individual gui elements can be set via MQTT. A possible associated script as defined in the gui configuration is executed as well. Format: match_topic_prefix/gui/gui_element/instance/attribute.
subscribe_all_sensors	R/W	When enabled any sensor value can be set via MQTT. Format: match_topic_prefix/sensor/device/instance/attribute.
permit_sensor_creation	R/W	When enabled, incoming sensor_topics that specify a sensor that does not already exist in the system will automatically be created. This simplifies adding new external data sources but also implies the danger that too many sensors (due to incorrect or rouge data) could be created filling up the sensor table.
limit_to_mqtt_sensors	R/W	When enabled, only sensor that were initially created by MQTT can be set. This way MQTT cannot be (mis)used to overwrite the values of other sensors.
event_command_access	R/W	When enabled, internal system events used to register SmartOffice elements are exposed. This permits, for example, fully integrated device drivers via MQTT.
run_script_access	R/W	When enabled, scripts can be run via MQTT. The script must already reside on the system. Command line parameter can be used via topic or payload. The script access rights are governed by the mqtt_cfg_username.
permitted_scripts	R/W	When run_script_access is enabled, this field can be used to limit the available scripts to protect the system. Wildcards can be used. Enter * to permit any script. When subroutines are used, follow the script name with * to permit all subroutines of file. The more precise the name, the more secure. Also observe possible app names prepended to the script name.
configuration_access	R/W	Depending on the setting it is possible to see and/or modify the configuration of the system via MQTT. This is very powerful but also potentially dangerous. Therefore, this option should be used with care. Observe the associated parameter mqtt_cfg_username. This must also be configured to define which access restrictions apply.
mqtt_cfg_username	R/W	The access restrictions defined for the selected user also apply for access via MQTT. When no username or an invalid user name is configured, MQTT configuration access is blocked.

topic_map[DYNAMIC].		This table is used to map topics to local names that fit into the SmartOffice naming scheme. At this time no wildcards are permitted. This table permits publishing of individual actors, rather than publishing all. Also this table is used to receive well defined topic and make them internally available as sensors.
name	R/W	Unique name to reference this entry and to remember its functionality.
mode	R/W	Defines whether the topic is subscribed to and mapped to local name or if an existing local name is published. The entry may be disabled to turn off all activity without losing the mapping information.
topic	R/W	Unique name of the element. {xxx} expansion as shown in mqtt.help_topic_variables command may be used here. Wildcards + or # cannot be used.
local_name	R/W	This defines the sensor list entry that is generated and linked to this topic for subscribed mode. In publish mode the name of an existing actor or a new virtual actor is required. In both cases the name must be in the format: device:instance:attribute. Example: mqtt:1:temperature. Alternative a persistent variable can be assigned starting with \$.
transformation	R/W	May be used to transform the value between external and internal format. Syntax: text=value,text=value or value=text or text=other_text,.. Or calculations: =\$*10 Example C to F: =(\$*1.8)+32
quality_of_service	R/W	This QoS defines with which level the subscriber subscribes or with which QoS is published.
broker_access.		This section defines all connectivity and security aspects between this system and the MQTT broker. This applies regardless of the fact that a local or remote broker is used.
broker_address	R/W	IP address or symbolic name of the MQTT broker. When empty the local broker is used.

client_id	R/W	The client id is used by the broker to verify permissions to access topics. An empty field will use a random id which will only allow access to unprotected brokers. The expanded client id can be up to 127 characters but may be cut off after 23 characters by the broker according to MQTT 3.1 protocol specification. Topic expansion as shown with <code>mqtt.help_topic_variables</code> command applies.
security_mode	R/W	Define the security method to apply for all messages.
username	R/W	The username is optional and will be added to outgoing messages if set.
enter_password	X	Set a password for the user. No spaces are permitted.
encrypted_password	R/W	This holds the encrypted password. Do not modify.
keep_alive_timer	R/W	The system will periodically send keep alive messages when the value is not 0. The time is specified in seconds.
trace_mode	R/W	For testing a trace mode may be enabled that displays MQTT activity to the console for trouble shooting.
local_broker_config.		This section only applies if this system should also provide the broker. It may be accessed by remote and local clients.
enable_local_broker	R/W	Run a local MQTT broker on port 1883. Also websocket on port 9001 is available.
permit_anonymous	R/W	Permit access without any username. This should be used for initial testing only!
permit_crypted_sockets	R/W	Permit access using encrypted websockets on port 8081.
permit_encrypted_ssl	R/W	Permit access using encrypted SSL on port 8883.
permit_certified_ssl	R/W	Permit access using encrypted SSL with certificate on port 8884.
certificate_name	R/W	The certificate itself is loaded via <code>Management.Files.certification</code> commands.
local_broker_user[DYNAMIC].		Define user/password pairs to protect access to the broker. The username can further be used to restrict access to certain topics.
username	R/W	Define a username to protect access to the broker. Must be 3 character at least.
enter_password	X	Set a password for the user. No spaces are permitted.
encrypted_password	R/W	This holds the encrypted password. Do not modify.

permitted_topic	R/W	Wildcards as per MQTT are permitted here. Use # for the remainder of the topic and /+/ to create a wildcard for a section. At this time only one topic is configurable. Use the pattern table for more granularity.
topic_access	R/W	Define the allowed access method of the permitted topic.
local_broker_acl[DYNAMIC].		Define user/password pairs to protect access to the broker. The username can further be used to restrict access to certain topics.
name	R/W	Unique name to reference this entry and to remember its function.
permitted_topic	R/W	Wildcards as per MQTT are permitted here. In addition the terms /%c/ may be used to specify the current client_id and /%u/ can be used to specify current user. Use # for the remainder of the topic and /+/ to create a wildcard for a section.
topic_access	R/W	Define the allowed access method of the permitted topic.

35.4 MQTT Configuration Parameters

Group	General Parameters	
Path	Protocol.MQTT	
enable_mqtt	Master enable for all MQTT related functions.	
	Values	enabled, disabled
	OID	1.3.6.1.4.1.3181.10.6.2.110.1 (mqttEnableMqtt)
help_topic_variables	Displays useful information about topic expansion using curly brackets. Note that help is only displayed when MQTT is generally enabled.	
	Action	Execute command.
	OID	1.3.6.1.4.1.3181.10.6.2.110.2 (mqttHelpTopicVariables)
Group	topic_map , dynamical size	
Path	Protocol.MQTT.topic_map	
Description	This table is used to map topics to local names that fit into the SmartOffice naming scheme. At this time no wildcards are permitted. This table permits publishing of individual actors, rather than publishing all. Also this table is used to receive well defined topic and make them internally available as sensors.	
name	Unique name to reference this entry and to remember its functionality.	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.110.5.1.2 (topicMapName)
mode	Defines whether the topic is subscribed to and mapped to local name or if an existing local name is published. The entry may be disabled to turn off all activity without losing the mapping information.	
	Values	<i>DISABLED</i> This entry is ignored <i>SUBSCRIBE</i> The topic is subscribed too (received) <i>PUBLISH</i> The topic is published (send)
	OID	1.3.6.1.4.1.3181.10.6.2.110.5.1.3 (topicMapMode)
topic	Unique name of the element. {xxx} expansion as shown in mqtt.help_topic_variables command may be used here. Wildcards + or # cannot be used.	
	Value	String, max. 128 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.110.5.1.4 (topicMapTopic)

local_name	<p>This defines the sensor list entry that is generated and linked to this topic for subscribed mode. In publish mode the name of an existing actor or a new virtual actor is required. In both cases the name must be in the format: device:instance:attribute. Example: mqtt:1:temperature. Alternative a persistent variable can be assigned starting with \$.</p> <p>Value String, max. 64 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.5.1.5 (topicMapLocalName)</p>
transformation	<p>May be used to transform the value between external and internal format. Syntax: text=value,text=value or value=text or text=other_text,.. Or calculations: =\$*10 Example C to F: =(\$*1.8)+32</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.5.1.6 (topicMapTransformation)</p>
quality_of_service	<p>This QoS defines with which level the subscriber subscribes or with which QoS is published.</p> <p>Values <i>AT_MOST_ONCE</i> Unacknowledged transfer <i>AT_LEAST_ONCE</i> Acknowledged transfer <i>EXACTLY_ONCE</i> Acknowledged transfer. Safest but slowest.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.5.1.7 (topicMapQualityOfService)</p>
Group Path Description	<p>local_broker_user, dynamical size</p> <p>Protocol.MQTT.local_broker_user</p> <p>Define user/password pairs to protect access to the broker. The username can further be used to restrict access to certain topics.</p>
username	<p>Define a username to protect access to the broker. Must be 3 character at least. ATTENTION: Not implemented.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.8.1.2 (localBrokerUserUsername)</p>
enter_password	<p>Set a password for the user. No spaces are permitted.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.8.1.3 (localBrokerUserEnterPassword)</p>
encrypted_password	<p>This holds the encrypted password. Do not modify.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.8.1.4 (localBrokerUserEncryptedPassword)</p>

permitted_topic	Wildcards as per MQTT are permitted here. Use # for the remainder of the topic and /+/ to create a wildcard for a section. At this time only one topic is configurable. Use the pattern table for more granularity. Value String, max. 128 characters. OID 1.3.6.1.4.1.3181.10.6.2.110.8.1.5 (localBrokerUserPermittedTopic)
topic_access	Define the allowed access method of the permitted topic. Values <i>SUBSCRIBE</i> The topic may be subscribed too <i>PUBLISH</i> The topic may be published <i>FULL</i> The topic may be read and written OID 1.3.6.1.4.1.3181.10.6.2.110.8.1.6 (localBrokerUserTopicAccess)
Group Path Description	local_broker_acl , dynamical size Protocol.MQTT.local_broker_acl Define user/password pairs to protect access to the broker. The username can further be used to restrict access to certain topics.
name	Unique name to reference this entry and to remember its function. ATTENTION: Not implemented. Value String, max. 32 characters. OID 1.3.6.1.4.1.3181.10.6.2.110.9.1.2 (localBrokerAcIName)
permitted_topic	Wildcards as per MQTT are permitted here. In addition the terms /%c/ may be used to specify the current client_id and /%u/ can be used to specify current user. Use # for the remainder of the topic and /+/ to create a wildcard for a section. Value String, max. 128 characters. OID 1.3.6.1.4.1.3181.10.6.2.110.9.1.3 (localBrokerAcIPermittedTopic)
topic_access	Define the allowed access method of the permitted topic. Values <i>SUBSCRIBE</i> The topic may be subscribed too <i>PUBLISH</i> The topic may be published <i>FULL</i> The topic may be read and written OID 1.3.6.1.4.1.3181.10.6.2.110.9.1.4 (localBrokerAcITopicAccess)

Group Path Description	publisher_config Protocol.MQTT.publisher_config This section defines outgoing messages published by this system to the outside world.
enable_publishing	<p>Master enable for publishing function. When enabled outgoing MQTT messages indicating the changes according to the selected smart office elements will be generated.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.3.1.2 (publisherConfigEnablePublishing)</p>
topic_prefix	<p>This prefix is prepended to all outgoing topics. Any valid string may be used. Trailing slash is optional. Any number of levels may be specified. The system will append in the following logic: prefix/device/instance/attribute for individual actor/sensors and in this format for groups: prefix/groupname/attribute or prefix/gui/gui_element. Topic variable expansion is available. Additional information available with mqtt.help_topic_variables command. Variables may be used like location/{MAC}/subtopic.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.3.1.3 (publisherConfigTopicPrefix)</p>
quality_of_service	<p>This defines the QoS with which the publish_all.. elements are published. Actors published through the topic_map use their own local QoS setting.</p> <p>Values <i>AT_MOST_ONCE</i> Unacknowledged transfer <i>AT_LEAST_ONCE</i> Acknowledged transfer <i>EXACTLY_ONCE</i> Acknowledged transfer. Safest but slowest.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.3.1.4 (publisherConfigQualityOfService)</p>
publish_all_actorgroups	<p>When enabled any changes to any actor_group are reported.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.3.1.5 (publisherConfigPublishAllActorgroups)</p>
publish_all_sensorgroups	<p>When enabled any changes to any sensor_group are reported.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.3.1.6 (publisherConfigPublishAllSensorgroups)</p>
publish_all_actors	<p>When enabled any changes to any actor are reported. This can create a significant amount of traffic. Usually it is preferred to only publish actorgroup changes.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.3.1.7 (publisherConfigPublishAllActors)</p>

publish_all_sensors	<p>When enabled any changes from any sensor are reported. This can create a significant amount of traffic. Usually it is preferred to only publish sensorgroup changes.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.3.1.8 (publisherConfigPublishAllSensors)</p>
publish_gui_elements	<p>When enabled any GUI activity of elements for which the parameter remote_accessible is enabled is reported. NOTE: For now the remote_accessible is ignored and all activities are reported.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.3.1.9 (publisherConfigPublishGuiElements)</p>
Group	subscriber_config
Path	Protocol.MQTT.subscriber_config
Description	This section defines reaction to incoming messages not defined in the topic map.
enable_subscription	<p>Master enable for subscription function. When enabled incoming MQTT messages matching the following topics will be accepted. This is independent from specific definitions defined by the topic map. It is intended when the system is generally MQTT controlled to avoid the requirement for a very large topic map.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.4.1.2 (subscriberConfigEnableSubscription)</p>
match_topic_prefix	<p>When a topic starting with the defined prefix is received, then the next keyword is used to select actor, actorgroup, sensor or gui. For additional syntax check the individual subscription enable text. The wildcard + is permitted in the match topic. Topic variable expansion is available. Additional information available with mqtt.help_topic_variables command. Variables may be used like location/{MAC}/subtopic.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.4.1.3 (subscriberConfigMatchTopicPrefix)</p>
quality_of_service	<p>This QoS defines with which level the match_topic is subscribed.</p> <p>Values <i>AT_MOST_ONCE</i> Unacknowledged transfer <i>AT_LEAST_ONCE</i> Acknowledged transfer <i>EXACTLY_ONCE</i> Acknowledged transfer. Safest but slowest.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.4.1.4 (subscriberConfigQualityOfService)</p>

subscribe_all_actorgroups	<p>When enabled actor groups can be set via MQTT. Format: match_topic_prefix/actorgroup/groupname (using default priority 10) or match_topic_prefix/actorgroup/groupname/attribute/priority. Only use priority format if fully understood. Send empty double quotes to release a priority level. 1 is highest, 32 lowest priority. Standard is 10.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.4.1.5 (subscriberConfigSubscribeAllActorgroups)</p>
subscribe_all_actors	<p>When enabled individual actors can be set via MQTT provided they are not part of any actor group. Format: match_topic_prefix/actor/device/instance/attribute.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.4.1.6 (subscriberConfigSubscribeAllActors)</p>
permit_actor_creation	<p>When enabled, incoming actor_topics that specify an actor that does not already exist in the system will automatically be created. This simplifies adding new external data sources but also implies the danger that to many actors (due to incorrect or rouge data) could be created filling up the actor table.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.4.1.7 (subscriberConfigPermitActorCreation)</p>
subscribe_gui_elements	<p>When enabled individual gui elements can be set via MQTT. A possible associated script as defined in the gui configuration is executed as well. Format: match_topic_prefix/gui/gui_element/instance/attribute.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.4.1.8 (subscriberConfigSubscribeGuiElements)</p>
subscribe_all_sensors	<p>When enabled any sensor value can be set via MQTT. Format: match_topic_prefix/sensor/device/instance/attribute.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.4.1.9 (subscriberConfigSubscribeAllSensors)</p>
permit_sensor_creation	<p>When enabled, incoming sensor_topics that specify a sensor that does not already exist in the system will automatically be created. This simplifies adding new external data sources but also implies the danger that to many sensors (due to incorrect or rouge data) could be created filling up the sensor table.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.4.1.10 (subscriberConfigPermitSensorCreation)</p>

limit_to_mqtt_sensors	<p>When enabled, only sensor that were initially created by MQTT can be set. This way MQTT cannot be (mis)used to overwrite the values of other sensors.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.4.1.11 (subscriberConfigLimitToMqttSensors)</p>
event_command_access	<p>When enabled, internal system events used to register SmartOffice elements are exposed. This permits, for example, fully integrated device drivers via MQTT.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.4.1.12 (subscriberConfigEventCommandAccess)</p>
run_script_access	<p>When enabled, scripts can be run via MQTT. The script must already reside on the system. Command line parameter can be used via topic or payload. The script access rights are governed by the mqtt_cfg_username.</p> <p>Values enabled, disabled</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.4.1.13 (subscriberConfigRunScriptAccess)</p>
permitted_scripts	<p>When run_script_access is enabled, this field can be used to limit the available scripts to protect the system. Wildcards can be used. Enter * to permit any script. When subroutines are used, follow the script name with * to permit all subroutines of file. The more precise the name, the more secure. Also observe possible app names prepended to the script name.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.4.1.14 (subscriberConfigPermittedScripts)</p>
configuration_access	<p>Depending on the setting it is possible to see and/or modify the configuration of the system via MQTT. This is very powerful but also potentially dangerous. Therefore, this option should be used with care. Observe the associated parameter mqtt_cfg_username. This must also be configured to define which access restrictions apply.</p> <p>Values <i>DISABLED</i> No configuration access via MQTT <i>READ_ONLY</i> Configuration and status is read only via MQTT <i>READ_WRITE</i> Full access to configuration and status</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.4.1.15 (subscriberConfigConfigurationAccess)</p>
mqtt_cfg_username	<p>The access restrictions defined for the selected user also apply for access via MQTT. When no username or an invalid user name is configured, MQTT configuration access is blocked.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.4.1.16 (subscriberConfigMqttCfgUsername)</p>

Group	broker_access
Path	Protocol.MQTT.broker_access
Description	This section defines all connectivity and security aspects between this system and the MQTT broker. This applies regardless of the fact that a local or remote broker is used.
broker_address	<p>IP address or symbolic name of the MQTT broker. When empty the local broker is used.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.6.1.2 (brokerAccessBrokerAddress)</p>
client_id	<p>The client id is used by the broker to verify permissions to access topics. An empty field will use a random id which will only allow access to unprotected brokers. The expanded client id can be up to 127 characters but may be cut off after 23 characters by the broker according to MQTT 3.1 protocol specification. Topic expansion as shown with mqtt.help_topic_variables command applies.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.6.1.3 (brokerAccessClientId)</p>
security_mode	<p>Define the security method to apply for all messages.</p> <p>Values <i>NONE</i> No encryption is used <i>SSL_TLS</i> Use SSL encryption with certification file. <i>PSK_TLS</i> Use pre-shared-key based TLS support</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.6.1.4 (brokerAccessSecurityMode)</p>
username	<p>The username is optional and will be added to outgoing messages if set.</p> <p>Value String, max. 32 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.6.1.5 (brokerAccessUsername)</p>
enter_password	<p>Set a password for the user. No spaces are permitted.</p> <p>Action Execute command with parameter string max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.6.1.6 (brokerAccessEnterPassword)</p>
encrypted_password	<p>This holds the encrypted password. Do not modify.</p> <p>Value String, max. 128 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.6.1.7 (brokerAccessEncryptedPassword)</p>
keep_alive_timer	<p>The system will periodically send keep alive messages when the value is not 0. The time is specified in seconds.</p> <p>Value Number in range 0-0xFFFFFFFF</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.110.6.1.8 (brokerAccessKeepAliveTimer)</p>

trace_mode	For testing a trace mode may be enabled that displays MQTT activity to the console for trouble shooting. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.2.110.6.1.9 (brokerAccessTraceMode)
Group Path Description	local_broker_config Protocol.MQTT.local_broker_config This section only applies if this system should also provide the broker. It may be accessed by remote and local clients.
enable_local_broker	Run a local MQTT broker on port 1883. Also websocket on port 9001 is available. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.2.110.7.1.2 (localBrokerConfigEnableLocalBroker)
permit_anonymous	Permit access without any username. This should be used for initial testing only! Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.2.110.7.1.3 (localBrokerConfigPermitAnonymous)
permit_crypted_sockets	Permit access using encrypted websockets on port 8081. ATTENTION: Not implemented. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.2.110.7.1.4 (localBrokerConfigPermitCryptedSockets)
permit_encrypted_ssl	Permit access using encrypted SSL on port 8883. ATTENTION: Not implemented. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.2.110.7.1.5 (localBrokerConfigPermitEncryptedSsl)
permit_certified_ssl	Permit access using encrypted SSL with certificate on port 8884. ATTENTION: Not implemented. Values enabled, disabled OID 1.3.6.1.4.1.3181.10.6.2.110.7.1.6 (localBrokerConfigPermitCertifiedSsl)

certificate_name	The certificate itself is loaded via Management.Files.certification commands. ATTENTION: Not implemented.
Value	String, max. 64 characters.
OID	1.3.6.1.4.1.3181.10.6.2.110.7.1.7 (localBrokerConfigCertificateName)

36 Modbus

36.1 Functional Description

Preface

The Modbus/TCP industrial communications protocol. Often used with SCADA and PLC applications.

36.2 Modbus CLI Command Reference

The following table lists all CLI commands applicable for this feature section. For each parameter, the access mode is given:

R = Read Only, R/W = Read/Write, X = Executable Action.

Please note that the effective access rights are dependent on the login level of the user.

Category	Group	Table	Parameter	Options	Access	Description
Protocol.	modbus.					Modbus industrial communications protocol often used with SCADA and PLC applications.
			enable_modbus	R/W		Master enable for all Modbus TCP related functions.
			device_config[DYNAMIC].			This dynamic table is used to specify access parameter to one or more Modbus devices.
			name	R/W		Unique name used to identify the Modbus device. This name is referenced in the mapping tables.
			address	R/W		IP address or symbolic name of the Modbus device. IPv4 or IPv6 address may be specified.
			tcp_port	R/W		TCP port for Modbus IP connection. Standard port is 502.
			device_id	R/W		The device_id can be used to address sub-devices. Usually, the broadcast id 255 or a 1 should be selected.
			trace_mode	R/W		For testing a trace mode may be enabled that displays Modbus activity for this device to the console for trouble shooting.
			element_map[DYNAMIC].			This table is used to map Modbus data to local names that fit into the SmartOffice naming scheme.
			name	R/W		Unique name to reference this entry and to remember its functionality.
			mode	R/W		Defines whether the register or element is read from the device and mapped to local name or if the value of an existing local name is written to the device. The entry may be disabled to turn off all activity without losing the mapping information.
			device	R/W		The device name must exactly match the defined name of the device as defined in previous table.
			type	R/W		This entry defines which type of data are accessed which in turn defines the modbus function code to be used.

address	R/W	Coil or register address to be mapped. Value may be decimal or hex using 0xFF syntax. Careful, do not use leading 0 for decimal values or octal representation is expected.
length	R/W	Number of elements of requested type to be transferred. When multiple elements are transferred, the data are stored comma separated in one local element. The maximum length may be limited by the receiving data buffer and the selected formatting. A length of 0 skips the entry. For floating point or 32 bit values a length of 1 writes 2 registers (4 bytes).
poll_rate	R/W	The entry will be refreshed with the polling rate specified here. Same rate applies to writes. For writes only, the rate ON_CHANGE may be selected, which limits write to only when the local value has changed.
local_name	R/W	When the value is left empty, the data are only written to the element_data table or taken from there for write mode. When used, this defines the sensor list entry that is generated and linked to this element for read mode. In write mode the name of an existing actor or a new virtual actor is required. In both cases the name must be in the format: device:instance:attribute. Example: modbus_device:1:temperature. Alternative a persistent variable can be assigned starting with \$. Such variables can be used directly in microScript.
format	R/W	Since Modbus has no method to convey information about the data type this field allows to specify the best way to display the data. In combination with the unit parameter for example a meaningless value can be converted to easily understood value before further processing.
transformation	R/W	May be used to transform the value between external and internal format. Syntax: text=value,text=value or value=text or text=other_text,... Or calculations: =\$*10 Example C to F: =(\$*1.8)+32. Use # to append a unit to the value. Also in combination with calculation like: \$/1000#mW. For more options please refer to separate documentation. Note: Transformation is applied after format was applied.
manual_set_value	X	This command permits setting of the element_data value manually bypassing any internal script logic. The value is remains unchanged until the next manual write or any internal write to the element_data memory. Note: when a local_name is defined for an entry it has precedence and this action is meaningless.

device_status[16].		Summarizes the status of each configured Modbus device.
name	R	Unique name for reference. This correlates to the configured name.
operational_state	R	Indicates the operational state of the device. Device (not attribute) specific errors will be indicated here.
error_message	R	Contains the last error message related to the current state.
number_of_reads	R	Increments with every successful read message. This relates to one entry in the map.
number_of_read_errors	R	Increments with every unsuccessful read attempt. Error counter are reset when the device disconnects.
number_of_writes	R	Increments with every successful write message. This relates to one entry in the map.
number_of_write_errors	R	Increments with every unsuccessful write attempt. Error counter are reset when the device disconnects.
element_data[128].		Array of string variables that can be written and read by scripts. Several scripts may share data in these variables. The variables may also be accessed via SNMP.
name	R	Copy of the element name as configured in element_map.
operation_mode	R	Indicates the operational mode defined for this entry.
state	R	Indicates the operational state of this particular element entry.
error_message	R	Contains an error message if an error condition is pending.
number_of_updates	R	Increments every time this record is updated by reading the device or accessed to write data to the device.
last_update	R	Indicates the time when this entry was last updated or read or last accessed when writing to device.
value	R	For read elements this contains the received and formatted data. For elements that write to modbus, this contains a copy of the formatted data to be send out. Usually the send data are created programmatically but may also be set using the .manual_set_value action.

36.3 Modbus Configuration Parameters

Group	General Parameters	
Path	Protocol.Modbus	
enable_modbus	Master enable for all Modbus TCP related functions.	
	Values	enabled, disabled
	OID	1.3.6.1.4.1.3181.10.6.2.114.1 (modbusEnableModbus)
<hr/>		
Group	device_config , dynamical size	
Path	Protocol.Modbus.device_config	
Description	This dynamic table is used to specify access parameter to one or more Modbus devices.	
name	Unique name used to identify the Modbus device. This name is referenced in the mapping tables.	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.114.2.1.2 (deviceConfigName)
address	IP address or symbolic name of the Modbus device. IPv4 or IPv6 address may be specified.	
	Value	String, max. 128 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.114.2.1.3 (deviceConfigAddress)
tcp_port	TCP port for Modbus IP connection. Standard port is 502.	
	Value	Number in range 0-65535
	OID	1.3.6.1.4.1.3181.10.6.2.114.2.1.4 (deviceConfigTcpPort)
device_id	The device_id can be used to address sub-devices. Usually, the broadcast id 255 or a 1 should be selected.	
	Value	Number in range 0-255
	OID	1.3.6.1.4.1.3181.10.6.2.114.2.1.5 (deviceConfigDeviceId)
trace_mode	For testing a trace mode may be enabled that displays Modbus activity for this device to the console for trouble shooting.	
	Values	enabled, disabled
	OID	1.3.6.1.4.1.3181.10.6.2.114.2.1.6 (deviceConfigTraceMode)

Group	element_map , dynamical size	
Path	Protocol.Modbus.element_map	
Description	This table is used to map Modbus data to local names that fit into the SmartOffice naming scheme.	
name	Unique name to reference this entry and to remember its functionality.	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.114.3.1.2 (elementMapName)
mode	Defines whether the register or element is read from the device and mapped to local name or if the value of an existing local name is written to the device. The entry may be disabled to turn off all activity without losing the mapping information.	
	Values	<i>DISABLED</i> This entry is ignored <i>READ</i> The coil or memory is read (received) <i>WRITE</i> The coil or memory is written (send)
	OID	1.3.6.1.4.1.3181.10.6.2.114.3.1.3 (elementMapMode)
device	The device name must exactly match the defined name of the device as defined in previous table.	
	Value	String, max. 32 characters.
	OID	1.3.6.1.4.1.3181.10.6.2.114.3.1.4 (elementMapDevice)
type	This entry defines which type of data are accessed which in turn defines the modbus function code to be used.	
	Values	<i>COIL</i> One bit coil may be read or written. Boolean value. (FC01) <i>DISCRETE_INPUT</i> One bit input is read only. Boolean value. (FC02) <i>INPUT_REGISTER</i> 16 bit value is read only (FC03) <i>HOLDING_REGISTER</i> 16 bit value is read and writeable (FC04)
	OID	1.3.6.1.4.1.3181.10.6.2.114.3.1.5 (elementMapType)
address	Coil or register address to be mapped. Value may be decimal or hex using 0xFF syntax. Careful, do not use leading 0 for decimal values or octal representation is expected.	
	Value	Number in range 0-0xFFFFFFFF
	OID	1.3.6.1.4.1.3181.10.6.2.114.3.1.6 (elementMapAddress)
length	Number of elements of requested type to be transferred. When multiple elements are transferred, the data are stored comma separated in one local element. The maximum length may be limited by the receiving data buffer and the selected formatting. A length of 0 skips the entry. For floating point or 32 bit values a length of 1 writes 2 registers (4 bytes).	
	Value	Number in range 0-65535
	OID	1.3.6.1.4.1.3181.10.6.2.114.3.1.7 (elementMapLength)

poll_rate	The entry will be refreshed with the polling rate specified here. Same rate applies to writes. For writes only, the rate ON_CHANGE may be selected, which limits write to only when the local value has changed.	
Values	<i>ON_CHANGE</i>	Only applied to write mode. Update modbus device only when local actor value changes.
	<i>POLL_250MS</i>	Poll 4 times per second
	<i>POLL_500MS</i>	Poll twice per second
	<i>POLL_1000MS</i>	Poll every second
	<i>POLL_5000MS</i>	Poll every 5 seconds
OID	1.3.6.1.4.1.3181.10.6.2.114.3.1.8 (elementMapPollRate)	

local_name	When the value is left empty, the data are only written to the element_data table or taken from there for write mode. When used, this defines the sensor list entry that is generated and linked to this element for read mode. In write mode the name of an existing actor or a new virtual actor is required. In both cases the name must be in the format: device:instance:attribute. Example: modbus_device:1:temperature. Alternative a persistent variable can be assigned starting with \$. Such variables can be used directly in microScript.	
Value	String, max. 64 characters.	
OID	1.3.6.1.4.1.3181.10.6.2.114.3.1.9 (elementMapLocalName)	

format

Since Modbus has no method to convey information about the data type this field allows to specify the best way to display the data. In combination with the unit parameter for example a meaningless value can be converted to easily understood value before further processing.

Values	<i>RAW</i>	Values are stored as they are received
	<i>BOOL</i>	Null is false, anything else is true
	<i>UNSIGNED</i>	Non-negative 16bit decimal number
	<i>SIGNED</i>	Signed decimal 16bit number
	<i>STRING</i>	Treat bytes as string and append termination 0 if required.
	<i>HEX_PACKED</i>	Encode every byte into 2 chars representing a hex value. No spaces between bytes. E.g.: 7EAC
	<i>HEX_LIST</i>	Encode every byte into 4 chars representing a hex value comma separated. E.G.: 0x7E,0xAC
	<i>FLOAT_ABCD</i>	Four successive byte are treated as floating point value. Note the byte order to match the device.
	<i>FLOAT_BADC</i>	Four successive byte are treated as floating point value. Note the byte order to match the device.
	<i>FLOAT_CDAB</i>	Four successive byte are treated as floating point value. Note the byte order to match the device.
	<i>FLOAT_DCBA</i>	Four successive byte are treated as floating point value. Note the byte order to match the device.
	<i>UNSIGNED32_BIG</i>	Non-negative 32bit decimal number in big endian format
	<i>UNSIGNED32_LTL</i>	Non-negative 32bit decimal number in little endian format
	<i>SIGNED32_BIG</i>	Signed 32bit decimal number in big endian format
	<i>SIGNED32_LTL</i>	Signed 32bit decimal number in little endian format
OID	1.3.6.1.4.1.3181.10.6.2.114.3.1.10 (elementMapFormat)	

transformation

May be used to transform the value between external and internal format. Syntax: text=value,text=value or value=text or text=other_text,.. Or calculations: =\$*10 Example C to F: =(\$*1.8)+32. Use # to append a unit to the value. Also in combination with calculation like: \$/1000#mW. For more options please refer to separate documentation. Note: Transformation is applied after format was applied.

Value	String, max. 128 characters.
OID	1.3.6.1.4.1.3181.10.6.2.114.3.1.11 (elementMapTransformation)

manual_set_value	<p>This command permits setting of the element_data value manually bypassing any internal script logic. The value is remains unchanged until the next manual write or any internal write to the element_data memory. Note: when a local_name is defined for an entry it has precedence and this action is meaningless.</p> <p>Action Execute command with parameter string max. 1024 characters.</p> <p>OID 1.3.6.1.4.1.3181.10.6.2.114.3.1.12 (elementMapManualSetValue)</p>
------------------	---

36.4 Modbus Status Parameters

37 Frequently Asked Questions

Q: How do I assign an IP address to the switch?

There are different ways to assign an initial IP address.

NMP Autodiscovery

The Network Management Platform provides a simple mechanism to detect and configure MICROSENS switches, called 'MAC Discovery'.

As this function works on the Ethernet-Layer, the switch to be configured must be directly connected to the Ethernet segment the PC running NMP is attached to.

Before starting the procedure, check the interface setting in the 'Application settings' and select the correct host network interface. NMP has to be restarted before the new setting is applied.

By pressing the 'MAC Discovery' button in the toolbar, a window with a list of the detected devices opens. If the switch to be configured is not displayed, please check the NMP application host interface settings again. If the switch is in an unknown state, it may be helpful to execute a reset to factory defaults by pressing the factory button for more than 20 sec.

Now the IP settings of the switch can be entered. By pressing the 'Send' button, these settings are applied to the device. If the settings were applied successfully, the Status box left to the send button turns green.

The new IP settings take effect immediately, no reset of the device is required. Now the switch can be accessed with the IP settings assigned.

INFO: NMP is a separate product developed and licensed by MICROSENS. For productive use in networks, a commercial license is required. For configuring single devices, an evaluation license can be used free of charge. Please contact MICROSENS sales team for further information about NMP.

DHCP

By factory default, the switch IP stack is configured for dynamic IP address assignment via DHCP (Dynamic Host Configuration Protocol). Connecting the switch to a network with a running DHCP

server should automatically provide the device with a valid IP address. Under this address the switch management can be accessed.

Q: How do I update the firmware of a switch?

The firmware of the switch is stored in a single archive file on the memory card. Such a firmware file can include a full image, to replace all files including the Linux Kernel, or an incremental update, including only the files affected by changes. All update files contain an individual script file that installs the included files to the right locations. So a firmware update requires basically just two steps: transfer the update file and start the update script. This procedure can be executed via different interfaces:

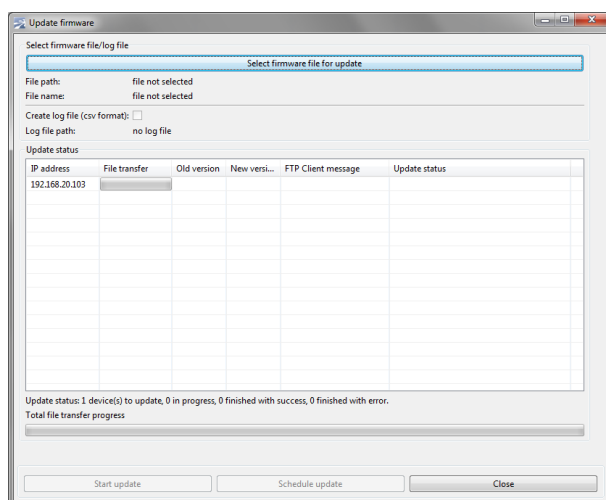
Firmware update via CLI

Before the update file can be transferred to the switch, the appropriate file transfer server must be activated on the device. File Transfer to and from the switch can be done via TFTP, FTP and SFTP. To enable the intended server, the corresponding parameter must be enabled via CLI. *'Management.Files.server.ftp_server = Enabled'* activates the FTP server. Using an external FTP tool (e.g. 'Filezilla' from Mozilla foundation), the firmware update file can be downloaded on the switch.

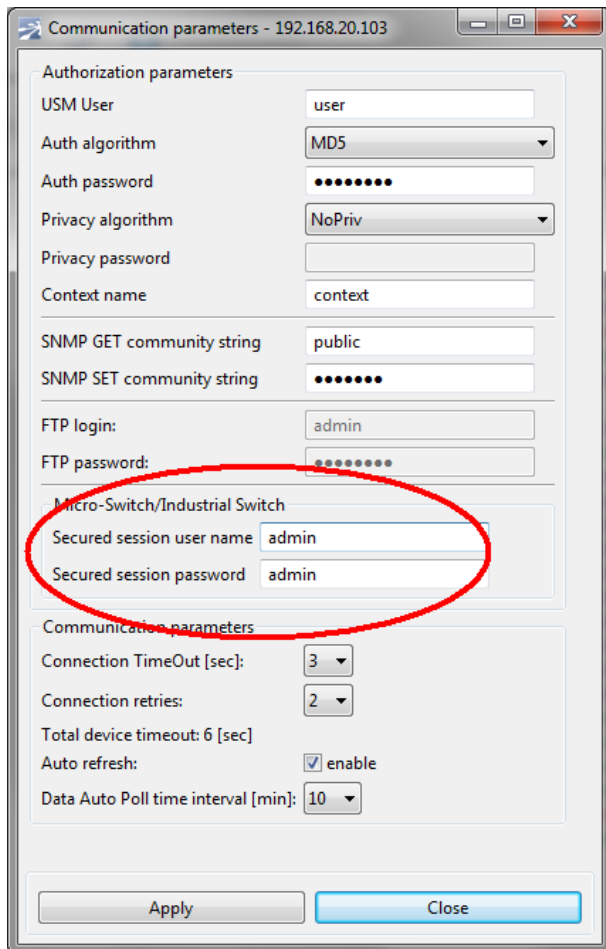
After successful download, the file availability can be checked via *'Management.Files.firmware.display_files'* command. Now the update can be installed by executing the command *'Management.Files.firmware.install_software_update = filename'*. The script file executed will provide feedback about the operation. After the execution, the update is installed. In most cases no reboot is required.

Firmware Update via NMP

The Network Management Platform is a separate tool to facilitate the configuration, administration and management of MICROSENS switches. By right-clicking on the device to be updated in the device list, the option 'firmware update' can be selected. Now the firmware file to be installed can be selected. The firmware is then automatically transferred to the device and installed. The status is shown in a separate window.



The transfer is done via FTP protocol using the internal FTP server of the switch. The server is automatically enabled before and disabled after the transfer.



Please check the username/password settings in the 'communication parameters setting' for the device. For a successful firmware update, the username/password of a valid administrator account on the switch must be configured.

Q: What do I do if anything went wrong during the firmware update and now the device is not functional anymore?

Don't panic, if the device is not responding to any action due to a software problem, it can always be reactivated by exchanging the memory card with a card of a known good status.

As the memory card stores the full system including kernel and configuration, the switch can always be reactivated. The switch device-internally only stores the basic device-specific parameters (article number, serial number etc.) and the boot loader. These files are write protected and never altered at runtime.

Generally the situation should occur only in rare cases. The memory card utilizes a journaling filing system that is failure-tolerant by design.

Q: How do I store an individual switch configuration on the device?

The configuration parameters are stored in XML-files, separate for each feature group (e.g. 'VLAN' or 'Port-based Access Control'). All these XML-files stored in a directory folder define the device configuration. A nearly unlimited number of folders for different configurations can be created on the device.

With the command *'Management.Files.configuration.backup_to_folder = foldername'*, the current device configuration is stored in a new folder with the given name.

The command *'Management.Files.configuration.restore_from_folder = foldername'*, a stored config from the folder given is activated as running config. The folders are accessible externally by FTP, TFTP or SFTP file transfer.

Q: What does XML-file format mean?

XML means eXtensible Markup Language and defines a text-based format for storing information. All data content is encapsulated with tags. Keywords for these tags can be freely defined to fit best for the intended purpose. While XML files are mainly intended for automated processing by software, they still remain human readable and editable.

MICROSENS switch configuration files use a flexible format that can be easily adapted and extended for different device types.

Q: How do I reset the switch configuration to factory default settings?

In some cases it can be required to set back the switch configuration to factory default values. This may be necessary if a misconfiguration blocks any access to the switch (e.g. by incomplete VLAN settings) or a clean system is required.

The factory default settings are stored in the internal configuration folder 'factory'. This folder is always available and write protected.

Via CLI, the command *'Management.Files.configuration.restore_from_folder = factory'* overwrites the running configuration with the stored factory default values.

If no network access to the device is possible, the configuration can also be restored by pressing the system button on the device front panel. The button must be pressed continuously for approx. 10 sec. to initiate the restore process. The system LED is blinking blue during the operation.

INFO: The factory default settings do not affect the IP address settings. After a reset to factory default, the device is still accessible via the configured IP address before the restore. The IP address can always be reassigned using NMP Auto-Discovery function.

Q: How do I define an individual factory default configuration for the switch?

Especially in locations with public access to the switch, it may not be desirable that the switch can be reset to a completely blank configuration, may allowing unrestricted access to the network and the switch management, leading to possible security threats.

For these cases, the folder from which the configuration is restored by pressing the system button can be configured. The parameter *'Management.Files.configuration.factory_default_folder'* holds the name of the configuration folder to be used. Changing this parameter to a different folder name

that has been created with an alternative configuration makes this folder to the new factory default configuration.

The folder 'factory' is not altered and can always be reactivated.

ATTENTION: Please check the function of the individual configuration used as default setting carefully before activation. If this configuration is faulty, there is no way to change it back. If a problem occurs with a faulty default configuration, it is always possible to reactivate the switch by exchanging the memory card to a new one with standard default settings.

38 GNU General Public License v3

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <http://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

- a. The work must carry prominent notices stating that you modified it, and giving a relevant date.
- b. The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".
- c. You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

- d. If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

- a. Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.
- b. Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.
- c. Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.
- d. Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.
- e. Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to

ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

- a. Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
- b. Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
- c. Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
- d. Limiting the use for publicity purposes of names of licensors or authors of the material; or
- e. Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
- f. Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients.

"Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero

General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

39 Disclaimer

All information in this document is provided "as is" and subject to change without notice. MICROSENS GmbH & Co. KG disclaims any liability for the correctness, completeness or quality of the information provided, fitness for a particular purpose or consecutive damage. Any product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "MICROSENS" is a trademark of MICROSENS GmbH & Co. KG. "IEEE" is a trademark of the Institute of Electrical and Electronics Engineers, Inc. "Microsoft", "Windows" and "Internet Explorer" are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. "Mozilla" and "Firefox" are registered trademarks of the Mozilla Foundation.

©2020 MICROSENS GmbH & Co. KG, Küferstr. 16, 59067 Hamm/Germany. All rights reserved. This document in whole or in part may not be duplicated, reproduced, stored or retransmitted without prior written permission of MICROSENS GmbH & Co. KG.

Document generated using Documentation rev. 211 and Unified_Config rev. 9842.