Nexans Switch Management

with Firmware-Version *V6.04H* *or later*

Manual KD674E30

FEATURES

- Modular respectively On-Board high-performance management for Nexans switches
- Configuration management and archiving via Nexans Device Manager (NEXMAN)
- Manual and automatic firmware update via Nexans Device Manager (NEXMAN)
- Automatic loading of a switch configuration via DHCP/BootP option
- Automatic loading of a new firmware via DHCP/BootP and command file
- Password protection using two access levels for access via WEB, Telnet/SSH/V.24 and NEXMAN
- Automatic IP address allocation via DHCP or fixed IP address
- Global management access protection via access list and up to 16 IP ranges
- Management Status-LED to display operating state
- Configuration is stored permanently in flash
- Display of product data such as product name, serial number, manufacturing date, temperature, etc.
- Ports can be enabled/disabled
- Autonegotiation or fixed setting of transmission parameters for each TP port
- Error counter per port for detection of incorrect duplex settings
- Support of 256 VLAN IDs in the range from 1 to 4095
- Untagged Default-VLAN can be set for each port
- Frame tagging (trunking) in accordance with IEEE802.1q selectable for each port
- Prioritisation possible for each port
- Four output queues per port for Prioritisation weighting using strict or weighted fair queuing
- Bandwidth limitation can be set separately per port for Rx and Tx frames
- Portsecurity via manual definition of up to three MAC addresses per port
- Portsecurity via automatic learning of up to three MAC addresses per port
- Loop/broadcast limiter for protection against inadvertent or malicious packet storms
- Switch state display and configuration via web browser (HTTP and HTTPS)
- Password protection using two access levels (R/W or R/O) for access via web browser
- Switch state display and configuration via SNMPv1/v2/v3 and CLI (SSH, TELNET, V.24)
- Password protection using two access levels (R/W or R/O) for access via Telnet
- Eight SNMP trap and Syslog destination IP addresses selectable, each with 30 different event types
- CLI and NEXMAN authentication via RADIUS server
- Portsecurity with authentication of the authorized MAC addresses via RADIUS server
- Portsecurity according to IEEE802.1X with authentication via RADIUS server
- Redundancy via Rapid Spanning Tree, Multiple Spanning Tree, Media Redundancy Protocol, Link Aggregation or HSR
- Zero Touch Configuration
- CLI and NEXMAN authentication and accounting via TACACS+ server
- CLI command authorization via TACACS+ server
- Access Control Lists (ACLs)
- Scripting

CONTENTS

1. Supported Standards

1.1. IEEE / ANSI / IEC / ISO / IETF / IANA:

IEEE 802.3	10BaseT
IEEE 802.3u	100BaseTX, 100BaseFX
IEEE 802.3ab	1000BaseT
IEEE 802.3af	DTE Power via MDI (Power over Ethernet - PoE)
IEEE 802.3at	DTE Power Enhancements (PoE Highpower 30W)
IEEE 802.3z	1000BaseX
IEEE 802.3x	Flow Control
IEEE 802.1AB	Link Layer Discovery Protocol
ANSI/TIA-1057	Link Layer Discovery Protocol for Media Endpoint Devices
IEEE 802.1AX	Link Aggregation (formerly IEEE 802.3ad)
IEEE 802.1D	MAC Bridges
IEEE 802.1D	Rapid Spanning Tree Protocol (formerly 802.1w)
IEEE 802.1D	Class of Service (formerly 802.1p)
IEEE 802.1Q	VLAN Tagging
IEEE 802.1Q	VLAN Classification by Protocol and Port (formerly 802.1v)
IEEE 802.1Q	Multiple Spanning Tree Protocol (formerly 802.1s)
IEEE 802.1ad	Provider Bridges (Q-in-Q)
IEEE 802.1X	Port-Based Network Access Control
ISO/IEC 15802-3	Media Access Control (MAC) Bridges
IEC 62439-2	Media Redundancy Protocol (MRP)
IETF-opsawg-tacacs-15	Draft TACACS+ Protocol
IANA	Internet Assigned Numbers Authority

1.2. RFCs:

RFC 768	UDP
RFC 783	TFTP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 951	BOOTP
RFC 1112	Host Extensions for IP Multicasting
RFC 1155	SMIv1
RFC 1157	SNMPv1
RFC 1321	MD5 Algorithm
RFC 1493	Dot1d
RFC 1542	BOOTP-Extensions
RFC 1757	RMON
RFC 1907	MIB2
RFC 1945	HTTP/1.0
RFC 1981	Path MTU Discovery for IPv6

RFC 2001	TCP Slow start congestion avoidance
RFC 2018	TCP Selective Acknowledge Options
RFC 2104	HMAC Message Authentication
RFC 2131	DHCP
RFC 2132	DHCP-Options
RFC 2236	Internet Group Management Protocol, Version 2
RFC 2284	EAP
RFC 2375	IPv6 Multicast Address Assignments
RFC 2460	Internet Protocol Version 6
RFC 2464	Transmission of IPv6 Packets over Ethernet Networks
RFC 2474	Definition of the Differentiated Services Files (DSField) in IPv4 & IPv6 Headers
RFC 2578	SNMPv2-SMI
RFC 2579	SNMPv2-TC
RFC 2710	Multicast Listener Discovery (MLD) for IPv6 (host-side only)
RFC 2711	IPv6 Router Alert Option (DSField) in the IPv4 & IPv6 Headers
RFC 2865	RADIUS
RFC 2866	RADIUS Accounting
RFC 2868	RADIUS Tunnel Extension
RFC 2869	RADIUS Extensions
RFC 3041	Privacy Extensions for Stateless Address Auto-configuration in IPv6
RFC 3164	SYSLOG
RFC 3484	Default Address Selection for IPv6
RFC 3487	IPv6 Global Unicast Address Format
RFC 3493	Basic Socket Interface Extension for IPv6
RFC 3579	RADIUS Support for EAP
RFC 3580	IEEE802.1X RADIUS Usage Guidelines
RFC 3587	IPv6 Aggregatable Global Unicast Address Format
RFC 3590	Source Address Selection for the Multicast Listener Discovery Protocol
RFC 3411	An Architecture for Describing SNMP Management Frameworks
RFC 3412	Message Processing and Dispatching for SNMP
RFC 3413	SNMP Applications
RFC 3414	User-based Security Model (USM) for SNMPv3
RFC 3416	Version 2 of the Protocol Operations for SNMP
RFC 3810	Multicast Listener Discovery Version 2
RFC 4007	IPv6 Scoped Address Architecture
RFC 4193	Unique Local IPv6 Unicast Addresses
RFC 4213	Transition Mechanisms for IPv6 Hosts and Routers
RFC 4250	Secure Shell (SSH) Protocol Assigned Numbers
RFC 4251	Secure Shell (SSH) Protocol Architecture
RFC 4252	Secure Shell (SSH) Authentication Protocol
RFC 4253	Secure Shell (SSH) Transport Layer Protocol
RFC 4254	Secure Shell (SSH) Connection Protocol
RFC 4291	IPv6 Addressing Architecture
RFC 4330	Simple Network Time Protocol (SNTP)
RFC 4372	Chargeable User Identity
RFC 4443	IPv6 Internet Control Message Protocol (ICMPv6) for IPv6
RFC 4861	Neighbor Discovery for IPv6

RFC 4862	IPv6 Stateless Address Auto-configuration
RFC 5095	Deprecation of Type 0 Routing Headers in IPv6
RFC 6933	Entity MIB

1.3. SNMP MIBs:

Private	NEXANS-MIB
Private	NEXANS-BM-MIB
RFC 1213	RFC1213-MIB (MIB-II)
RFC 2665	EtherLike-MIB
RFC 2819	RMON-MIB
RFC 2863	IF-MIB
RFC 3411	SNMP-FRAMEWORK-MIB
RFC 4188	BRIDGE-MIB
RFC 4318	RSTP-MIB
RFC 4363	Q-BRIDGE-MIB (formerly RFC 2674)
RFC 6933	ENTITY-MIB IANA-ENTITY-MIB (IMPORTS) UUID-TC-MIB (IMPORTS)
IEEE 802.1AB	LLDP-MIB
IANA	IANA-ADDRESS-FAMILY-NUMBERS-MIB

2. Switch Models

To distinguish between the different switch models, each functional different model has another switch type.

The current switch type can be verified via WEB, Telnet/SSH/V.24 console, SNMP and NEXMAN (see chapter *10.1. Determination of Switch Type and Management Version).*

2.1. Supported Switch Types

The below list indicates all switch versions which are supported by the current firmware release.

IMPORTANT:
The functions described in this document are not supported by all switch types and/or firmware versions.

Office switches:

1 FiberSwitch 100 BM
2 CopperSwitch 100 BM
3 FiberSwitch 100 BM-A Desk
3 Access FiberSwitch 4-10/100
4 CopperSwitch 100 BM-A Desk
5 FiberSwitch 100 BM-A
6 CopperSwitch 100 BM-A
7 FiberSwitch 100 BM+
8 CopperSwitch 100 BM+
9 FiberSwitch 100 BM+ Desk
9 Access FiberSwitch 4-10/100+
10 CopperSwitch 100 BM+ Desk
11 DualSwitch 100 BM+ Desk, Uplink= FO/FO
12 DualSwitch100 BM+ Desk, Uplink= TP/TP
13 DualSwitch100 BM+ Desk, Uplink= FO/TP
14 FiberSwitch 100 BM+ af Desk
15 CopperSwitch 100 BM+ af Desk
16 FiberSwitch M 100 BM
17 CopperSwitch M 100 BM
18 FiberSwitch 100 BM+ Vers.C Desk
19 CopperSwitch 100 BM+ Vers.C Desk
20 FiberSwitch 1000 BM+
21 DualSwitch 1000 BM+, Uplink = FO/FO
22 DualSwitch 1000 BM+ Desk, Uplink= FO/FO
23 DualSwitch 1000 BM+, Uplink = FO/TP
24 DualSwitch 1000 BM+, Uplink = TP/TP
25 CopperSwitch 1000 BM+
27 GigaSwitch 541 Desk
28 GigaSwitch 542 SFP Desk
50 GigaSwitch BM+, Uplink = FO
51 GigaSwitch BM+, Uplink = TP
52 GigaSwitch V2+, Uplink = FO
53 GigaSwitch V2+, Uplink = FO+TP
54 GigaSwitch V2+, Uplink = TP+TP
55 GigaSwitch V2+, Uplink = SFP+TP
56 GigaSwitch V2+, Uplink = TP
60 GigaSwitch V3, Uplink = FO+TP
61 GigaSwitch V3, Uplink = SFP+TP
62 GigaSwitch V3, Uplink = SFP+TP
63 GigaSwitch V3, Uplink = 2xSFP
64 GigaSwitch V3, Uplink = FO
66 FiberSwitch 1000 V3, Uplink = SFP+TP
67 FiberSwitch 100 V3, Uplink = FO
70 GigaSwitch 641 Desk, Uplink = SFP+TP
71 GigaSwitch 642 Desk, Uplink = 2xSFP
72 GigaSwitch V5, Uplink = TP+2xSFP
73 GigaSwitch V5, Uplink = TP+SFP

74 GigaSwitch V5, Uplink = 2xSFP
75 GigaSwitch 641 Desk V5, Uplink = SFP+TP
76 GigaSwitch 642 Desk V5, Uplink = 2xSFP
77 GigaSwitch V3 (HW5), Uplink = SFP+TP
78 GigaSwitch V5 (HW5), Uplink = SFP+2xTP

Industrial switches:
30 iSwitch 740
31 iSwitch 741
32 iSwitch 742
33 iSwitch G 1042
34 iSwitch G 1043
35 iSwitch 742 SFP-I
36 iSwitch G 1043 3VI
37 iGigaSwitch 541
38 iGigaSwitch 542 SFP-2VI
40 iGigaSwitch 1604 E+ SFP-4VI
40 iGigaSwitch 1604 E+ SFP-4VI HW3
41 iGigaSwitch 1608 E+ SFP-8VI HW3
42 iGigaSwitch 1612 E+ SFP-12VI HW3
85 iGigaSwitch 1002 E+ SFP-2VI HW5
86 iGigaSwitch 1004 E+ SFP-4VI HW5
87 iGigaSwitch 1008 E+ SFP-8VI HW5
90 iGigaSwitch 1604 SFP-4VI HW5
91 iGigaSwitch 1608 SFP-8VI HW5
92 iGigaSwitch 1612 SFP-12VI HW5
93 iGigaSwitch 1606 HSR SFP-6VI HW5
94 iGigaSwitch 1202 HSR SFP-2VI HW5

2.2. Supported Frame and MTU lengths, Jumbo Frame Support

In the table below, the maximum frame and MTU lengths of various switch types are indicated. The maximum MTU length is the maximum frame length minus a total of 18 bytes for the destination address, source address, type/length field and checksum (CRC).

Switch Type	Max. frame length 10/100/1000 Mbit/s	Max. MTU length 10/100/1000 Mbit/s	Jumbo Frame Support
iSwitch 74x iSwitch G 10xx	1632	1614	No
GigaSwitch V3 GigaSwitch 64x Desk V3 FiberSwitch 100 V3 FiberSwitch 1000 V3 iGigaSwitch HW3 GigaSwitch V5 GigaSwitch 64x Desk V5 iGigaSwitch HW5	9600	9582	Yes

NOTE ON JUMBO FRAME SUPPORT:
Although there is no IEEE standard for the maximum length of jumbo frames, the use of a maximum of 9000 bytes for jumbo frames is generally recommended. This ensures compatibility between different switch manufacturers. Thus the 9600 bytes permitted for Nexans Switches offer enough margin for future extensions of the packet length, especially for applications with additional VLAN tags.

2.3. Core Switching Latencies

The table below lists the latencies as defined in RFC 1242. Typically, LIFO values are relevant for store and forward switches. The FIFO values are indicated for the sake of completeness, although these are usually used for cut through switches.

Switch Type	100 MBit/s 64 Byte	100 MBit/s 1518 Byte	1 GBit/s 64 Byte	1 GBit/s 1518 Byte

	FIFO / LIF0	FIFO / LIF0	FIFO / LIF0	FIFO / LIF0
iSwitch 74x iSwitch G 10xx iGigaSwitch 54x GigaSwitch V3 GigaSwitch 64x Desk V3 FiberSwitch 100 V3 FiberSwitch 1000 V3	10 µs / 4,9 µs	126 µs / 5,0 µs	2,5 µs / 2,0 µs	14 µs / 2,2 µs
GigaSwitch V5 GigaSwitch 64x Desk V5 iGigaSwitch HW5	9 µs / 3,9 µs	125 µs / 4,0 µs	2,7 µs / 2,2µs	15 µs / 2,5 µs

2.4. Core Switching Capacities

The table below lists the switching capacities of various switch types. The indicated switches can independently and simultaneously transmit and receive on all ports (non-blocking).

Each GigaBit Port has a maximum full duplex switching capacity of 2 x 1.488.095 pps (packets per second).

Switch Type	Port Capacity	Core Switching Capacity non-blocking
iSwitch G 10xx	2x 2 GBit/s + 8x 200 MBit/s	8 GBit/s
iGigaSwitch 54x	5x 2 GBit/s	14 GBit/s
iGigaSwitch 100x HW5	10x 2 GBit/s	30 GBit/s,
iGigaSwitch 12xx/16xx HW5	16x 2 GBit/s	50 GBit/s
GigaSwitch V3 GigaSwitch V5	5-6x 2 GBit/s	20 GBit/s
GigaSwitch 64x Desk V3 GigaSwitch 64x Desk V5	6x 2 GBit/s	20 GBit/s

2.5. Core Switch Packet Buffer Sizes

The table below lists the switching capacities of various switch types. The packet buffer is dynamically distributed to all ports.

Switch Type	Buffer Size
GigaSwitch V3 GigaSwitch 64x Desk V3 iGigaSwitch 54x iSwitch G 10xx	128 kBytes
GigaSwitch V5 GigaSwitch 64x Desk V5 iGigaSwitch HW5	512 kBytes

3. Management Module and Firmware-Versions

3.1. Management Module Versions

Depending on the manufacturing period and scope of functions several Management Module versions (HW0, HW1, HW2, HW3 and HW5) are in use, while the versions HW0, HW1 and HW2 are not longer produced. In addition, for office and industrial switches there are separate versions with different temperature ranges available.

The following table shows a summary of the different Management Module versions HW3 and HW5:

Hardwareversion	**HW3 Office**	**HW3 Industrial**	**HW5 Office**	**HW5 Industrial**
Description	Management Module Vers. 3	Industrial Management Module Vers. 3	Office Management Hardware Vers. 5	Industrial Management Hardware Vers. 5
Sub-Versions See Note (1)	Vers. 3.0x = Plugable module Vers. 3.1x = On-Board Vers. 3.2x = On-Board		Vers. 3.5x = On-Board Vers. 5.xx = On-Board	
Part number	88301504	88301505	On-Board only	On-Board only
Bundle Code	ES3	PRO3	Not used	Not used
RAM	32 MByte		128 MByte	
NOR FLASH	8 MByte (Sub-Vers. 3.0x/3.1x) 16 MByte (Sub-Vers. 3.2x)		16 MByte	
NAND FLASH	None		256 MByte	
Ethernet connection of the management processor	External attached processor 100Mbps		Internal processor Direct memory access	
Firmware update	Update in a separate FLASH area. Corruption impossible.		Dual Firmware storage in FLASH. Corruption impossible.	
Application software	Nexans application code		Nexans application code 100% backwards compatible with HW3 switches	

Note (1) The sub-version indicates the version of the hardware (eg plugable or on-board module, FLASH size) and will be shown in firmware and manager version V3.66 or higher.

3.2. Firmware Families

The various firmware versions are summarized into the following firmware families depending on their scope of functions and switch version:

- Firmware families for office switches
- Firmware families for industrial switches

The firmware version currently installed in the switch can be verified via WEB, Telnet/SSH/V.24 Console, SNMP and NEXMAN (see *10.1. Determination of Switch Type and Management Version*)

Chapter *9. Summary of all State and Configuration Parameters* contains a complete list of all switch parameters. This list indicates which parameters can be displayed and/or configured via Web, Telnet/SSH/V.24 Console, SNMP or NEXMAN.

IMPORTANT:
The functions described in this manual are not supported by all switch types, management modules and/or firmware versions.

3.2.1. Office Firmware Families

The following table shows an overview of the available firmware versions:

Mgmt hardware version	Bundle code	Firmware version	Image filename	Notes
HW5	-	HW5-F40-P07-OFFICE	hw5-f40-p07-office-v5.xx.swu	For all HW5 office(1) switches
HW3	ES3	HW3-F21-P06-OFFICE	hw3-f21-p06-off-vx.xx.img	For all HW3 office(1) switches

(1) You can see an list over all office switches in *2.1 Supported Switch Types*

3.2.2. Industrial Firmware Families

The following table shows an overview of the available firmware versions:

Mgmt hardware version	Bundle code	Firmware version	Image filename	Notes
HW5	-	HW5-F47-P16-INDUSTRIAL	hw5-f47-p16-industrial-v5.xx.swu	For all HW5 industrial(1) switches with 16 ports
HW5	-	HW5-F46-P10-INDUSTRIAL	hw5-f46-p10-industrial-v5.xx.swu	For all HW5 industrial(1) switches with up to 10 ports
HW3	PRO3	HW3-F30-P16-INDUSTRIAL	hw3-f30-p16-ind-vx.xx.img	For all HW3 industrial(1) switches with 16 ports
HW3	PRO3	HW3-F22-P10-INDUSTRIAL	hw3-f22-p10-ind-vx.xx.img	For all HW3 industrial(1) switches with up to 10 ports

(1) You can see an list over all industrial switches in *2.1 Supported Switch Types*

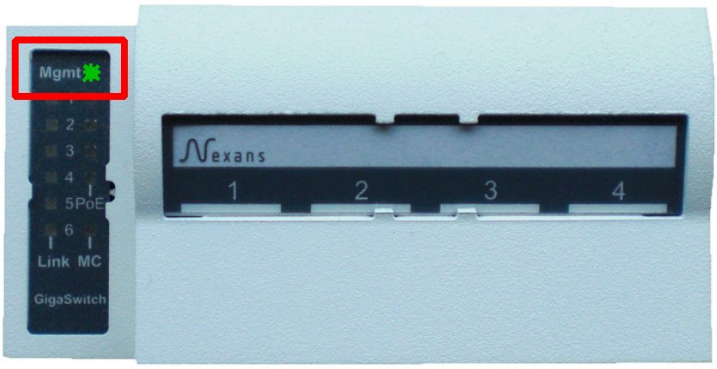
3.3. Management Status-LED

After the system is switched on, a self-test is carried out checking the hardware of the switch and the management module. The result of this test is shown by the Status-LED.

3.3.1. Status-LED on Office Switches of type 'GigaSwitch V3 / V5'

The following figures show the location of the Status-LED on Cable-Duct switches of type 'GigaSwitch V3 / V5':

GigaSwitch V3:



GigaSwitch V5:

GigaSwitch V3 / V5 Desk:

This on-board management has a multi colour LED marked ‘Mgmt’ with the following meaning:

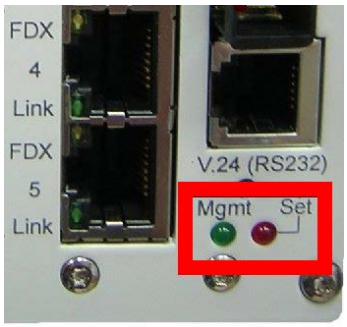
- Blue: Switch is booting
- Blue flashing: Switch is flashing new firmware
- Green flashing: Boot successful but DHCP waits for a valid IP address
- Green: Boot successful and valid IP address received via DHCP or IP address manual configured
- Red: Boot successful and switch runs with fixed IP address172.23.44.111
- Red flashing: Error condition, switch or management module may be damaged

During booting the Status-LED lights up in blue. The Status-LED changes to solid green only after all tests have been completed without error. If the LED flashes red or remains off, an error has been detected and the management processor has been stopped. This means the switch will have to be replaced.

3.3.2. Management Status-LED on Industrial Switches of type 'iSwitch 74X / 104X’

Industrial switches have two management Status-LEDs which are marked as **Mgmt** and **Set**.

The following figure shows the location of the two LEDs:

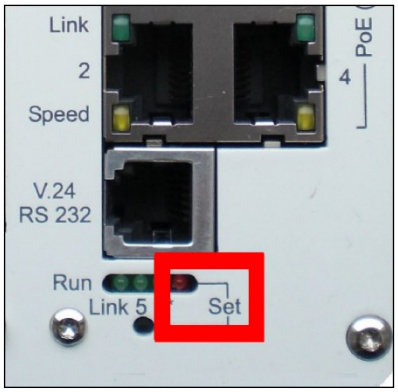


While switch is booting the Set-LED must light for some seconds. When all tests have been completed without errors, the Set-LED is turned off and the Mgmt-LED is turned on permanently. If the Mgmt-LED remains off or the SET-LED flashes repeatedly, there must be an error and the management processor has been stopped. This means the management module, and/or the switch will have to be replaced.

3.3.3. Management Status-LED on Industrial Switches of type 'iGigaSwitch 54X'

Industrial switches of type **iGigaSwitch** have only a Set-LED.

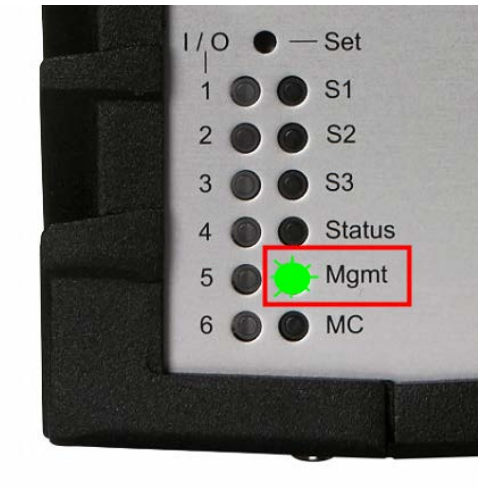
The following figure shows the location of the Set-LED:



While switch is booting the Set-LED must light for some seconds. When all tests have been completed without errors, the Set-LED is turned off permanently. If the LED remains on or flashes repeatedly, there must be an error and the management processor has been stopped. This means the management module, and/or the switch will have to be replaced.

3.3.4. Status-LED on Office Switches of type 'iGigaSwitch 100x and 16XX'

The following figure shows the location of the Status-LED.



This on-board management has a multi colour LED marked ‘Mgmt’ with the following meaning:

- Blue: Switch is booting
- Blue flashing: Switch is flashing new firmware
- Green flashing: Boot successful but DHCP waits for a valid IP address
- Green: Boot successful and valid IP address received via DHCP or IP address manual configured
- Red: Boot successful and switch runs with fixed IP address172.23.44.111
- Red flashing: Error condition, switch or management module may be damaged

During booting the Status-LED lights up in blue. The Status-LED changes to solid green only after all tests have been completed without error. If the LED flashes red or remains off, an error has been detected and the management processor has been stopped. This means the switch will have to be replaced.

3.4. Management Configuration Switches and Pushbuttons

The configuration switch is used for selecting the following operating modes:

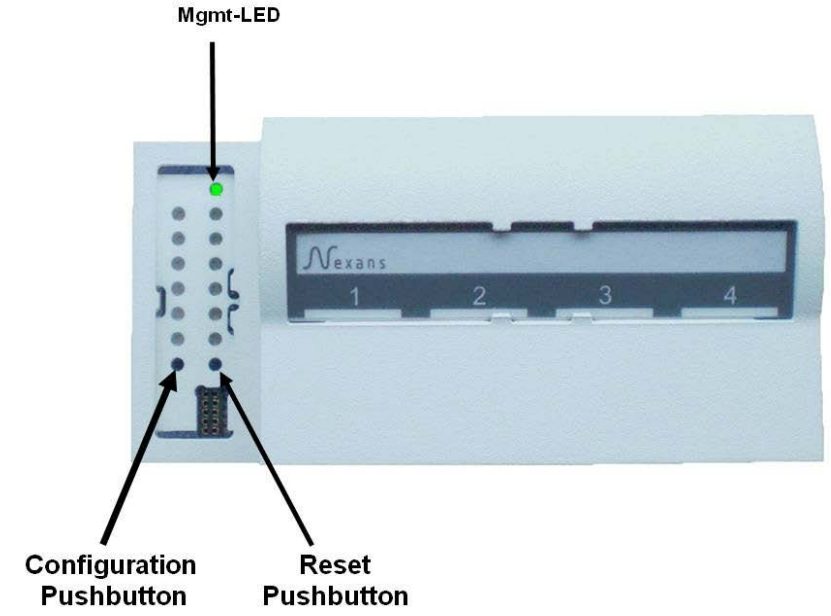
- Booting with flash configuration (normal mode)
- Booting with fixed IP address
- Booting with factory default settings
- Booting with factory default settings and fixed IP address (optional)

For a detailed description of the above modes see chapter *3.6. Management Operation Modes*.

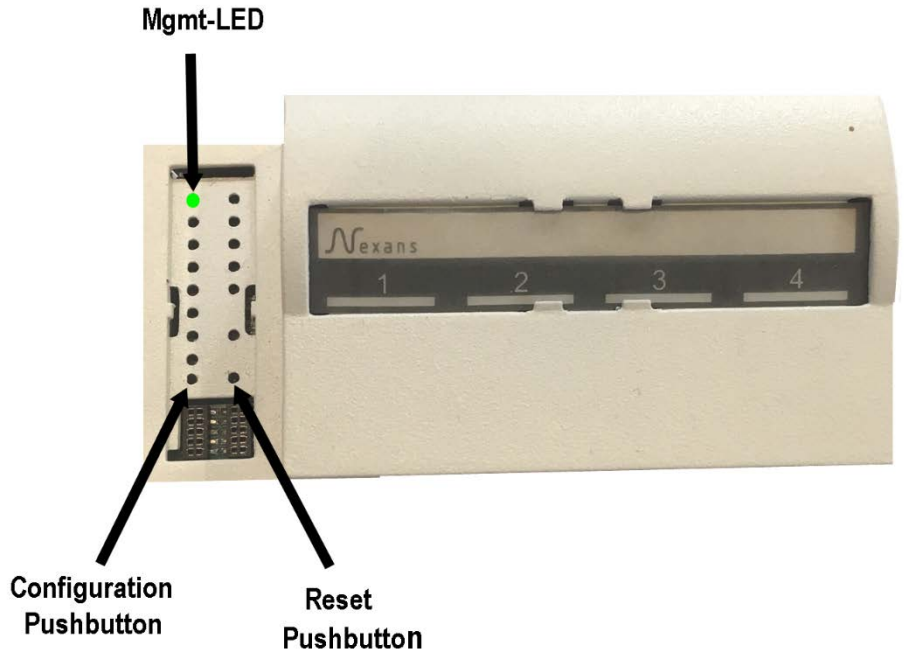
3.4.1. Configuration- and Reset-Button on Cable-Duct Switches 'GigaSwitch V3 / V5'

The pushbuttons are accessible after removing the LED cover plate. They can be operated using a thin pin, such as a bent-open paper clip.

GigaSwitch V3:



GigaSwitch V5:



These switchtyps have two pushbuttons:

- Configuration-Pushbutton
- Reset-Pushbutton

Configuration-Pushbutton:

IMPORTANT NOTE:
If features of the configuration pushbutton have been disabled via the management feature, please proceed as indicated in chapter *3.5. Disabling Configuration Switches*.

By pressing and holding the pushbutton (min. 3 seconds) the switch will change into the configuration mode, which is indicated by the Mgmt-LED going out. As soon as the Mgmt-LED is permanently off, the pushbutton must be released. A rapidly flashing blue Mgmt-LED shows that function number 1 has been selected.

By briefly pressing the pushbutton (min. 0.1 second) the desired function can now be selected, which is indicated via the respective LED colour:

Function	Colour	Boot function	See chapter
1	Blue	Booting with flash configuration	*3.6.1. Booting with Flash Configuration (Normal Mode)*
2	Red	Booting with fixed IP address	*3.6.2. Booting with Fixed IP Address*
3	White	Booting with factory default settings	*3.6.3. Booting with Factory Default Settings*
4	Cyan	Booting with Customer-Default settings	*3.6.5 Booting with Customer Default Settings*
5	Magenta	Booting without Customer-Reboot setting	*3.6.6 Booting without Customer Reboot Settings*

In order to execute the selected function, the pushbutton must be pressed and held for at least 3 seconds. The Status-LED flashes briefly and goes out to show that the switch has accepted the command. Now the pushbutton can be released, and the switch will boot to execute the command.

NOTE:

The configuration mode is automatically exited, when the pushbutton is not pressed for more than 30 seconds.

NOTE:

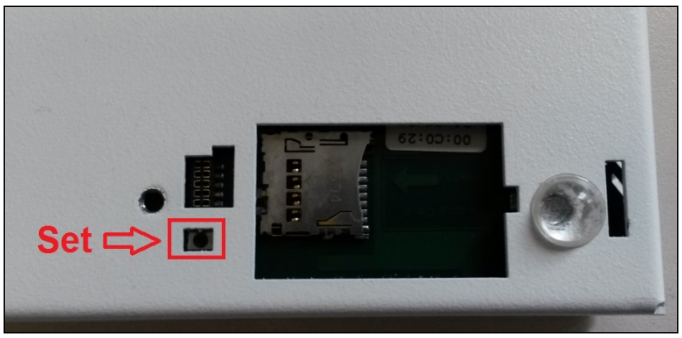
The functions four and five are only displayed if the respective configuration is stored.

Reset-Pushbutton:

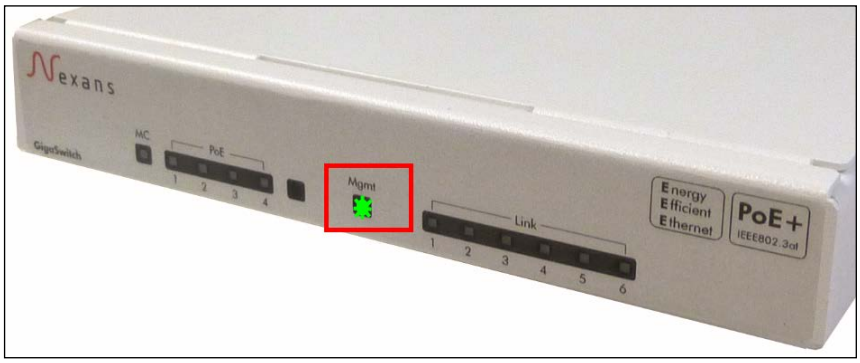
By pressing the Reset- and Configuration-Button simultaneously a hardware reset of the switch is executed.

3.4.2. Configuration Pushbutton on Desk Switches of type 'GigaSwitch Desk V3 / V5'

On Desk switches of type **GigaSwitch 64X** the management module is not accessible via the outside. Therefore, this switchtype has a configuration pushbutton behind a small cap at the bottom side.



The Managment LED is visible at the front side:



IMPORTANT NOTE:
If features of the configuration pushbutton have been disabled via the management feature, please proceed as indicated in chapter *3.5. Disabling Configuration Switches*.

By pressing and holding the pushbutton (min. 3 seconds) the switch will change into the configuration mode, which is indicated by the Mgmt-LED going out. As soon as the Mgmt-LED is permanently off, the pushbutton must be released. A rapidly flashing blue Mgmt-LED shows that function number 1 has been selected.

By briefly pressing the pushbutton (min. 0.1 second) the desired function can now be selected, which is indicated via the respective LED colour:

Function	Colour	Boot function	See chapter
1	Blue	Booting with flash configuration	*3.6.1. Booting with Flash Configuration (Normal Mode)*
2	Red	Booting with fixed IP address	*3.6.2. Booting with Fixed IP Address*
3	White	Booting with factory default settings	*3.6.3. Booting with Factory Default Settings*
4	Cyan	Booting with Customer-Default settings	*3.6.5 Booting with Customer Default Settings*
5	Magenta	Booting without Customer-Reboot setting	*3.6.6 Booting without Customer Reboot Settings*

In order to execute the selected function, the pushbutton must be pressed and held for at least 3 seconds. The Status-LED flashes briefly and goes out to show that the switch has accepted the command. Now the pushbutton can be released, and the switch will boot to execute the command.

NOTE:

The configuration mode is automatically exited, when the pushbutton is not pressed for more than 30 seconds.

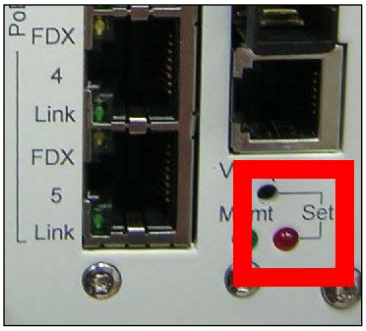
NOTE:

The functions four and five are only displayed if the respective configuration is stored.

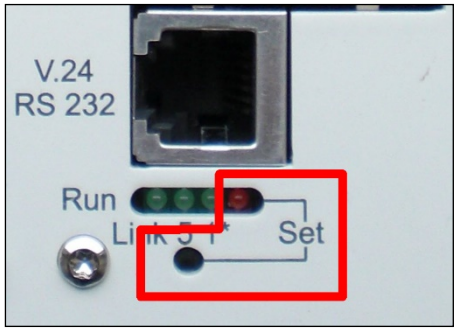
3.4.3. Configuration Pushbutton on Industrial Switches of type 54x, 74x and 104x

With industrial switches the configuration switch is located in the lower right corner of the front panel and is marked with 'Set':

iSwitch:

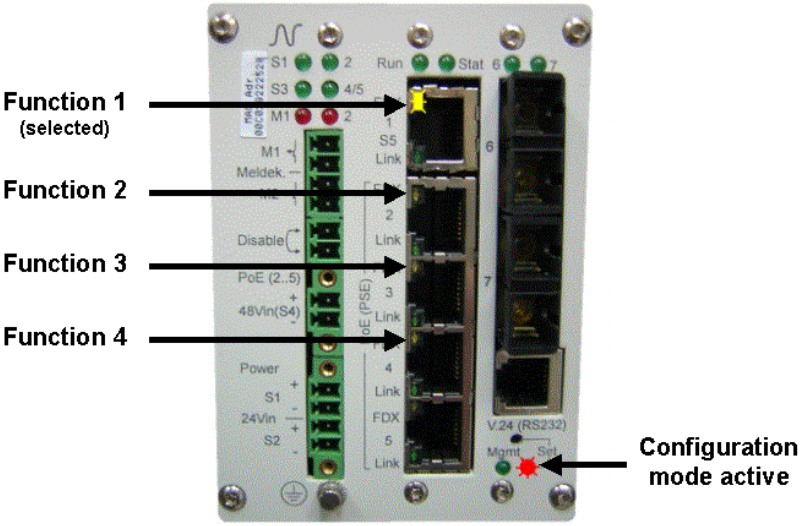


iGigaSwitch:



The configuration pushbutton can be accessed via a small hole in the front panel. The pushbutton can be operated using a thin pin, such as a bent-open paper clip.

By pressing and holding the pushbutton (min. 3 seconds) the switch will change into the configuration mode, which is indicated by the red LED. As soon as the Status-LED lights up, the pushbutton must be released again. The yellow LED of TP socket 1 now shows that Function 1 is selected:



By briefly pressing the pushbutton (min. 0.1 second, max. 2 seconds) the desired function can be selected, which is indicated via the respective yellow LED of the TP sockets:

Function	LED	Boot function	See chapter
1	TP1	Booting with flash configuration	*3.6.1. Booting with Flash Configuration (Normal Mode)*
2	TP2	Booting with fixed IP address	*3.6.2. Booting with Fixed IP Address*
3	TP3	Booting with factory default settings	*3.6.3. Booting with Factory Default Settings*
4	TP4	Booting with factory default settings and fixed IP address	*3.6.4. Booting with Factory Default Settings and Fixed IP Address*
5	TP1 + TP2	Booting with Customer-Default settings	*3.6.5 Booting with Customer Default Settings*
6	TP3 + TP4	Booting without Customer-Reboot settings	*3.6.6 Booting without Customer Reboot Settings*
Hardware Reset	-	By pressing and holding the pushbutton for more than 30 seconds	

		a hardware reset of the switch is initiated, which is followed by a booting operation with flash configuration. NOTE: This hardware reset is not supported for switches of type 'iGigaSwitch'.	

In order to execute the selected function, the pushbutton must be pressed and held for at least 3 seconds. The Set LED flashes briefly and goes out to show that the switch has accepted the command. Now the pushbutton can be released, and the switch will boot to execute the command.

NOTE:

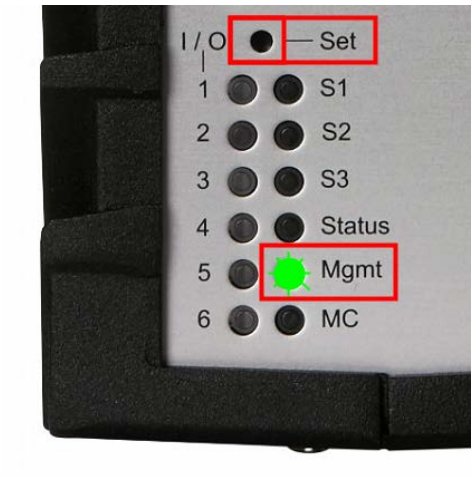
The configuration mode is automatically exited, when the pushbutton is not pressed for more than 30 seconds. In this case the red Status-LED will go out and the yellow LEDs show their normal functionality.

NOTE:

The functions five and six are only displayed if the respective configuration is stored.

3.4.4. Configuration Pushbutton on Industrial Switches of type 100x and 16XX

On industrial switches of type iGigaSwitch 100X and iGigaSwitch 160X the management module is not accessible via the bottom side. Therefore, this switchtype has a configuration pushbutton on the front side and is marked ‘Set’. The pushbutton can be operated using a thin pin, such as a bent-open paper clip:



IMPORTANT NOTE:

If features of the configuration pushbutton have been disabled via the management feature, please proceed as indicated in chapter *3.5. Disabling Configuration Switches*.

By pressing and holding the pushbutton (min. 3 seconds) the switch will change into the configuration mode, which is indicated by the Mgmt-LED going out. As soon as the Mgmt-LED is permanently off, the pushbutton must be released. A rapidly flashing blue Mgmt-LED shows that function number 1 has been selected.

By briefly pressing the pushbutton (min. 0.1 second) the desired function can now be selected, which is indicated via the respective LED colour:

Function	Colour	Boot function	See chapter
1	Blue	Booting with flash configuration	*3.6.1. Booting with Flash Configuration (Normal Mode)*
2	Red	Booting with fixed IP address	*3.6.2. Booting with Fixed IP Address*
3	White	Booting with factory default settings	*3.6.3. Booting with Factory Default Settings*
4	Cyan	Booting with Customer-Default settings	*3.6.5 Booting with Customer Default Settings*
5	Magenta	Booting without Customer-Reboot setting	*3.6.6 Booting without Customer Reboot Settings*

In order to execute the selected function, the pushbutton must be pressed and held for at least 3 seconds. The Status-LED flashes briefly and goes out to show that the switch has accepted the command. Now the pushbutton can be released, and the switch will boot to execute the command.

NOTE:

The configuration mode is automatically exited, when the pushbutton is not pressed for more than 30 seconds.

NOTE:

The functions four and five are only displayed if the respective configuration is stored.

3.5. Disabling Configuration Switches

The boot functions ‘Booting with fixed IP Address’ and ‘Booting with Factory Default Settings’ can be individually disabled via the management feature to prevent an accidental or deliberate manipulation by the user.

For each switch the following settings are possible:

- Enabled factory default, the corresponding switch is enabled
- Disabled the corresponding switch is disabled and without function

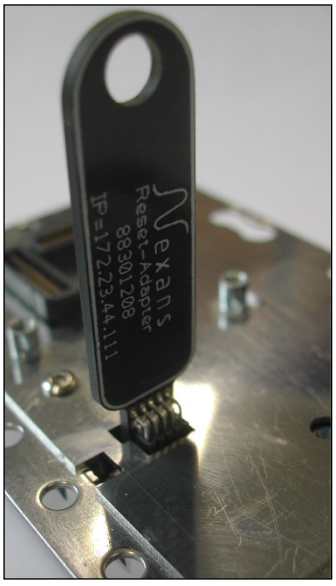
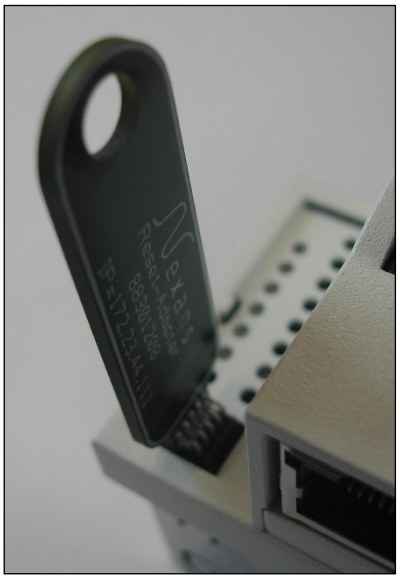
After disabling the switch "Boot with factory default settings", a reset of the switch to factory default settings is only possible via management access (if name and password are known for the Admin Account). If no access is possible via the management feature, e.g. because name or password are unknown or the VLANs are configured wrongly, the switch can nevertheless be reset via a special reset plug. This plug can be ordered under part number 88301208 from Nexans.

NOTE:
A connected reset plug will only be detected during the booting of the switch. Thus, any disconnecting or connecting of the plug during the operation of the switch will not have any immediate effect.

NOTE:
On Desk switches of type **GigaSwitch 54X** the management module is integrated into the switch and not accessible from outside. Therefore, a reset via reset plug is only possible after opening the housing of the switch.

NOTE:
On Desk switches of type **GigaSwitch 64X** the management module is not accessible via the outside. The management module is behind a small cap at the bottom side.

In case of disabled configuration switches please proceed as follows to reset to factory defaults:

1	**Connect the reset plug.** The reset plug should be plugged into the management module or GigaSwitch V3 as shown in the below picture. **IMPORTANT:** Do not in any case use force here. Instead you should use the following picture to check the correct position:  Mgmt module HW0-HW3  GigaSwitch V3  GigaSwitch Desk
2	**Reboot the switch in one of the following ways.** • Remove the mains plug briefly and insert it again. • Alternatively, for cable-duct switches: - On GigaSwitch V3 press the Reset- and Configuration-Pushbuttons simultaneously - RJ45 adapter WITHOUT switch: Remove the RJ45 adapter and insert it again. - RJ45 adapter WITH switch: Set the switch from the ON position briefly into the Reset/Standby position.

3	**Check, if switch has booted correctly.** See notes on the function of the Status-LED in chapter *3.3. Management Status-LED*
4	**Remove the reset plug.**
5	**Reboot the switch in one of the following ways.** • Remove the mains plug briefly and insert it again. • Alternatively for cable-duct switches: - On GigaSwitch V3 press the Reset- and Configuration-Pushbuttons simultaneously - RJ45 adapter WITHOUT switch: Remove the RJ45 adapter and insert it again. - RJ45 adapter WITH switch: Set the switch from the ON position briefly into the Reset/Standby position.

3.6. Management Operation Modes

By factory default the operation mode is configured to 'Booting with Flash Configuration'.

3.6.1. Booting with Flash Configuration (Normal Mode)

With this function the switch will boot in the normal operating mode. All configuration settings saved in flash will be applied. If a Customer Reboot configuration is available, the current configuration will be overwritten with the reboot configuration parameters.

This is the delivery condition. This configuration should only be used in exceptional cases, e. g. for commissioning or for resetting to factory default.

3.6.2. Booting with Fixed IP Address

This function will enable the following temporary IP settings:
- IP address 172.23.44.111
- Network mask255.255.255.0
- MAC address 00:C0:29:01:FF:FF

The switch can then be accessed via this temporary IP address in order to configure the required switch parameters (e. g. the IP address).

NOTE:
The Nexans Basic Configurator should be preferred for configuring the IP address (see chapter *5.1.Configuration of the IP Address using Nexans Basic Configurator*).

The operating mode with fixed IP address, as described here, is only required, if:
- The Nexans Basic Configurator is not available

or
- the Admin name and password have been changed

or
- switch port TP1 and the management are set to different VLANs.

In addition to the IP parameters the following temporary switch settings are made:
- All ports in the same VLAN
- Trunking disabled for all ports
- Admin state disabled for all ports
- Link Setup set to Autonegotiation / Autocrossover for all ports
- Portsecurity disabled for all ports
- Rapid Spanning Tree global disabled

The above settings ensure that the switch can be accessed via any port using the fixed IP address 172.23.44.111.

Moreover the IP, Link, VLAN, trunking and Portsecurity settings can be made without these settings taking immediate effect. Only after a {Booting with Flash Configuration} the stored configurations will be enabled.

Moreover the fixed IP address can be used to check the configuration of the switch (e.g. if the switch cannot be accessed via the expected IP address because of badly configured VLANs etc.).

In order to be able to access the management module via a PC, a routing entry must be added in the PC for address 172.23.44.111.
Example: For a PC with IP address 100.10.10.1 the command is:

```
route add 172.23.44.111 100.10.10.1
```

If you would like to retain this routing entry also after a reboot of the PC, you can add the option '-p':

```
route add 172.23.44.111 100.10.10.1 -p
```

Alternatively the PC can also be set to an IP address in the 172.23.44.x range (except 172.23.44.111) and the network mask can be set to 255.255.255.0 (in this case no routing entry is required). A specific gateway IP address is not required and would not have any effect.

NOTE:
The fixed MAC address allows you to configure several switches one after the other without having to clear the PC's ARP cache.

IMPORTANT:
Only one switch may be operated at a time in the network with fixed IP address, because otherwise address conflicts would occur.

3.6.3. Booting with Factory Default Settings

In this case ALL settings stored in the flash memory will be overwritten with factory default values. Afterwards the normal operating mode will be activated.

3.6.4. Booting with Factory Default Settings and Fixed IP Address

In this case ALL settings stored in the flash memory will be overwritten with factory default values. Afterwards the function {Booting with fixed IP Address} will be executed (see above chapter *3.6.2. Booting with Fixed IP Address*

3.6.5. Booting with Customer Default Settings

This option will boot the switch using the defined Customer Configuration. In this case all parameters are set to Factory Default and then the Customer Configuration parameters are loaded.

3.6.6. Booting without Customer Reboot Settings

If a Reboot Configuration is available, this option will perform a reboot without overwriting the current configuration with the Reboot Configuration parameters.

4. Memory Card (MC)

The optional use of a memory card (MC) is supported by industrial and office switches.

The memory card stores the following Switch specific information:

- MRP License (optional, only for Industrial-Switches with Redundancy protocol MRP)
- Switch-Configuration (from Firmware-Version V4.11ao with AES-256 Encryption)
- Firmware-Update (from Firmware-Version V4.11df)

The respective cards are available from Nexans as accessory parts. Four versions are available:

- Memory Card for Office Switch with MAC Addr. Part–Nr. 88300691
- Memory Card for Office Switch with MAC Addr. integrated Part–Nr. 88300693
- SD Memory Card for i-Series with MAC Addr. Part–Nr. 88300692
- SD Memory Card for i-Series with MAC Addr. integrated Part–Nr. 88300696
- SD Memory Card for i-Series with MAC Addr. and MRP-Multiple licence Part–Nr. 88300694

NOTE:

Only the above listed memory cards can be used since these are specified for the extended temperature range. In the computer trade available cards, which mostly have a limited temperature range, are not accepted by the switch.

NOTE:

Integrated means, that the Memory Card is clicked in by default.

4.1. Memory Card Write-Protection on HW5 Industrial Switches

On HW5 industrial switches the MC can be write-protected by the DIP switch F2 at the front of the switch. If the DIP switch is turned on while booting (switch position “On”), write-protection is avtivated. I.e. the current switch configuration and new firmware updates are not stored on MC. Memory Card write-protection is indicated by a blue lighting MC LED.

NOTE:

Toggling DIP switch F2 during running operation has no impact on write-protection of the MC.

NOTE:

The write-protection cannot be turned on or off by the lock switch at the edge of the MC.

4.2. Memory Card MAC-Address

The version with MAC address has its own unique MAC address stored on the MC at the factory. The address is also imprinted onto the card. If a switch is booted with such an MC, the MAC address of the MC is used instead of the MAC address of the switch. That means that, when the switch is replaced, the MAC address of the switch will be retained so that existing DHCP server entries, if any, can be kept unchanged.

IMPORTANT NOTE:

The MAC address of the MC is only read when booting the switch. This means that while a hot-plugged MC will be detected, the MAC address will only be displayed and become effective after the next rebooting.

4.3. Memory Card MRP License

Switches that support the redundancy protocol MRP require an MRP license up to and including firmware version V5.03go. To activate MRP, a corresponding memory card with an MRP license must be present in the switch.
From firmware version V5.03gp MRP can also be activated without a corresponding memory card, since the MRP patent expired in May 2019.

4.4. Memory Card Switch-Configuration

The memory card allows the redundant storage of the complete switch configuration. As soon as the card is inserted the configuration stored on the MC is kept consistent with the configuration stored in the internal flash of the switch. If a switch needs to be replaced, you only need to take the MC from the old switch and insert it into the new switch. During power-up the configuration will then be read from the MC and transferred into the internal flash of the switch.

By default, the local passwords are saved on the MC using a proprietary encryption procedure. To better protect these passwords, the Password Encryption Mode should be set to “SHA1 hash”. If the access policy is set to “Allow secure protocols and strong passwords only”, the Password Encryption Mode is fixed to “SHA1 hash”.

With this setting the passwords of the two local accounts are exclusively saved as an SHA1 hash. If the passwords are sufficiently complex (at least 8 characters, recommended: 12 characters), it is practically impossible to discover the password in case the Memory Card and the hash value are compromised.

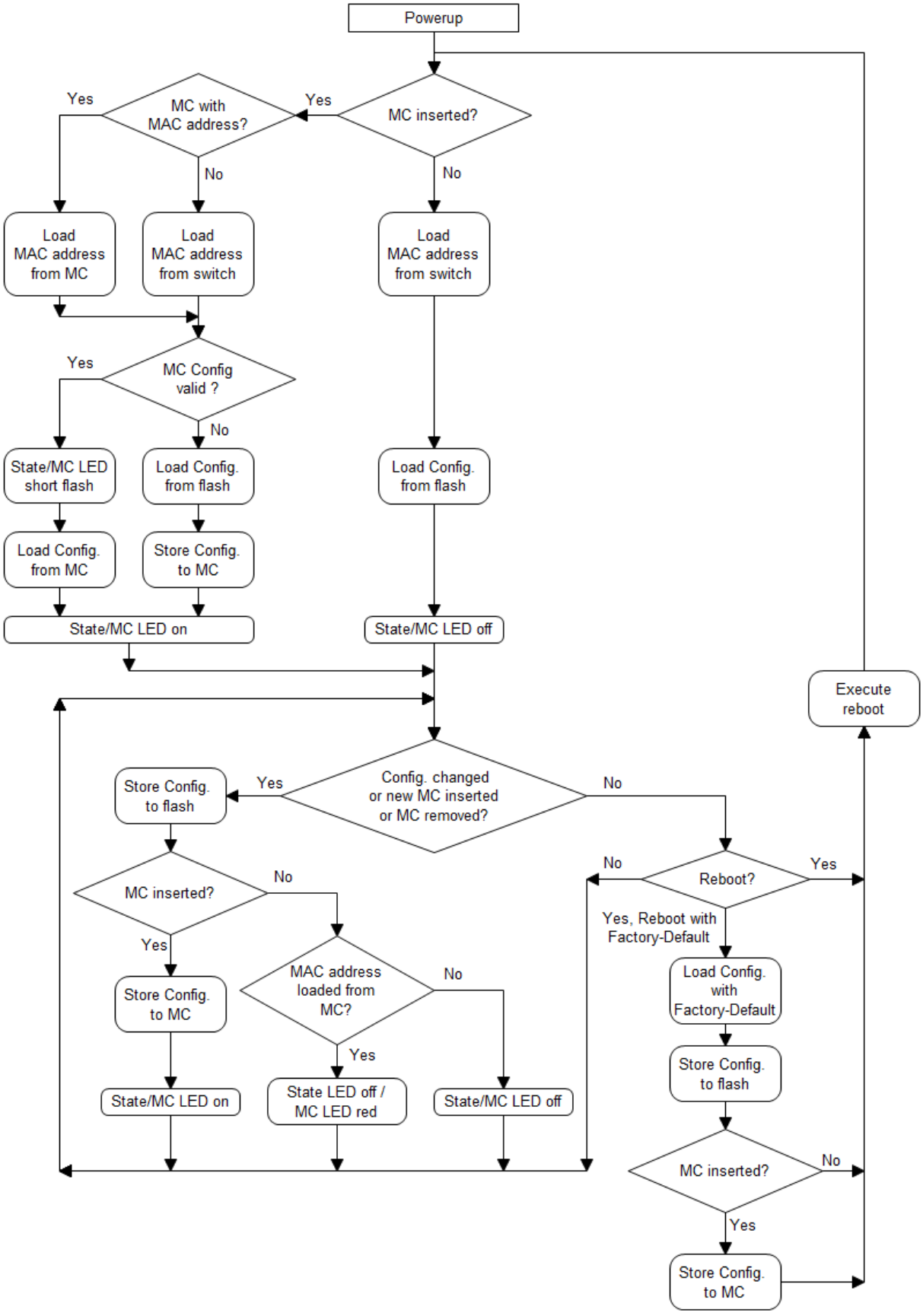
NOTE:

From firmware version V4.11ac the complete switch configuration is saved on the MC using an AES-256 encryption. This prevents the switch configuration from being read by SD card readers.

IMPORTANT NOTE:

Switches with a Firmware older then 4.11ac are not able to read the encrypted switch configuration that is stored on the MC.

The loading and storage of the switch configuration (with or without MC) is illustrated in the below flowchart:

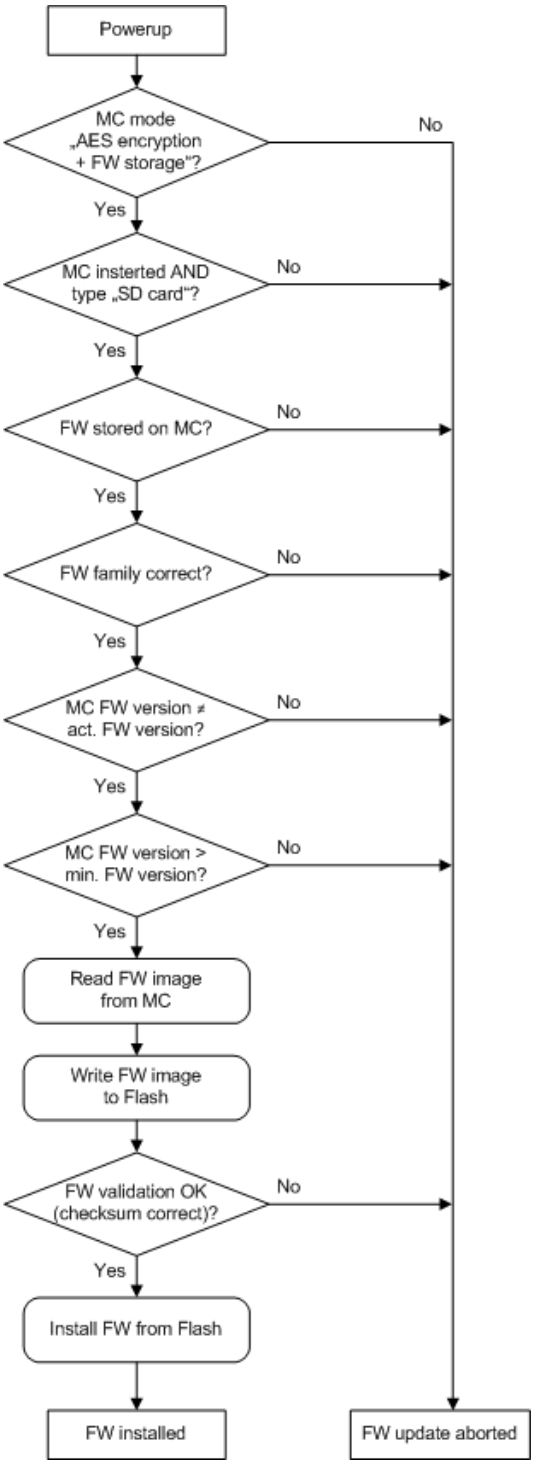


4.5. Memory Card Firmware-Update

From firmware version V4.11df the firmware file is redundantly stored on the MC during a firmware update (see section 4.6 Memory Card Mode).

If an MC is plugged in during the firmware update, the firmware file will be stored in the internal flash of the switch and on the MC.

If an MC with a stored firmware is plugged in during rebooting, the firmware version will be checked and compared with the currently installed version. If the firmware version on the MC is different from the currently installed version, the installation of the firmware (FW) from the MC will be initiated:



NOTE:

The firmware stored on MC can be deleted with reset command „Reset Firmware on Memory Card" (see chapter *9.3 Reset Commands*).

4.6. Memory Card Mode

The Memory Card Mode allows you to disable the memory card features. The following settings are available:

- Enabled
- Enabled with AES-256 encryption
- Enabled with AES-256 encryption and Firmware storage
- Disabled
- Permanently Disabled

Enabled:
This is the factory default. In this mode the memory card function is enabled.

Enabled with AES-256 encryption:

The Memory Card (MC) function is active. The switch configuration is encrypted with AES-256 encryption before being stored on the MC. An encrypted configuration stored on the MC can be read, even if the Memory Card Mode is not set.

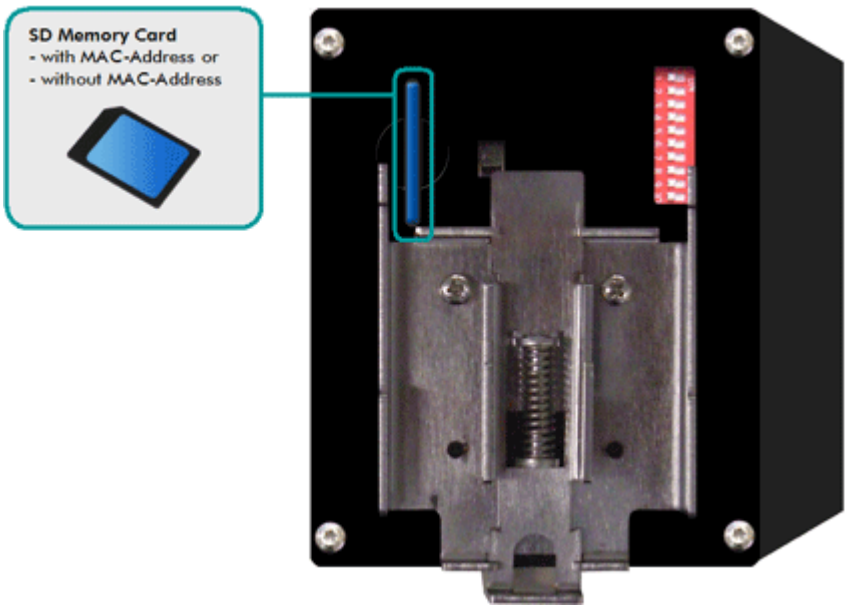
Enabled with AES-256 encryption and Firmware storage:

The Memory Card (MC) function is active. In addition to storing the configuration during a firmware update the firmware file is stored in flash memory and on the MC.

Disabled:
If the Memory Card Mode is set to „Disabled“, the memory card function is disabled.

Permanently Disabled:
Selecting this mode will irrevocably disable the memory card function. It is not possible to re-enable it. Resetting the switch to its factory default settings has no influence on this mode, either. In order to be able to use the memory card function again, the switch must be returned to Nexans ANS. Please contact our support at www.nexans-ans.de/support.

4.7. Memory Card on Industrial Switches of types ‘iSwitch 74X / 104X’

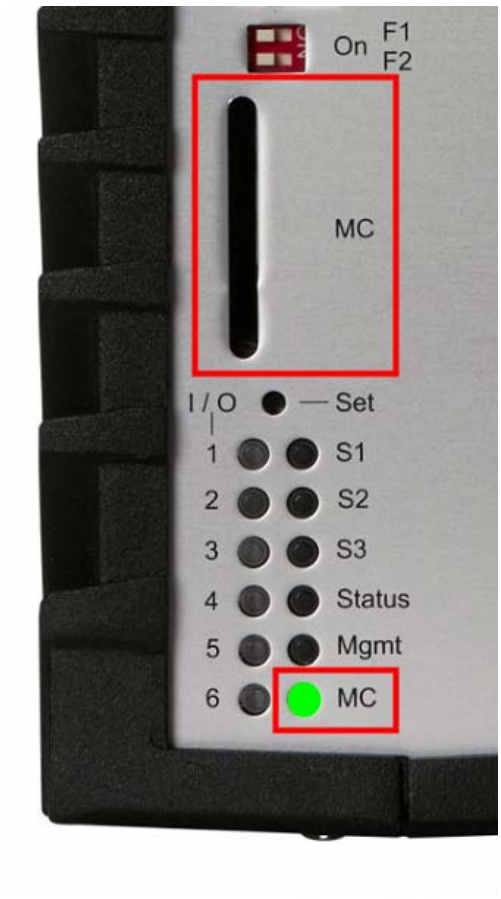


The green LED marked ‘State’ on the front panel indicates whether or not a valid MC is inserted. Moreover, the state is indicated on the Info page in WEB, Telnet and NEXMAN.

If the switch is booted with an inserted memory card which contains a valid switch configuration, the 'State' LED flashes shortly during the boot procedure. After the configuration of the memory card has been completely loaded, the 'State' LED lights up permanently.

Furthermore, if the MC card is removed during runtime, the ‘'State' LED turns off.

4.8. Memory Card on Cable-Duct Switches of type 'iSwitch 100X / 16xx'



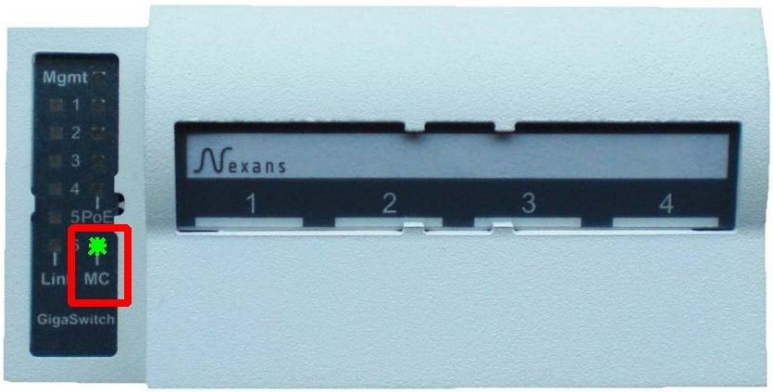
The multicolour ‘MC’ LED on the front panel shows if a valid MC has been plugged in. Additionally, the status can be accessed on the Info page in WEB, Telnet, SSH and NEXMAN.

If the switch is booted with a plugged-in MC card having a valid switch configuration, the ‘MC’ LED will light up in blue for some seconds during booting. When the loading of the configuration of the MC card is completed, the ‘MC’ LED lights up permanently in green.

If the MC card is removed during runtime and the MAC address has been loaded from MC card on powerup, the ‘MC’ LED lights up in red. Otherwise the ‘MC’ LED turns off.

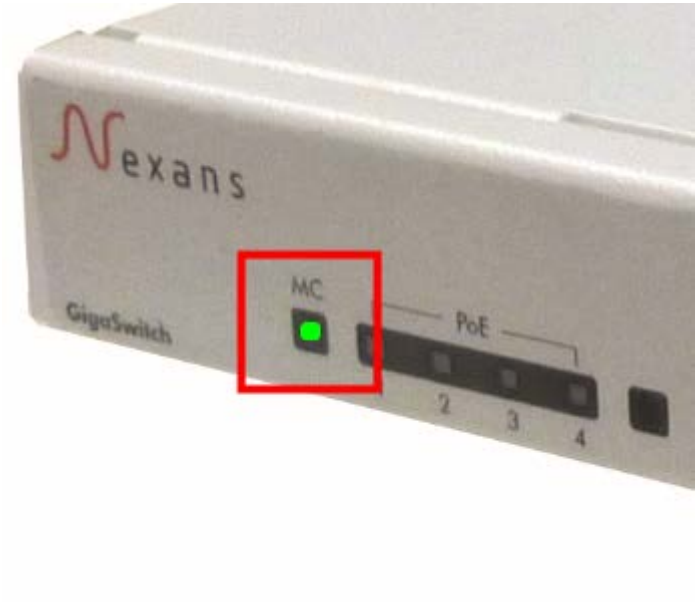
4.9. Memory Card on Cable-Duct Switches of type 'GigaSwitch V3 / V5'

GigaSwitch V3:



GigaSwitch V5:

GigaSwitch V3 / V5 Desk:



The multicolour ‘MC’ LED on the front panel shows if a valid MC has been plugged in. Additionally, the status can be accessed on the Info page in WEB, Telnet, SSH and NEXMAN.

If the switch is booted with a plugged-in MC card having a valid switch configuration, the ‘MC’ LED will light up in blue for some seconds during booting. When the loading of the configuration of the MC card is completed, the ‘MC’ LED lights up permanently in green.

If the MC card is removed during runtime and the MAC address has been loaded from MC card on powerup, the ‘MC’ LED lights up in red. Otherwise the ‘MC’ LED turns off.

5. IP Address Configuration

The IP address can be configured in four different ways:
- via Nexans Basic Configurator
- via V.24 Console interface
- via DHCP
- via configuration switches

By factory default the switch is set to DHCP and thus can receive its basic configuration directly from a DHCP server (see chapter *5.3. IP Address Configuration via DHCP*, *5.4. Setting the switch name using DHCP* and 7.2.5 *Loading Switch Configuration automatically via DHCP/BootP*).

5.1. Configuration of the IP Address using Nexans Basic Configurator

IMPORTANT: Detailed information on performing the configuration using Nexans Basic Configurator or Nexans Device Manager can be found in the corresponding manual.

Nexans Basic Configurator is part of Nexans Device Manager (NEXMAN). It provides the basic configuration of the switch and includes the following parameters:
- Switch description (name, location, contact)
- IP parameters (DHCP, IP address, netmask, gateway)
- Trunk uplink parameters (trunk port, mgmt VLAN-ID)

Nexans Basic Configurator supports two different operating modes:

- **(Local Mode):**
The (Local Mode) has been designed for the local on-site configuration of the switch parameters. This requires the PC to be directly connected via the network cable with the first Twisted Pair port (TP1) of the switch.

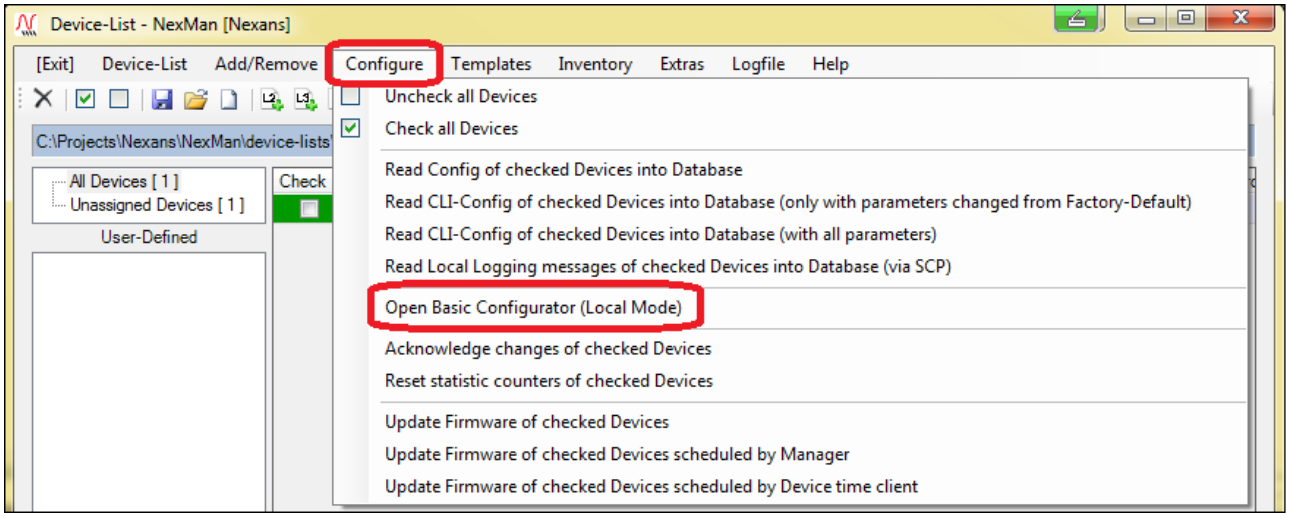
- **(MAC Address Mode):**
The (MAC Address Mode) has been designed for the centralized configuration of the switch parameters within the NEXMAN 'Autodiscover Devices on local segments (Layer-2)' feature and consequently can only be called from NEXMAN.

After completion of the basic settings via the Basic Configurator any further configuration can be executed via the Device-List of the Nexans Device Manager (NEXMAN).

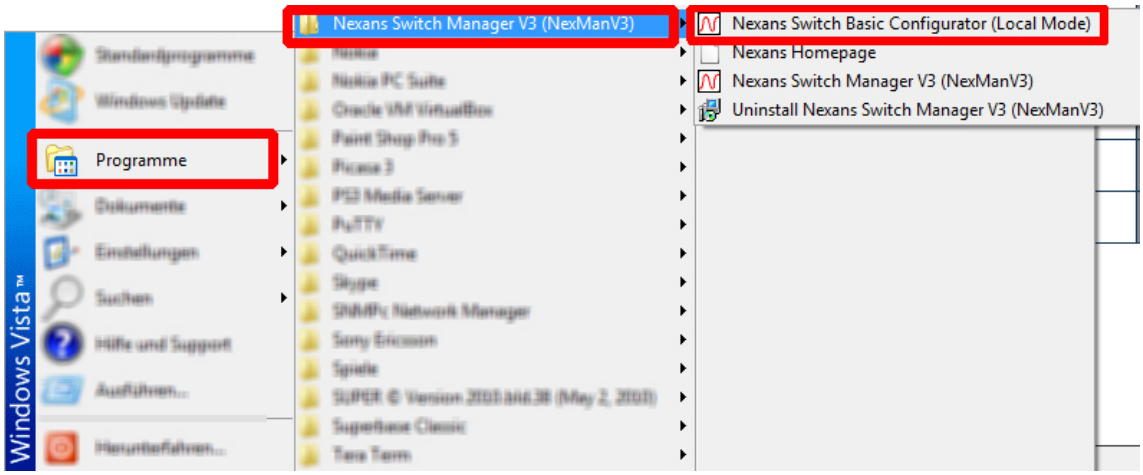
5.1.1. Starting Basic Configurator (Local Mode)

Starting in (Local Mode) can be performed in two ways:

- Within NEXMAN via the **Configure > Open Basic Configurator (Local Mode)** menu:



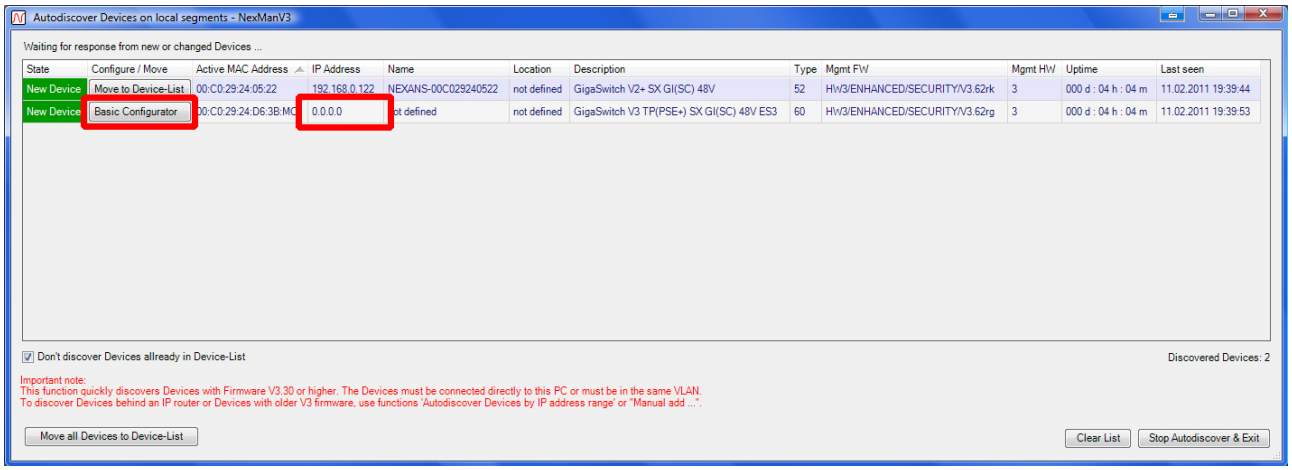
• Via the Windows start menu:



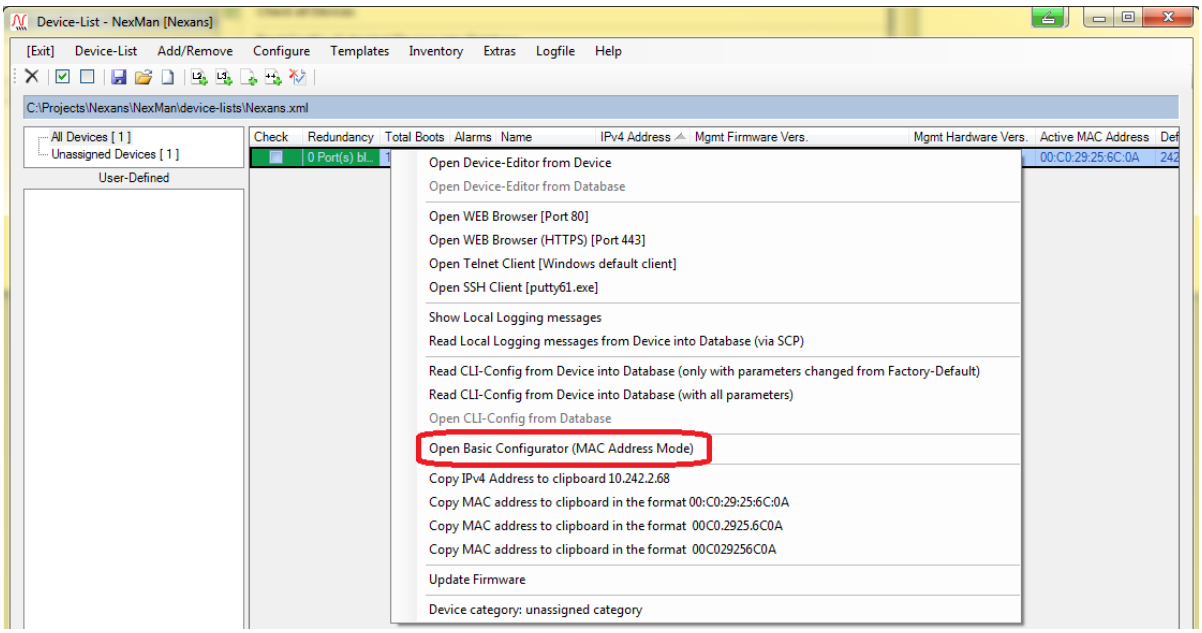
5.1.2. Starting Basic Configurator in (MAC Address Mode)

Starting in (MAC Address Mode) can be performed in two ways:

• Within NEXMAN via the menu option
Add/Remove > Autodiscover Devices on local segments (Layer-2):



• Within NEXMAN by right-clicking onto the corresponding line of the switch and selecting the **Open Basic Configurator from Device (MAC Address Mode)** menu option:

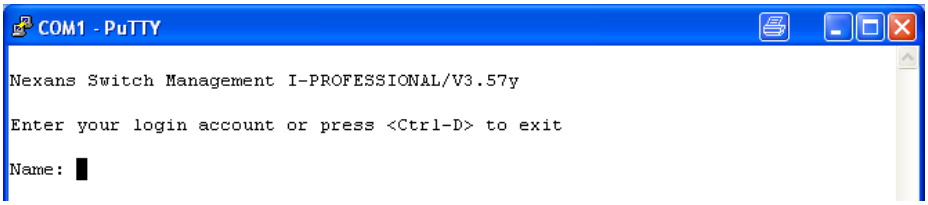
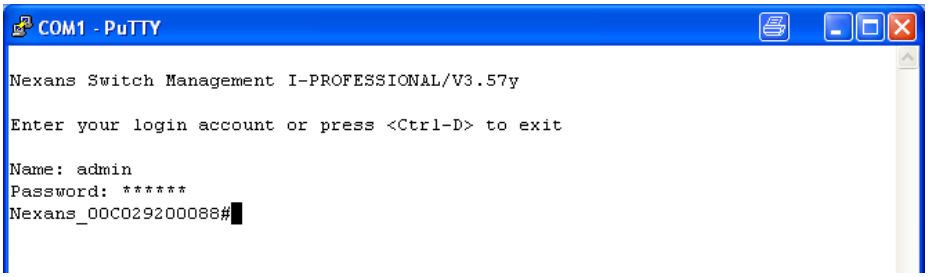


5.2. Configuration of the IP Address using V.24 console interface

Configuration of IP parameters via V.24 console interface is supported by industrial switches and desk switches of type 'GigaSwitch'. The installed firmware version must be release 3.10 or later.

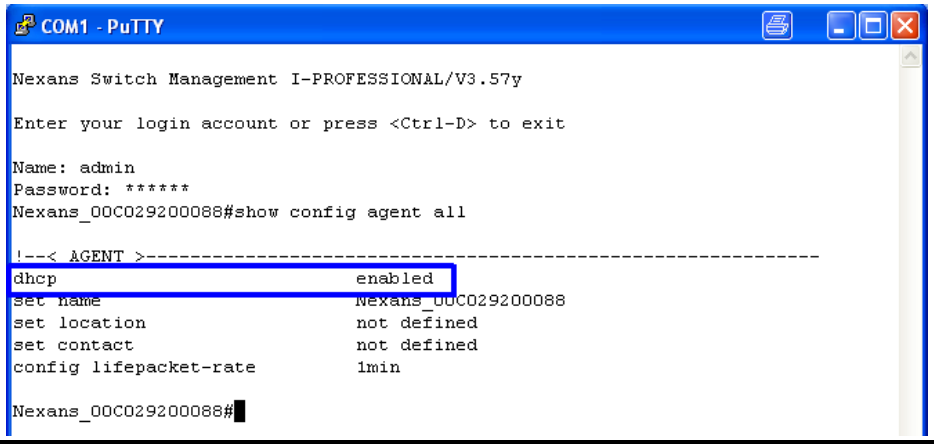
For this purpose, there is a RJ11 connector at the front panel of the switches which must be connected via a special adaption cable to a serial port of the configuration PC. A ready-to-use adaption cable is available from Nexans and must be ordered separately (Nexans order number 88300688).

You will find the pins assignment of the RJ11 connector and the transmission parameter in chapter *6.3. Switch Configuration via V.24* .

1	**Check, if the management Status-LED on the front panel of the Switch lights correctly** Notes on the function of the Status-LED see chapter *3.3 Management Status-LED*.
2	**Connect the RJ11 connector via the special adaption cable with the configuration PC** IMPORTANT: The above listed V.24 communication parameters must be correctly set.
3	**Start login mode by pressing the <Enter> key** 
4	**Enter the user name and password**  Enter 'admin' as the user name and 'nexans' as the password. This are the factory default settings.

5 **Display current IP settings**

Enter the console command '`show config agent all`':



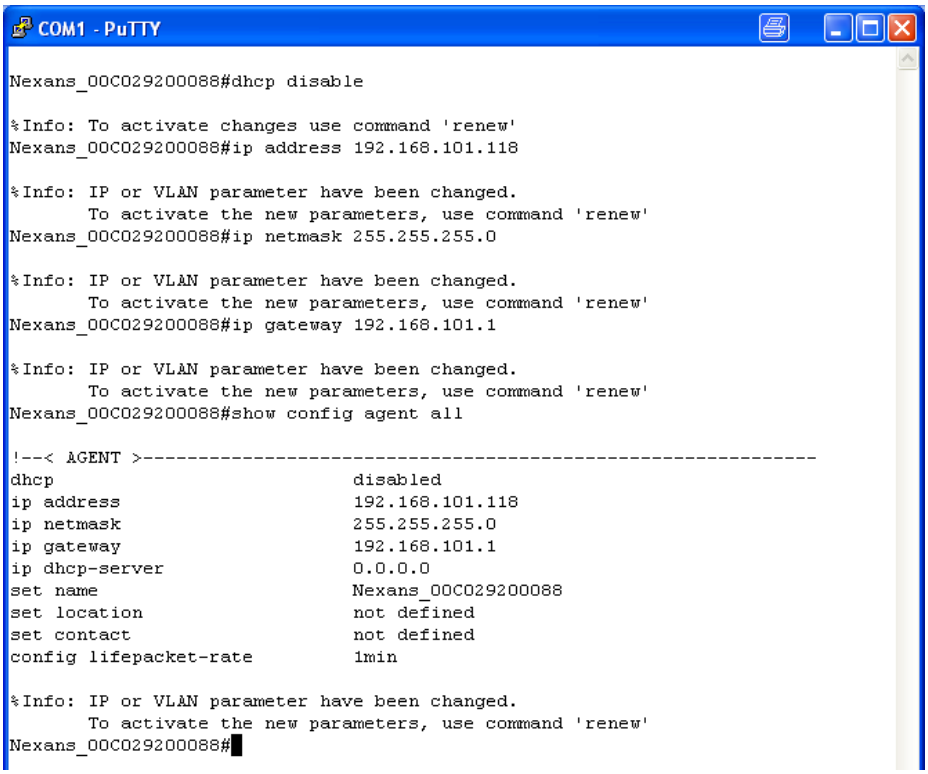
6 **Enter IP parameters**

The following console commands are available:

Disable DHCP:	dhcp disable
IP address:	ip address a.b.c.d
Network mask:	ip netmask a.b.c.d
Gateway:	ip gateway a.b.c.d

The fist command must always disable the DHCP. Then the other IP parameters can be edited.

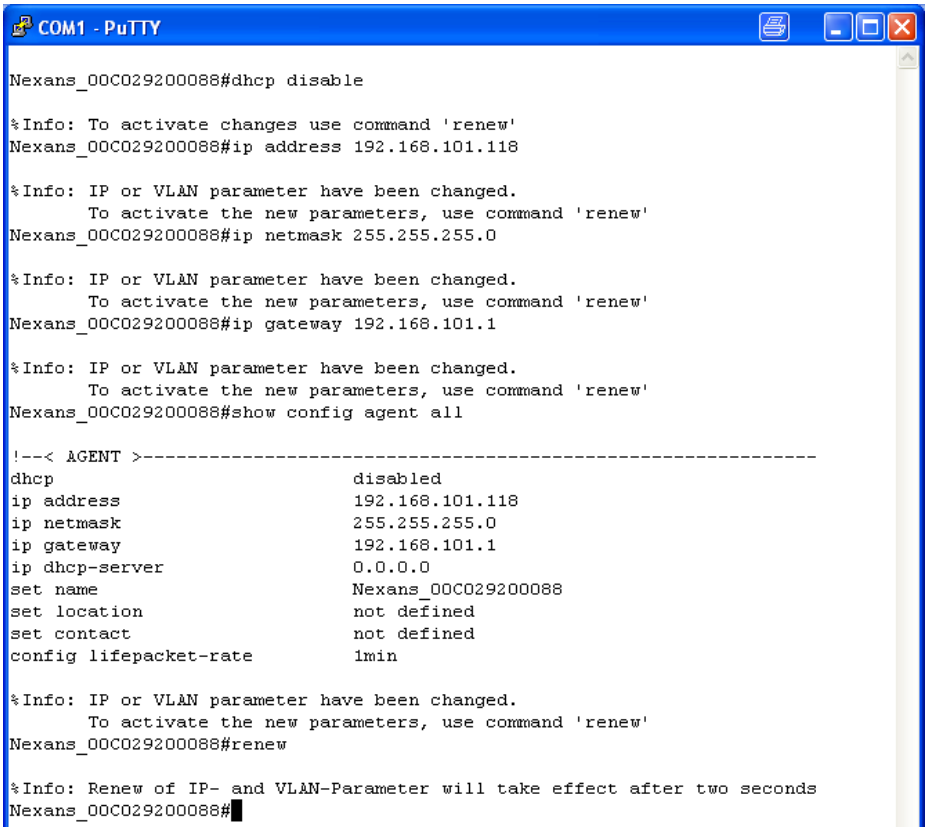
See the following example:



7 **Activating the new IP parameters**

Changes to the configuration of IP and VLAN parameters via RS233, Telnet, Web or SNMP do not take immediate effect, but only after execution of the command {Renew IP- and VLAN-Parameter}.

The corresponding console command is: `renew`



After executing this command the new IP parameters will take effect immediately without rebooting the switch.

5.3. IP Address Configuration via DHCP

For configuration through DHCP a DHCP server is required. The DHCP (Dynamic Host Configuration Protocol) automatically assigns IP addresses from a fixed IP address range to the switch, thus accelerating the configuration of larger networks. In addition to the IP address the switch also receives supplementary information such as the address of the gateway and the network mask.

If the Nexans switch needs to receive a fixed IP address, the MAC address of the switch has to be made known to the DHCP server and a fixed IP address to be entered for this MAC address.

Due to the high number of different DHCP servers it is not possible to explain the procedure for configuring the server here, so the network administrator should be contacted for any such matters.

The MAC address of switch required for the DHCP server can be found on the type plate of the system or (for cable-duct modules) underneath the RJ-45 adapter (remove the adapter):

`00 C0 29 __ __ __` (12 characters)

The switch sends a DHCP request as soon as the Status-LED lights up permanently on the management module. If it receives a valid response from a DHCP server, the IP parameters are accepted, and the management module can be immediately accessed via the assigned IP address. If the switch does not get a response, the DHCP request is repeated at increasing time intervals (with a maximum interval of approx. 30 seconds).

A Ping command, for example, can be executed as a simple connectivity test. When the module can be addressed via the assigned IP address, the DHCP function may be disabled, if desired and further changes can be made to the IP parameters via WEB, Telnet, SNMP or NEXMAN, if necessary.

DHCP is the factory default setting of the management module. All IP parameters of the last successful DHCP Acknowledge will be stored in flash (including the DHCP server IP address). After a reboot or power-up the system will first try to obtain the IP parameters via DHCP Request from the stored DHCP server. Only after three unsuccessful attempts or after a Factory Default Reset a DHCP Discover is executed.

Depending on the Lease Time value in the DHCP Acknowledge the Nexans switch transmits a new DHCP Request to confirm the IP Address at the DHCP server. The first DHCP Request will be sent after half the Lease Time and the switch will first try to obtain the IP parameters from the stored DHCP server. Only after three unsuccessful attempts a DHCP Discover will be executed to which all DHCP servers may respond. The DHCP Discover is repeated every 30 seconds until a DHCP server responds. After expiry of the complete Lease Time the previous IP address in the Nexans switch will be deleted. After each reception of a DHCP Acknowledge the Lease Time will be re-set in the switch, i.e. any change to the Lease Time on the DHCP server will be taken over with the next DHCP Request of the switch.

We recommend setting the Lease Time to a value of 10 days or more. This will guarantee that the switches can be reached also in case of a lengthy DHCP server failure (a Lease Time of 10 days would tolerate a DHCP server failure of a maximum of 5 days).

The following options are sent in the DHCP Discover or DHCP Request from the switch:

Option	Description	Comment
53	DHCP Message Type	Contains either “Discover” or “Request” as types.
60	Vendor Class Identifier	Contains the manufacturer and device type of the switch in the following format: 266:XXX 266 is the Nexans Private Enterprise number according to IANA (see http://www.iana.org/assignments/enterprise-numbers). XXX is the type of switch according to Chapter: *2.1 Supported Switch Types*
61	Client Identifier	The MAC address of the switch.
50	Requested IP Address	Is exclusively sent in the DHCP Request and contains the requested IP address. This address was previously transmitted by the DHCP server via DHCP Offer or DHCP Acknowledge.
54	DHCP Server Identifier	Is exclusively sent in the DHCP Request and contains the IP address of the requested DHCP server. This IP address was imported from the last valid DHCP server.
12	Host Name	The user-defined name of the switch. NOTE: If the DHCP server returns this option, the contained host name is taken as the switch name.

55	Parameter Request List	A list of information requested from the DHCP server. This list includes the following values: 1 Subnet Mask 3 Router IP 12 Host Name 66 TFTP Server Name 67 Bootfile Name

The following options in the DHCP server's DHCP Acknowledge are interpreted by the switch:

Option	Description	Comment
53	DHCP Message Type	Must contain either the type "Offer" or "Acknowledge".
12	Host Name	The transmitted host name is taken as the switch name.
66 67	TFTP Server Name Bootfile Name	If in Option 66 a valid IP address and in Option 67 a file name were transmitted, the switch will load the indicated file via the IP address per TFTP and execute it as a CLI script. For a detailed description of this function see Chapter *7.2.5 Loading Switch Configuration automatically via DHCP/BootP*

NOTE:
In the DHCP Discover and DHCP Request of the switch a host name is transmitted. The switch uses the switch name in these requests.

If the DHCP function has been disabled, it can be restored to the factory default setting via the configuration switches.

5.4. Setting the switch name using DHCP

As an option the name of the switch can be assigned via the 'Host Name' DHCP option 12. If this option is not included in the DHCP response from the server, the name of the switch is not changed.

5.5. IP Address Configuration via configuration switches

Setting the IP address by means of the configuration switches and of the function {Booting with fixed IP Address} is only required, if:

- the Nexans Basic Configurator V3 is not available

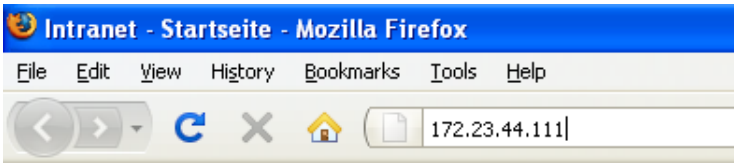
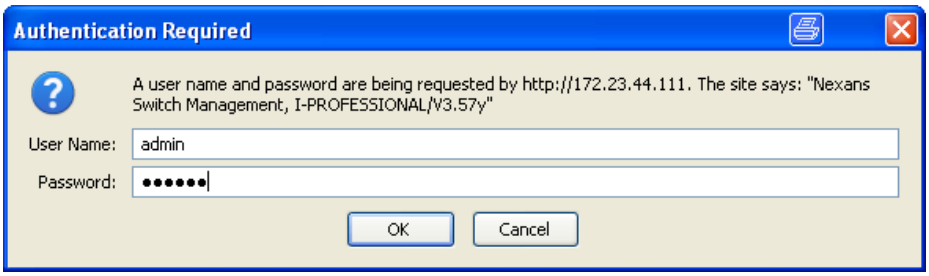
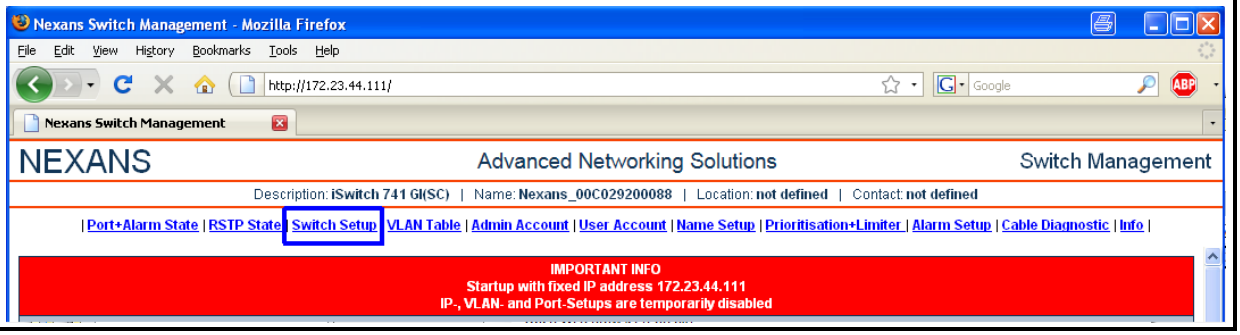
or

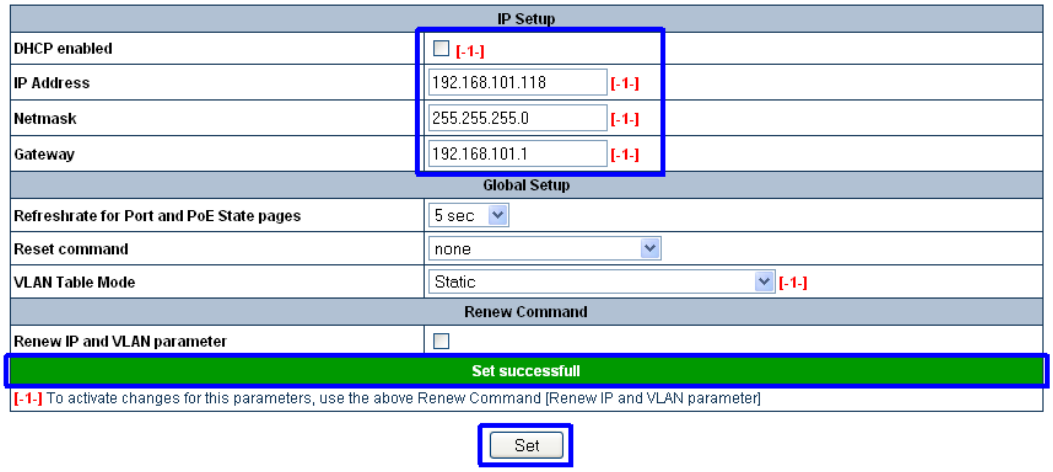
- the Admin name and password have been changed

or

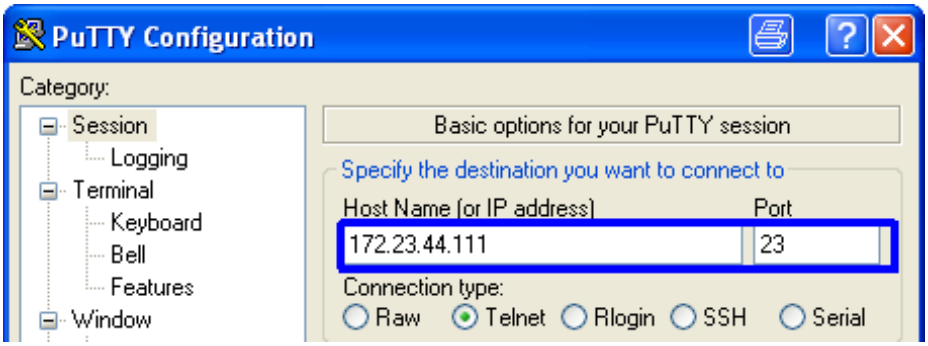
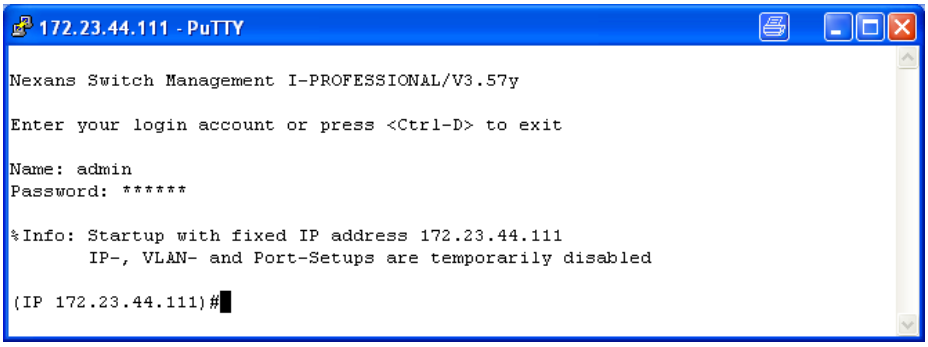
- switch port TP1 and the management are set to different VLANs.

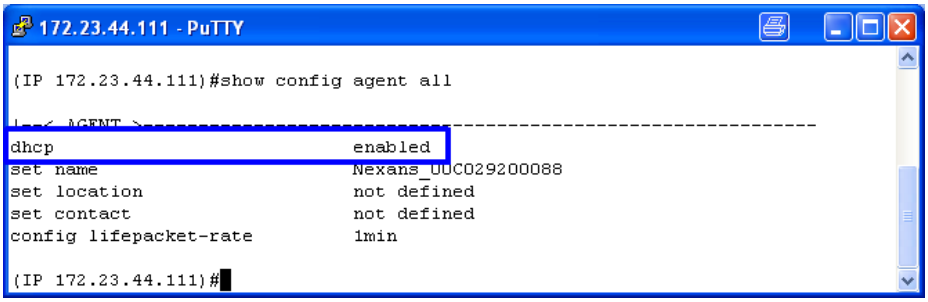
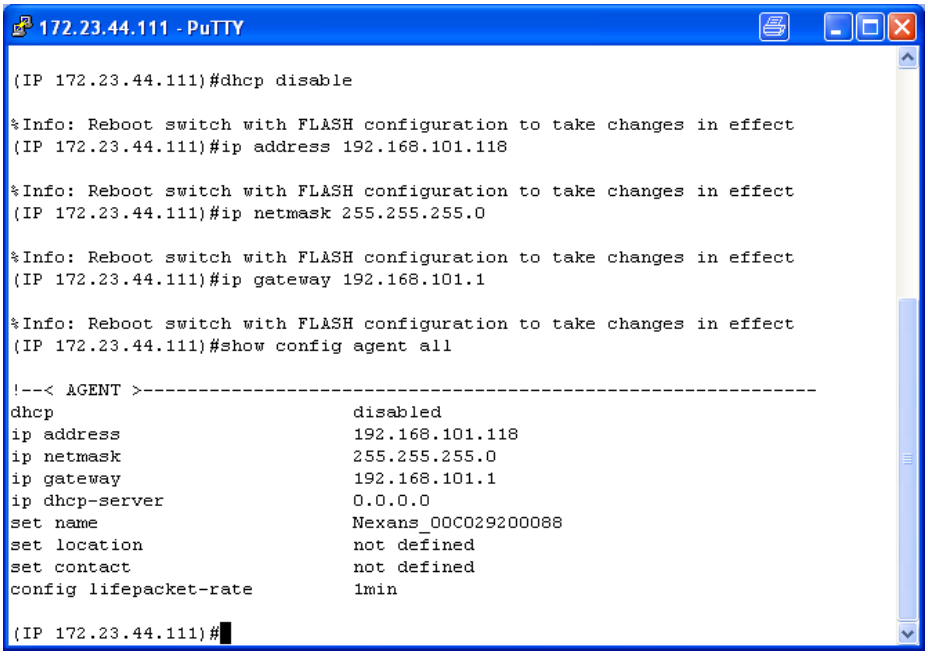
5.5.1. Setting of the IP Address via configuration switches and Web browser

1	**Booting with fixed IP address** Booting the switch via the configuration switches with fixed IP address. Detailed procedure see chapter *3.4 Management Configuration Switches and Pushbuttons*.
2	**Check, if the Status-LED on the management module lights up permanently** Notes on the function of the Status-LED see chapter *3.3 Management Status-LED*.
3	**Connect the switch via the network with the configuration PC** The configuration PC is connected either via a direct TP link between the switch and the PC or via the uplink port and the existing in-house network. IMPORTANT: The IP parameters of the PC must be correctly set. Notes see chapter *3.6.2. Booting with Fixed IP Address*
4	**Start the web browser and enter the IP address 172.23.44.111** 
5	**Enter the user name and password for access to the management module**  Enter 'admin' as the user name and 'nexans' as the password.
6	**Go to the 'Switch Setup' web page.** 

7	**Enter IP parameters** The check mark in the DHCP line must be removed to make sure the IP parameters are adopted as fixed values. Finally all settings have to be stored by clicking on the Set button. 
8	**Booting with flash configuration** Booting the switch via the configuration switches with flash configuration. Detailed procedure see chapter *3.4 Management Configuration Switches and Pushbuttons.*
9	**Check, if the Status-LED on the management module lights up permanently** Now the switch has been successfully initialized with the new IP parameters and can be accessed in the final subnetwork under the new IP address. Further settings such as Name Setup, Port Setup, VLAN Setup etc. should not be made until now.

5.5.2. Setting of the IP Address via configurations switches and TELNET console

1	**Booting with fixed IP address** Booting the switch via the configuration switches with fixed IP address. Detailed procedure see chapter *3.4 Management Configuration Switches and Pushbuttons*.
2	**Check, if the Status-LED on the management module lights up permanently** Notes on the function of the Status-LED see chapter *3.3 Management Status-LED*.
3	**Connect the switch via the network with the configuration PC** The configuration PC is connected either via a direct TP link between the switch and the PC or via the uplink port and the existing in-house network. IMPORTANT: The IP parameters of the PC must be correctly set. Notes see chapter *3.6.2. Booting with Fixed IP Address*
4	**Start Telnet using the IP address 172.23.44.111** 
5	**Enter the user name and password for access to the management module**  Enter 'admin' as the user name and 'nexans' as the password. NOTE: In order to confirm that the switch has been set to the fixed IP address, the IP address is shown as a prompt and an appropriate message is displayed.

6	**Display current IP settings** Enter the console command '`show config agent all`':  When {Booting with fixed IP Address} the values displayed for the IP address, network mask and gateway are random and can be overwritten with the desired new IP parameters.
7	**Enter IP parameters** The following Telnet commands are available: Disable DHCP: dhcp disable IP address: ip address a.b.c.d Network mask: ip netmask a.b.c.d Gateway: ip gateway a.b.c.d The fist command must always disable the DHCP. Then the other IP parameters can be edited. See the following example: 
8	**Booting with flash configuration** Booting the switch via the configuration switches with flash configuration. Detailed procedure see chapter *3.4 Management Configuration Switches and Pushbuttons*.
9	**Check, if the Status-LED on the management module lights up permanently** Now the switch has been successfully initialized with the new IP parameters and can be accessed in the final subnetwork under the new IP address. Further settings such as Name Setup, Port Setup, VLAN Setup etc. should not be made until now.

6. Switch Configuration

6.1. Switch Configuration using the Nexans Device Manager (NEXMAN)

NEXMAN is a Windows application for systems running Windows Me or later.

An evaluation version of this software is available at our Support Homepage:

http://www.nexans-ans.de/support/

By including your email address in the Software Update Newsletter, you will be automatically notified of the latest firmware updates.

6.1.1. Firmware Requirements

Configuration via NEXMAN (Nexans Device Manager) is supported by all firmwarefamilies. At least Release V3.01 must be installed.

NOTE:
If a firmware version V1.xx or V2.xx is installed on the switch, an update to firmware V3.xx or higher must be performed first. This update must be performed using NEXMAN.

6.1.2. Login

Several modes are selectable in the switch for authentication of NEXMAN towards the switch. With the Factory Default setting the switch uses SCP (ecure copy) for writing and reading the configuration.

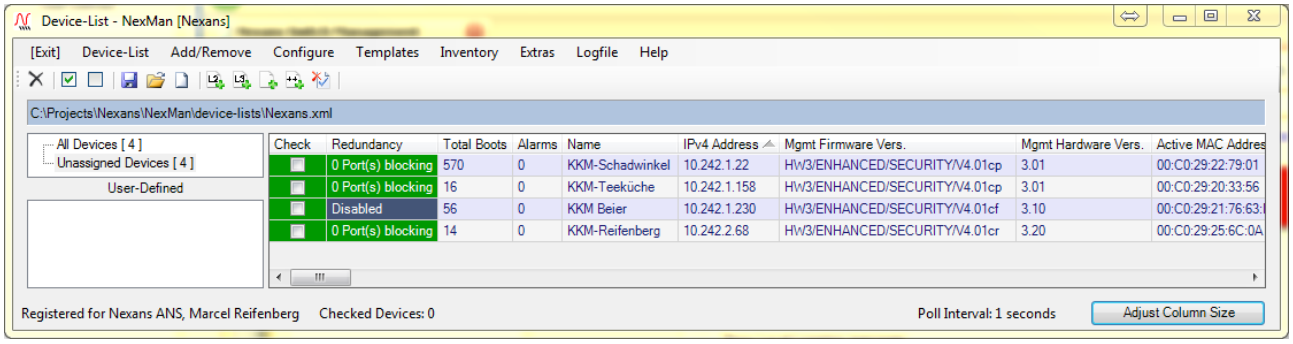
The default settings for Name and Password are: Name=admin, Password=nexans

For a detailed description of the modes see chapter *10.10. Manager Authentication Mode*

6.1.3. Configuration

NEXMAN allows the switch configuration to be downloaded and archived. Moreover, the configuration can be modified and transferred back to a single switch or to a list of switches.

For detailed information on configuration and update using NEXMAN please read the NEXMAN manual.



6.2. Switch Configuration via Web Browser (HTTP/HTPS)

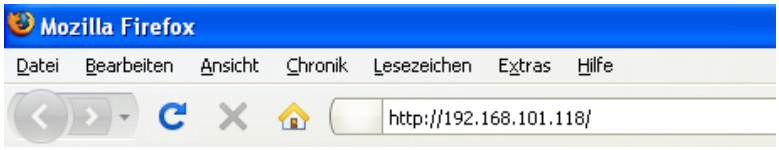
6.2.1. Authentication / Login

Important note:
The web interface can be disabled for HTTP and HTTPS separately via NEXMAN. In this case no access will be possible via the HTTP or HTTPS.

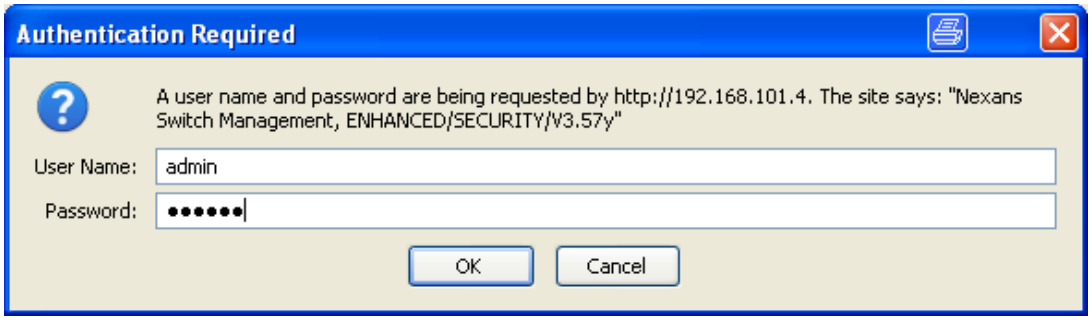
The web module can be accessed via HTTP with any standard web browser. The module must already be configured with an IP address, and the network mask and gateway have to be set correctly on the switch and PC here. A Ping command, for example, can be executed as a simple connectivity test.

When using HTTPS the following points have to be observed:
- Management hardware version HW3 or higher is needed.
- On the switches a certificate signed by Nexans Advanced Networking Solutions CA (Nexans-ANS CA) is installed (RSA, 1024 Bit Key, SHA-256).
- The Nexans CA Certificate is available at our Support Hompage http://www.nexans-ans.de/support/.
- The Nexans-ANS CA Certificate can be imported as a root certificate into the WEB browser used in order to bypass the security warnings when first accessing the switch. It should however be noted, that the switch must not be accessed via the IP address (this is a fundamental restriction of the HTTPS certificate concept), but via a symbolic name. This name must then be resolved either by a DNS server or by the host file into the corresponding IP address. On all Nexans switches an identical certificate is installed, which has been signed for the symbolic name of *.switch.nexans. The asterisk (*) may be replaced by any switch name (which, however, must not contain a dot (.)) so that the browser recognises the switch certificate as valid.

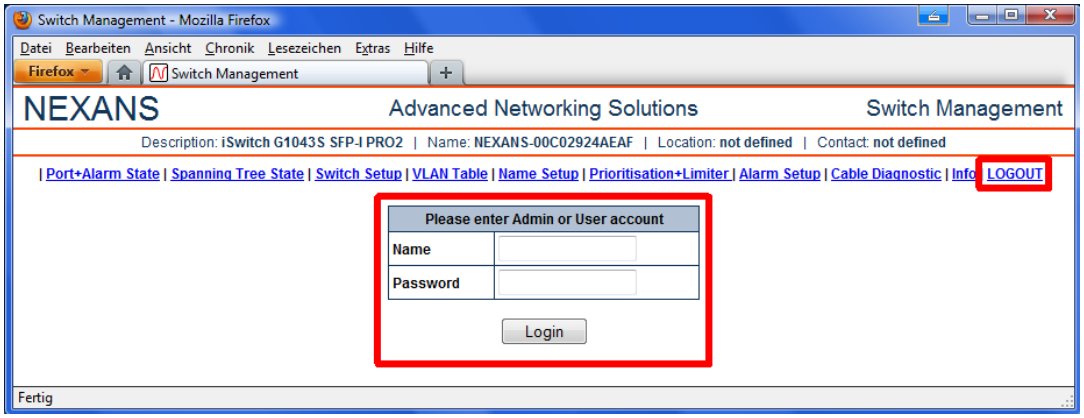
When the web browser has started, the IP address or symbolic name of the switch has to be entered in the browser address line:



Access to the management module is password-protected:



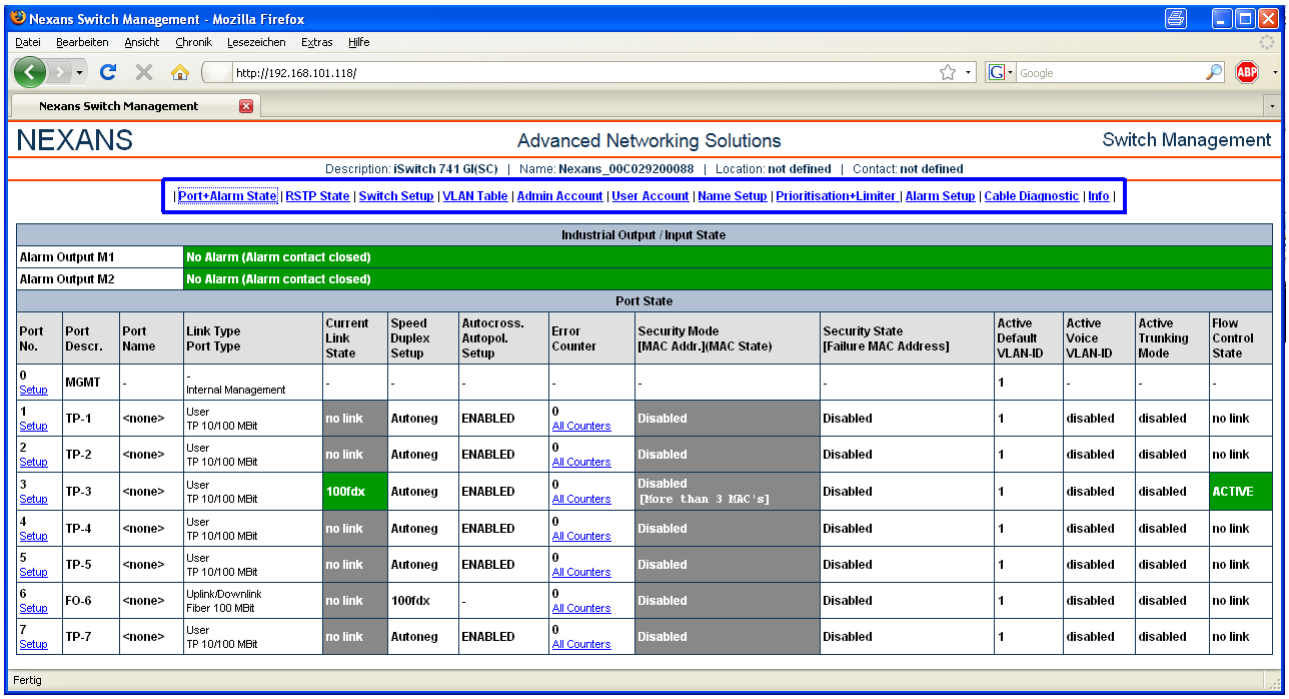
From management hardware version HW3 or higher, the name and passwort are entered within the browser window:



The default settings for Name and Password are: Name=admin, Password=nexans
for User level: Name=user, Password=nexans

6.2.2. Configuration

After successful login the different functions of the switch can now be accessed via the menu bar:



6.3. Switch Configuration via V.24 Console

Configuration using the V.24 console interface is supported by industrial switches and desk switches of type 'GigaSwitch'.

The following V.24 transmission parameters have to be set in the terminal program of the PC:

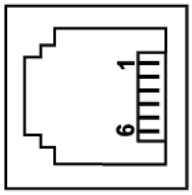
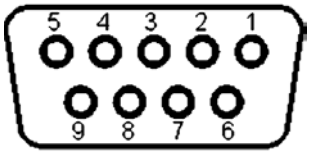
- 9600 Baud
- 8 data bits
- 1 stop bit
- no parity
- Flow control: Xon/Xoff or None

6.3.1. Connection to Switches with RJ11-Connector

For this purpose, an RJ11 connector is provided on the front panel of the Switch as V.24 interface. This RJ11 connector must be connected via a special RJ11/DSUB9 adapter cable with the serial port of the PC.

Nexans offers such a terminated adapter cable as an accessory part (Nexans order number 88300688).

The following figure shows the assignment of the RJ11 socket on the switch and the D-Sub connector on the adapter cable:

RJ11 socket on the switch	D-Sub connector on the adapter cable	
		
Pin	Pin	Signal name

1	7	CTS (DA)
2	-	-
3	3	TxD
4	5	GND
5	2	RxD
6	8	RTS (DE)
	1 4 6 NOTE: These three pins are shorted inside the connector.	DCD DTR DSR

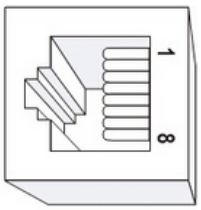
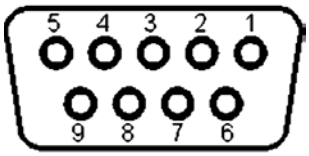
6.3.2. Anschluss beim Industrie-Switch mit RJ45-Buchse

A RJ45 connector is provided on the front panel of the Switch as V.24 interface. This connector must be used with a special RJ45/DSUB9 adapter cable that is connected to the serial interface of the PC:

Nexans offers such a terminated adapter cable as an accessory part (Nexans order number 88646169).

Info: This cable is compatible with the standard *Cisco* console cable (e.g. *Cisco* Part-Numberr.: 72-3383-01):

The assignment of the 8pol, RJ45 and the 9pol D-SUB connector on the adapter cable is as follows:

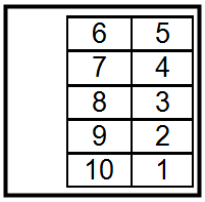
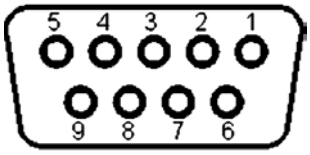
8 pol. RJ45-Socket on the Switch 	9pol. D-Sub- connector on the adapter cablel 	
Pin	Pin	Signal name
1	8	CTS
2 This Pin is bridged with Pin 7 at the switcht	6	DSR
3	2	RxD
4 5	5	GND
6	3	TxD
7 This Pin is bridged with Pin 2 at the switcht	4	DTR
8	7	RTS

6.3.3. Socket location at GigaSwitch V3 and GigaSwitch 5xx Desk

On the GigaSwitch V3 the V.24 socket is situated below the LED insert, and on the GigaSwitch 5xx Desk on the bottom side of the switch below the memory card cover.

The 10-pin socket is connected via an active DSUB9 custom adapter cable with the PC's serial interface. The appropriate adapter cable can be ordered from Nexans as an accessory (Nexans part number: 88300695).

The pin-out on the D-SUB socket is as follows:

10pol. Mini-conector  Pin	9pol. D-Sub-connector on the adapter cablel  Pin	Signalname
1	5	GND
3 (3,3Volt Pegel)	2 (V.24 Pegel)	RxD
4 (3,3Volt Pegel)	3 (V.24 Pegel)	TxD
	1 4 6 These three Pins are bridged in the connector	DCD DTR DSR
	7 8 These two Pins are bridged in the connector	RTS CTS

6.3.4. Firmware Requirements

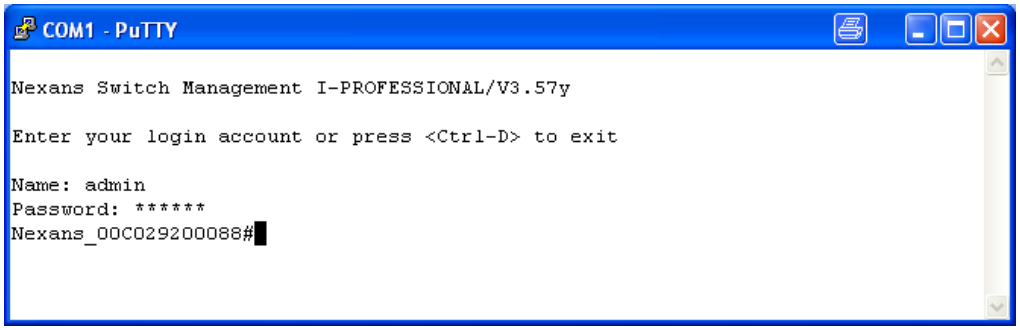
Firmware release 3.10 or later is required.

6.3.5. Authentication / Login

The switch can be accessed via any standard V.24 terminal application.

In order to avoid any configuration conflicts only one console connection (Telnet or V.24) may be open at a time, i.e. the switch will reject any further simultaneous connection setup attempts. In order to prevent the console from blocking the active console connection will be automatically released after 5 minutes of inactivity.

After starting the terminal program, the Login mode must be activated first by pressing <Enter>. Then the correct Login name and the corresponding password must be entered:



The factory default settings for name and password are: Name=user, Password=nexans

For a detailed description of V.24 authentication see chapters *10.14. V.24 Console Authentication Mode* and *10.56.RADIUS Console Authentication Modes*

6.3.6. Configuration

After successful login the switch answers with its prompt. Depending on the access level the prompt will be displayed as '#' (Admin level) or '>' (User level).

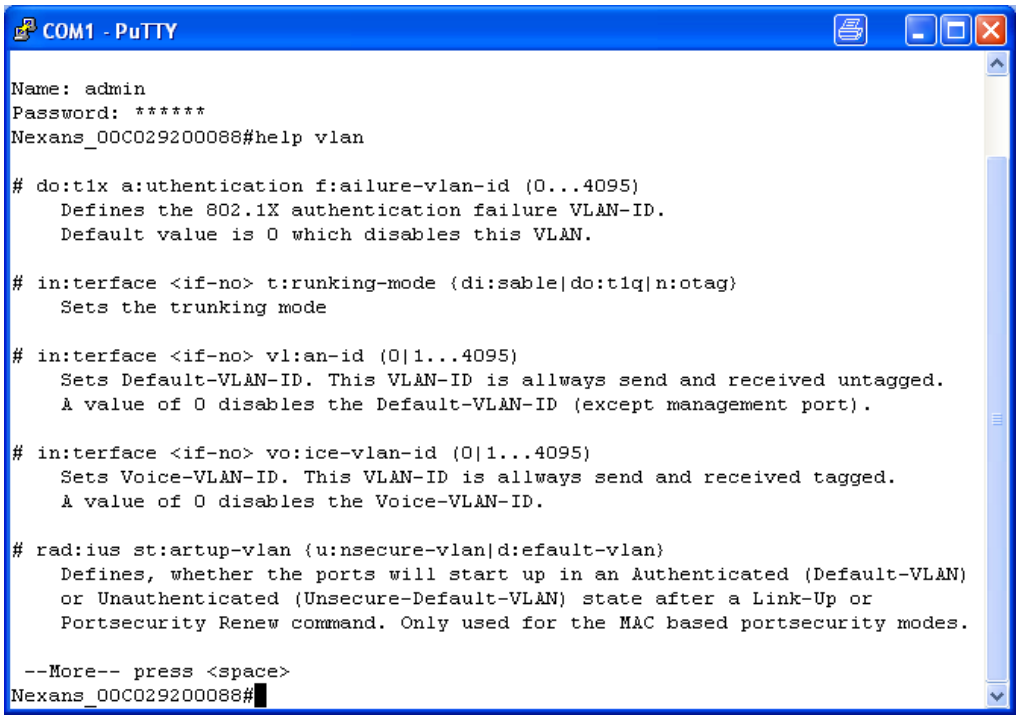
The 'Nexans-00C029200088' prompt in the illustration above is the name of the switch which is factory-preset to 'Nexans-xxxxxxxxxxxx'. Whereas xxxxxxxxxxxx will be replaced by the MAC address of the switch

This name can be edited using the Telnet command *`set n:ame [<string 1...50 chars>]`*. Moreover, this name is identical with the sysName SNMP variable in the MIB-II system group and can also be edited via SNMP.

The switch supports a history buffer, which stores the last 10 commands entered. The keys ↑ and ↓ can be used to scroll through the buffer.

The console commands 'help' or '?' display an overview of all valid console commands.
For searching a command up to two search strings can added. The syntax is as following:
`h:elp [<search-string>] [<search-string>]`

Example:



Chapter *9. Summary of all State and Configuration Parameters* contains a summary of all switch parameters with their respective console commands.

6.4. Switch Configuration via Telnet or SSH Console

6.4.1. Authentication / Login

The switch can be accessed via any Telnet or SSHv2 standard client. The module must already be configured with an IP address, and the network mask and gateway have to be set correctly on the switch and PC here. A ping request, for example, can be executed as a simple connectivity test.

Without any exception, all parameters of the switch can be configured via TELNET or SSH console.

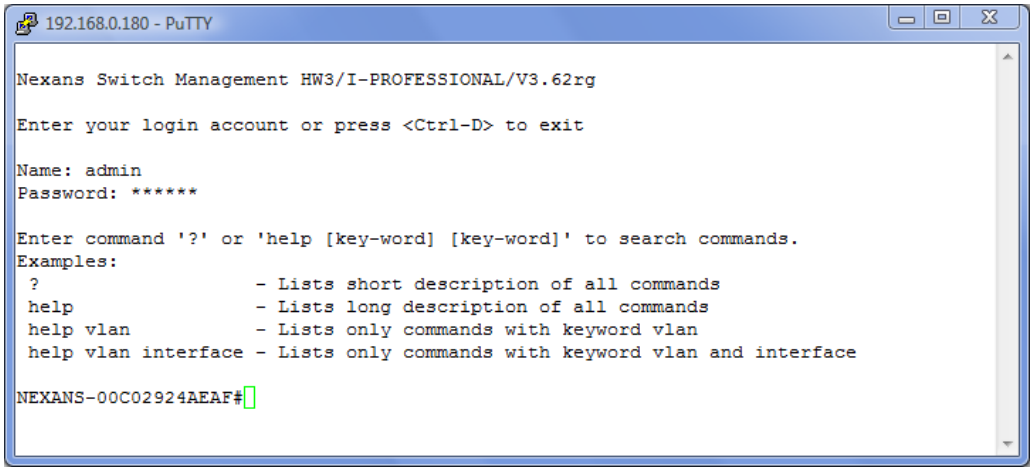
Please note the following items when using SSHv2:

- requires Management Hardwareversion HW3 or higher
- supports SSH Version 2 only
- supports 1024 Bit RSA-Keys only
- a 1024 Bit RSA-Key-Pair is pre-installed by factory default
- to create a new 1024 Bit RSA-Key-Pair use CLI reboot command "reload new-rsa-key"
- rebooting with factory default settings will automatically create a new 1024 Bit RSA-Key-Pair
- in this release the public part of Key-Pair can't be displayed
- simultaneously access via SSH, Telnet or V.24 console sessions isn't possible

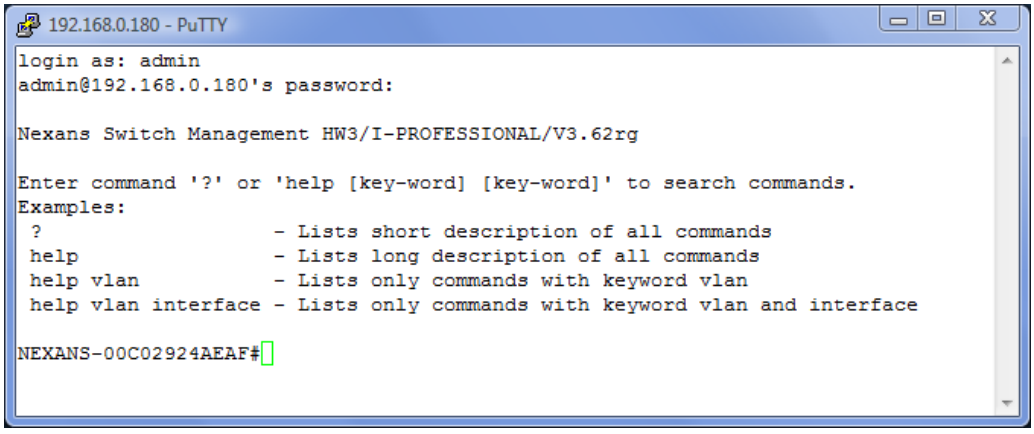
In order to avoid any configuration conflicts only one console connection (Telnet, SSH or V.24) may be open at a time, i.e. the switch will reject any further simultaneous connection setup attempts. In order to prevent the Telnet console from blocking the active Telnet connection will be automatically released after 15 minutes of inactivity.

After starting the Telnet resp. SSHv2 client with the IP address of the management module the correct Login name and the appropriate password must be entered first:

Telnet:



SSHv2:



The factory default settings for name and password are: Name=user, Password=nexans

For a detailed description of the Telnet/SSH authentication see chapters *10.48.Telnet Console Authentication Mode*, *10.49 SSHv2 Console Authentication Mode*, *10.56. RADIUS Console Authentication Modes*

or *10.64 TACACS+ Console Authentication Modes*.

6.4.2. Configuration

After successful login the switch answers with its prompt. Depending on the access level the prompt will be displayed as '#' (Admin level) or '>' (User level).

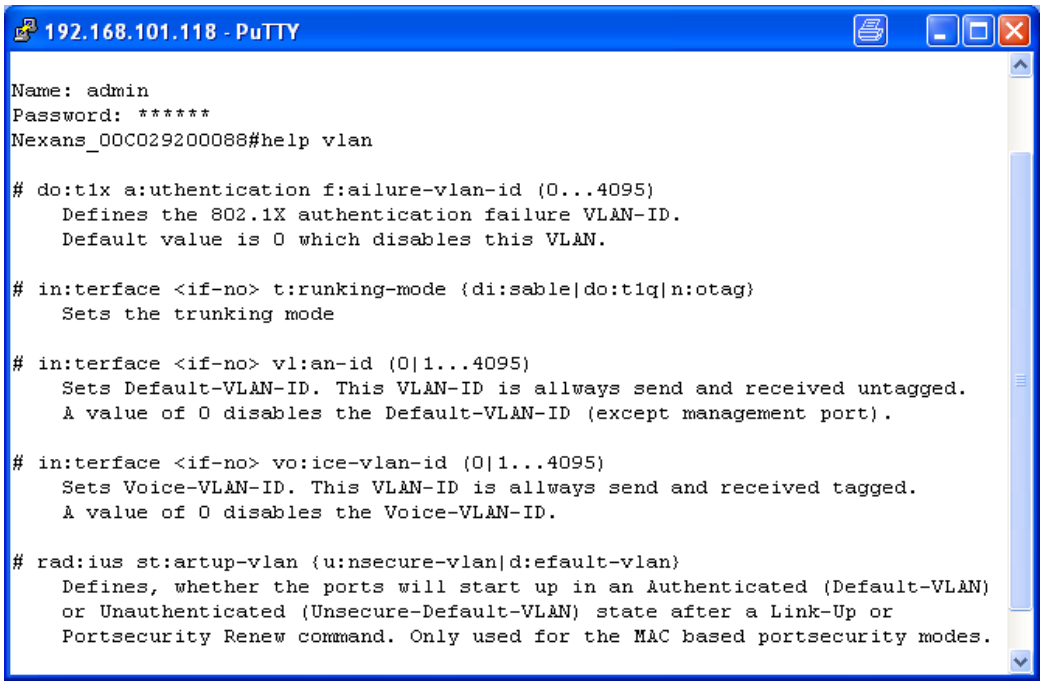
The 'Nexans-00C029200088' prompt in the illustration above is the name of the switch which is factory-preset to 'Nexans-xxxxxxxxxxxx'. Whereas xxxxxxxxxxxx will be replaced by the MAC address of the switch

This name can be edited using the console command *`set n:ame [<string 1...50 chars>]`*. Moreover, this name is identical with the sysName SNMP variable in the MIB-II system group and can also be edited via SNMP.

The switch supports a history buffer, which stores the last 10 commands entered. The keys ↑ and ↓ can be used to scroll through the buffer.

The console commands 'help' or '?' display an overview of all valid console commands.
For searching a command up to two search string can added. The syntax is as following:
`h:elp [<search-string>] [<search-string>]`

Example:



Chapter *9. Summary of all State and Configuration Parameters* contains a summary of all switch parameters with their respective console commands.

6.5. Switch Configuration via SNMP

6.5.1. Authentication / Communities

Access via SNMP is possible with any standard SNMP manager.

The SNMPv1/v2c communities and SNMPv3 username/password will be evaluated accordingly and have to be correctly set at the SNMP manager.

For a detailed description of the SNMP communities see chapter *10.53. SNMP Support*.

6.5.2. Configuration

Please consult chapter *10.53.7. List of SNMP MIBs* for the SNMP MIBs currently supported by the switch.

Chapter *9. Summary of all State and Configuration Parameters* contains a summary of all switch parameters with their respective SNMP variables.

The Nexans private MIBs required for management integration can be downloaded via our support portal (www.nexans-ans.de/support.

7. Firmware Update and Switch Configuration

7.1. Firmware Update

An appropriate firmware file containing the new release is required to update the management module firmware. The latest release can be downloaded after a short registration from the Nexans Advanced Networking Solutions Support-Portal: www.nexans-ans.de/support. By including your email address in the Software Update Newsletter, you will be automatically notified of the latest firmware updates.

NOTE:
The update will not modify the configuration settings already made in the switch. Only for newly-added features, the factory default settings will be used.

7.1.1. Dual Firmware Storage

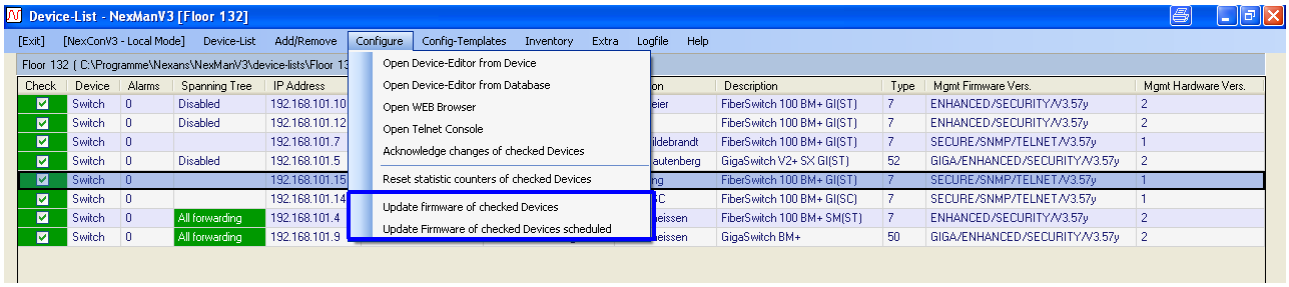
On HW5 switches two firmware versions are parallelly stored on different boot partitions. When a firmware update is installed, the currently running firmware is saved as backup, and the installed firmware becomes the new running firmware. In case the newly executed firmware is unstable or damaged, the backup firmware will be started from the other boot partition and the backup firmware will become the running firmware again.

On demand you you can manually reload the backup firmware version in CLI and Manager, see chapter *9.12 Management > Agent*.

7.1.2. Firmware Update via Nexans Device Manager (NEXMAN)

NEXMAN allows you to perform an automatic firmware update of a single switch or of a complete list of switches. NEXMAN is a Windows application requiring Win7 or higher.

For detailed information on the update via NEXMAN please read the NEXMAN manual.



NEXMAN offers the following advantages:

- Fast Layer-2 and Layer-3 Auto Discovery feature for finding active switches
- Extended device list with individual sorting parameters e.g. IP address, MAC addresses, device name or software version
- Freely definable categories in tree structure
- Highlighting of switch and category by incoming alarms
- Easy to handle User-Management with different access levels, roles and user specified device lists
- Online remote diagnostic and monitoring information of SFP-modules
- Time scheduled firmware update for elected switches
- Master configuration may specify different parameters for distribution
- Creation of multiple master configurations for distribution to one or more switches
- Storage of device configurations in local or remote database
- Storage of old device configurations via history function in the database
- Extended import and export function
- Comprehensive information in system log

7.1.3. Firmware Update via Telnet/SSH/V.24 console

HINT: This function requires management hardwareversion HW2 or higher installed.

A new firmware can be loaded via a TFTP command from the Telnet or V.24 console. However, for this function an external TFTP server is needed to provide the firmware file. Here the switch itself acts as a TFTP client. For execution of the corresponding command you have to login onto the console with the Admin Account first.

The command syntax is as follows:

```
tf:tp <ip-address> put <path> {<filename>.cfg|$ip$.cfg|$name$.cfg} [all]
```

Parameters:

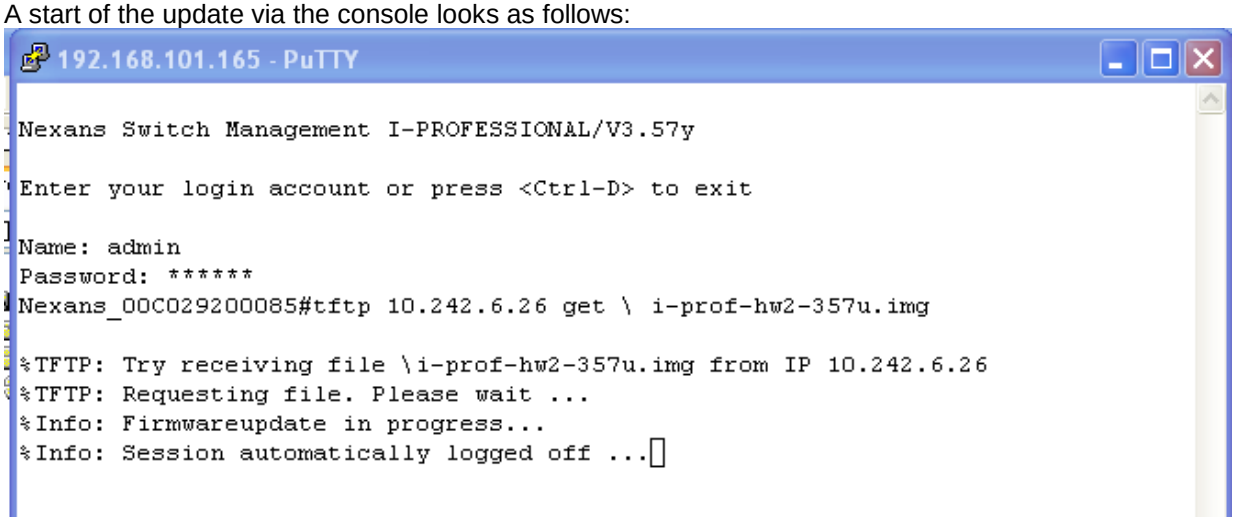
`<ip-address>`	IP address of the external TFTP server
`<path>`	Path on the TFTP server, e.g. '/' or '/nexans-fw/iswitch/'
`<filename>.IMG|BIN`	Name of the firmware file, e. g. 'i-prof-hw2-355.img'
iip,cfg	Place holder for the IP-Adress of the Switch
$name$.cfg	Place holder for the name of the Switch

The strings of the <path> and <filename.xxx> parameters must not exceed 25 characters each. This is a limitation imposed by the console command interpreter.

Prior to the update with the indicated firmware file, the header of the file will be read, and checked whether the image is suited for the switch. If no, a corresponding error message will be issued on the console and the further update is cancelled.

If the image is suited for the switch type and the management module, the console session will be automatically closed, and the rest of the firmware file will be read via TFTP. Once the file has been successfully transferred, the management module reprograms itself automatically with the new firmware, and then reboots after approximately 5 seconds.

A start of the update via the console looks as follows:



7.1.4. Firmware Update automatically via DHCP/BootP

HINT: This function requires management hardwareversion HW2 or higher installed.

A successful update of the firmware via DHCP/BootP requires the loading of a switch configuration as command file via DHCP/BootP. Please, first read chapter *7.2.5 Loading Switch Configuration automatically via DHCP/BootP*.

The first command in the command file loaded via DHCP/BOOTP should be the update command with the following syntax:

```
tftp check-min-fw  <version-number> <path> {<filename>.img|bin} [<hw-version>]
tftp check-this-fw <version-number> <path> {<filename>.img|bin} [<hw-version>]
```

Parameters:

`<version-number>`	Version number without dot, e. g. '356' for version 3.56
`<path`	Path on the TFTP server, e. g. '/' or '/nexans-fw/iswitch/'
`<filename>.img|bin`	Name of the firmware file, e. g. 'i-prof-hw2-355.img'
`<hw-version>`	Optional: Management Hardwareversion, e. g. '2'

The strings of the <path> and <filename.xxx> parameters must not exceed 25 characters each. This is a limitation imposed by the console command interpreter.

The command **`check-min-fw`** will perform the update using the indicated firmware file, if the firmware version currently running on the switch has a lower number than the <version-number> indicated in the

command. If the installed version number is equal or higher than the one indicated, the command will be ignored.

The command **`check-this-fw`** will perform the update using the indicated firmware file, if the firmware version currently running on the switch has a lower or higher number than the <version-number> indicated in the command. Only if the installed version is identical with the indicated version, the command will be ignored.

The optional parameter [<hw-version>] defines for which management module hardware version the indicated firmware shall be installed. If the indicated version does not match the actual management module version, this line will be ignored. This makes sense, e. g. if the same command file shall be used for switches with different management hardware versions needing different firmware versions. In this case, for each hardware version one line with the corresponding firmware version must then be included in the command file.

IMPORTANT: The <version-number> must be included in the <filename> (e. g. <version-number> = 359 and <filename> = secu-hw2-359). Otherwise, the line will be ignored.

Prior to the update with the indicated firmware file, the header of the file will be read and checked whether the image is suited for the switch. If not, the further update will be cancelled and the remaining commands in the loaded command file will be executed.

If the image is suited for the switch type and the management module, the rest of the firmware file will be read via TFTP. Once the file has been successfully transferred, the management module reprograms itself automatically with the new firmware and then reboots after approximately 5 seconds.

7.1.5. Firmware Update via PC Console and SCP

NOTE: This feature requires management hardware version HW3 or higher.

The firmware image has to be sent to the switch using the Secure Copy (SCP) protocol. Secure FTP (SFTP) cannot be used. http://www.putty.org/. Under Windows you can use e.g. the “pscp.exe” program, which is included in the SSH/Telnet Client “PuTTY” package (see http://www.putty.org). For Linux operating systems the standard command “scp” is available for this purpose.

For transferring the firmware with immediate execution of the update the following syntax applies:

Windows: `pscp -scp -P 50271 <filename>.img <username>@<ip-address>:/img`
Linux: `scp -P 50271 <filename>.img <username>@<ip-address>:/img`

For transferring the firmware with time-controlled update via SNTP server the following syntax applies:

Windows: `pscp -scp -P 50271 <filename>.img <username>@<ip-address>:/img_yyyymmdd_hhmm`
Linux: `scp -P 50271 <filename>.img <username>@<ip-address>:/img_yyyymmdd_hhmm`

NOTE: The time-controlled update is only executed, if the switch has received a valid time from the time server.

After successful transfer of the firmware image and immediate or time-controlled execution of the update, a reboot will be automatically performed after about 5 seconds.

7.1.6. Firmware Update via PC Console und TFTP

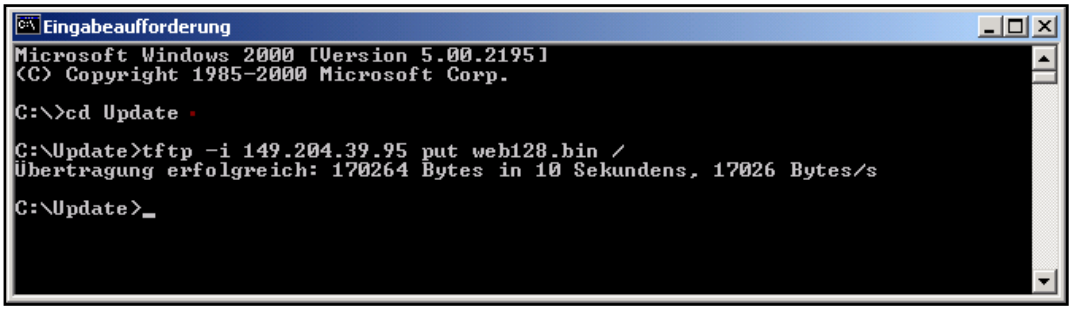
Manually updating the firmware using PC console program is only possible, if the 'Manager authentication mode' in the switch is set to {none} or a prior authentication via SNMP is performed (see chapter *7.5 TFTP Authentication using SNMP*).

For the update to be successful the module must already be configured with an IP address, and the network mask and the gateway must be set correctly on the switch and on the PC. A ping request, for example, can be executed as a simple connection test.

The firmware image now has to be sent to the Management Module via TFTP. The TFTP program which is included in Windows NT/2000/XP, for example, can be used here. Depending on the file extension of the image file the command syntax is as follows:

- **<name>.bin**
  `tftp -i <IP-Address> put <image.bin> /`
- **<name>.img**
  `tftp -i <IP-Address> put <image.img> /img`

Example:
A successful update will look like this for a switch with IP address 149.204.39.95 and for an update file 'c:\update\web128.bin':



Once the file has been successfully transferred, the management module reprograms itself automatically with the new firmware, and then reboots after approximately 5 seconds.

WARNING !

We recommend using the *Nexans Device Manager* (NEXMAN) for the update, since it will execute all functions automatically thus excluding any errors during the update.

7.2. Managing the Switch Configuration

7.2.1. File Formats of Switch Configuration

Principally two different file formats are supported for processing the switch configuration:

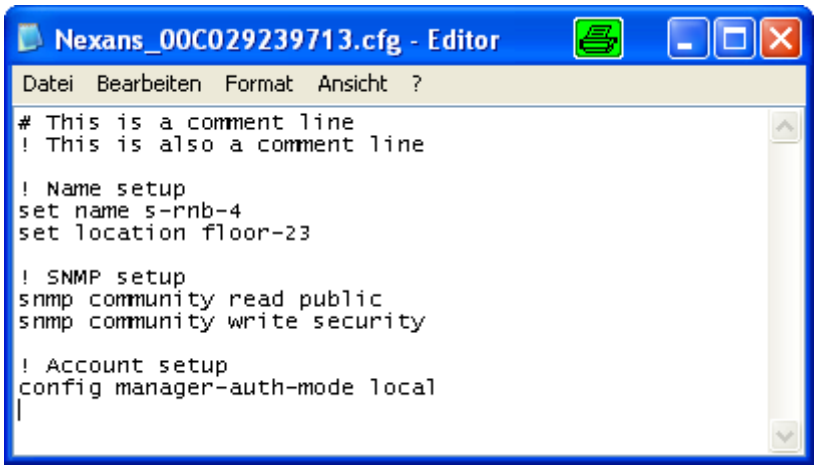
- **Binary format (.dat)**

If the file name ends with the '.dat' extension, the file will be interpreted as a binary file. The Nexans Device Manager (NEXMAN) is using exclusively this file format, because it allows a fast and efficient reading and writing of the switch configuration.

- **Command line format (.cfg)**

A configuration file in the command line format contains a sequence of Telnet/SSH/V.24 commands and must have the '.cfg' extension. PC, UNIX and MAC file formats are acceptable.

Please find below an example of the contents of such a file:



NOTE: Comment lines must begin with '#' or '!'.

7.2.2. Administration of Switch Configuration using NEXMAN

Modification and management of the switch configurations can be performed very comfortably using Nexans Device Manager (NEXMAN). Via the History function of NEXMAN also older configurations can be loaded into the switch editor and written back into the switch. NEXMAN will store the configuration files in the so-called 'Database folder'. For each switch a file of the name `a_b_c_d.dat` is created (`a_b_c_d` is the IP address a.b.c.d of the switch). Within the folder another folder called 'history' is created containing the archived history configuration.

Reading and writing the configuration via NEXMAN is done exclusively in the binary format. Here the switch is working as SCP server using TCP port 50271. For more information see chapter *10.10. Manager Authentication Mode)*.

7.2.3. Storing Switch Configuration via Telnet/SSH/V.24 Console

NOTE: This feature requires management hardwareversion HW2 or higher installed.

The switch configuration can be saved in the command format via a TFTP command from the Telnet or V.24 console. However, for this function an external TFTP server is needed which accepts the configuration file. Here the switch itself acts as a TFTP client. For the execution of the corresponding command you have to login onto the console with the Admin account first.

The command syntax is as follows:

```
tftp <ip-address> put <path> {<filename>.cfg} [all]
```

Parameter:

`<ip-address>`	IP address of the external TFTP servers
`<path>`	Path on the TFTP server, e. g. '/' or '/nexans-cfg/iswitch/'

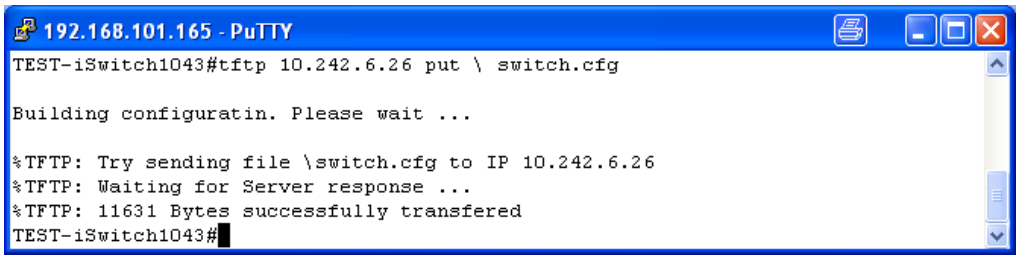
`<filename>.cfg`	Name of the command file, e. g. 'Nexans-00c029245634.cfg'
`[all]`	Optional parameter: see below

Without indication of the optional "all" parameter only settings deviating from factory default will be saved. With indication of the "all" parameter all configuration settings, also those set to factory default, will be saved.

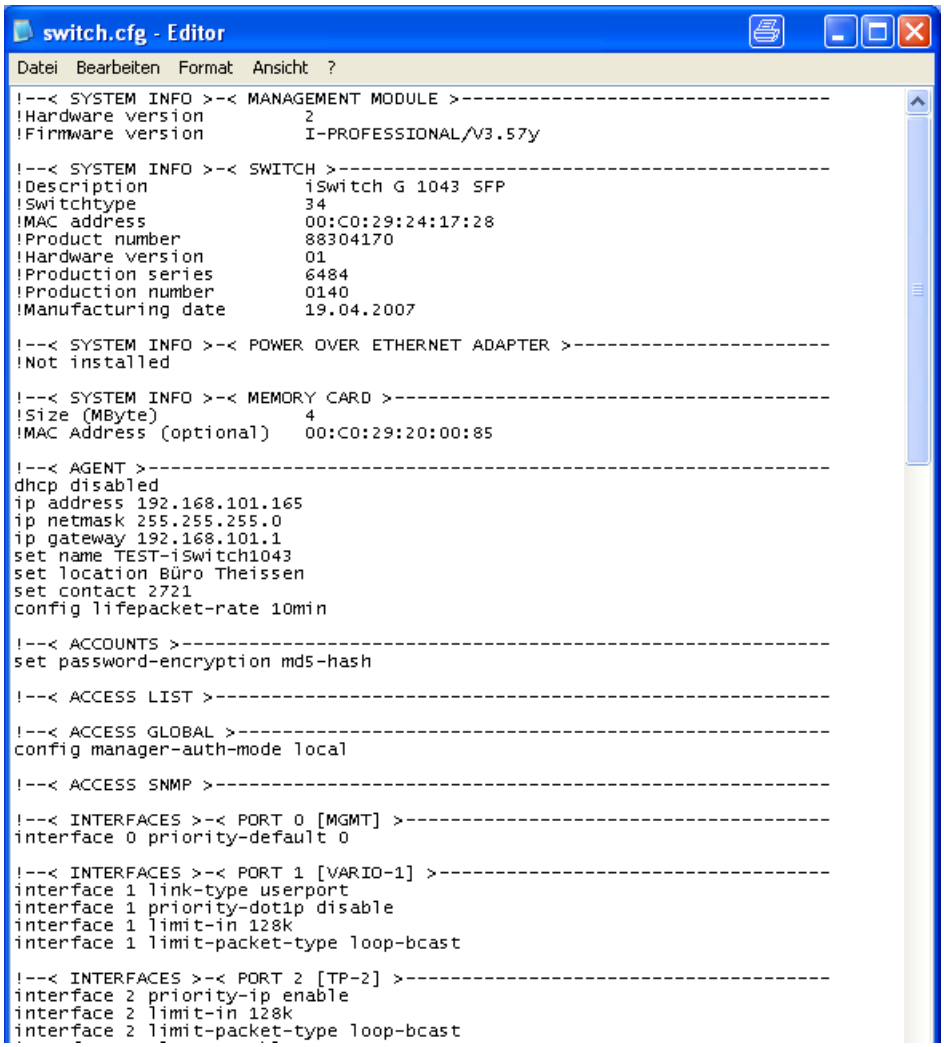
The strings of the <path> and <filename.xxx> parameters must not exceed 25 characters each. This is a limitation imposed by the console command interpreter.

After sending the command, first the configuration file is created in the memory (identical with the 'show running-config' command) and then transmitted via TFTP.

A successfully completed Save operation via the console looks as follows:



Please find below an example extract of the contents of such a file:



7.2.4. Loading Switch Configuration via Telnet/SSH/V.24 Console

NOTE: This feature requires management hardwareversion HW2 or higher installed.

The switch configuration can be loaded via a TFTP command from the Telnet or V.24 console. However, for this function an external TFTP server is needed to provide the configuration files. Here the switch itself acts as a TFTP client. For the execution of the corresponding command you have to login onto the console with the Admin Account first.

7.2.4.1. Loading the configuration from a command file

Command syntax:

```
tftp <ip-address> get <path> <filename>.cfg
```

Parameters:

`<ip-address>`	IP address of the external TFTP servers
`<path>`	Path on the TFTP server, e. g. '/' or '/nexans-cfg/iswitch/'
`<filename>.cfg`	Name of the command file, e. g. 'Nexans-00c029245634.cfg'

The strings of the <path> and <filename.xxx> parameters must not exceed 25 characters each. This is a limitation imposed by the console command interpreter.

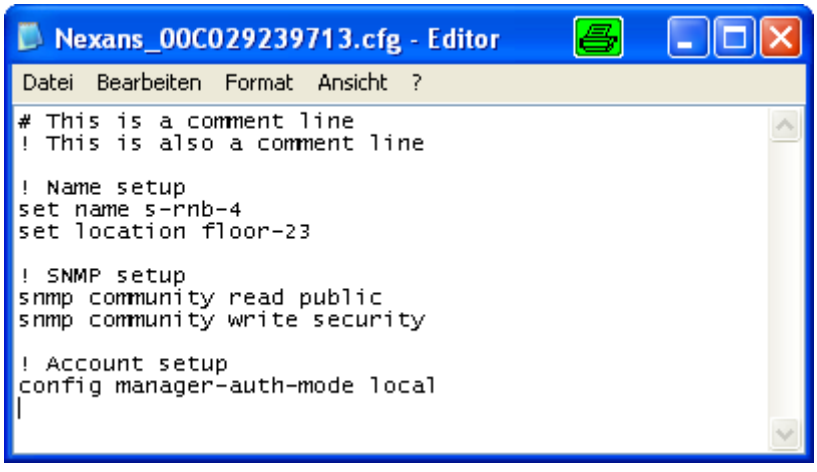
After loading a file with a '.cfg' extension, first the complete switch configuration is reset to factory default and the contents subsequently interpreted line-by-line as a sequence of console commands. PC, UNIX and MAC file formats are acceptable.

HINT:
The following parameters will be kept if the switch is set to factory default:

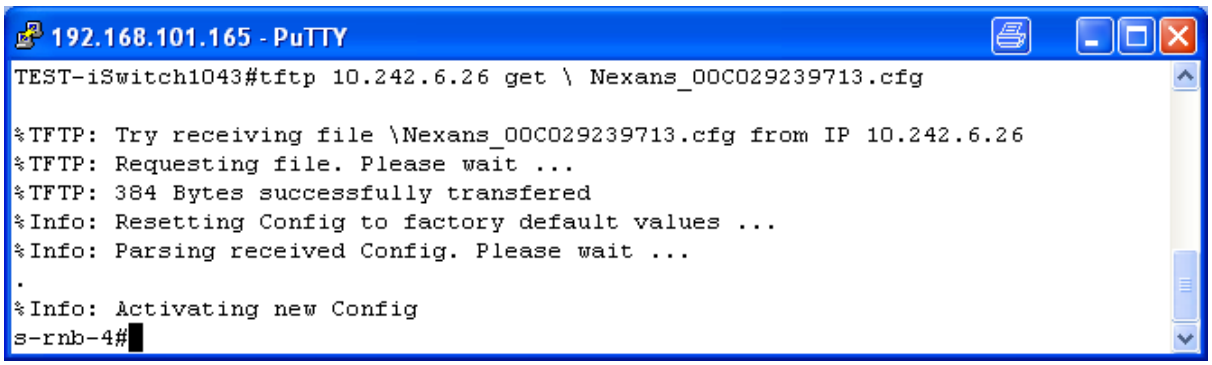
- Switch Name and Location
- IP Address, Gateway and Netmask
- Admin Account Name and Password
- User Account Name and Password
- Password Encryption Mode

If the mentioned parameters should also be replaced, the corresponding console commands can be added to the configuration file.

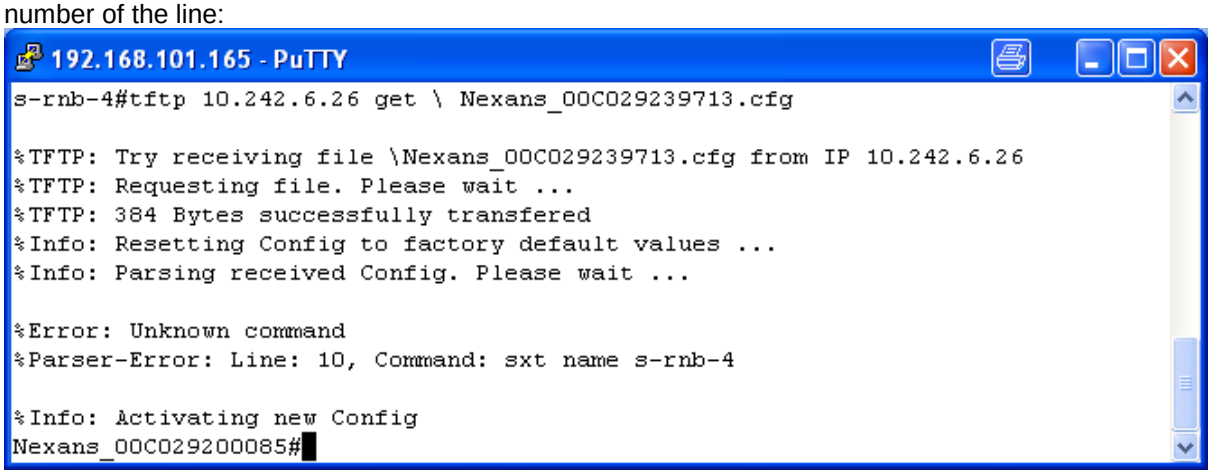
Please find below an example of the contents of such a file:



A successfully completed loading operation via the console looks as follows:



If the file contains unknown or invalid commands, an appropriate error message will be issued indicating the number of the line:



After the successful processing of all commands (with the exception of the failed commands) the new configuration will be activated, and a corresponding message displayed: '`%Info: Activating new Config`'.

7.2.4.2. Loading the configuration from a binary file

Command syntax:

```
tftp <ip-address> get <path> <filename>.dat
```

Parameters:

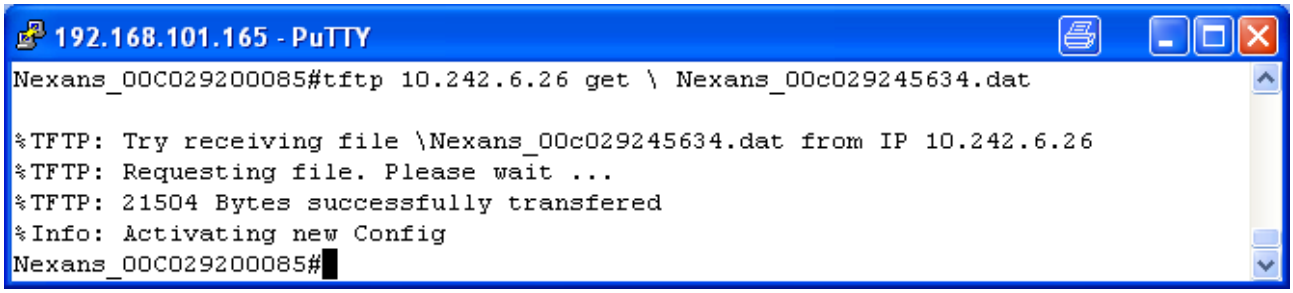
`<ip-address>`	IP address of the external TFTP server
`<path>`	Path on the TFTP server, e. g. '/' or '/nexans-cfg/iswitch/'
`<filename>.dat`	Name of the binary file, e. g. 'Nexans-00c029245634.dat'

The strings of the <path> and <filename.xxx> parameters must not exceed 25 characters each. This is a limitation imposed by the console command interpreter.

If the file name ends with the 'dat' extension, the file will be interpreted as a binary file. Binary files can be very conveniently created and managed using NEXMAN. In this process, first a configuration template is created in the Device Editor via the menu 'Config-Templates -> Save as BOOTP Config'. Now the configuration can be edited in the Device List using the menu command 'Config-Templates -> Edit BOOTP Config'.

IMPORTANT:
The IP parameters and the name of the switch are kept when loading a binary file. For this reason, these parameters are hidden in the BOOTP editor of NEXMAN.

A successfully completed loading operation via the console looks as follows:



After receiving an error-free binary file the included configuration will be activated and a corresponding message issued: '`%Info: Activating new Config`'.

If the check sum of the configuration is not correct, the configuration will not be accepted and the following error message issued instead: '`%Error: Config has wrong checksum`'.

7.2.5. Loading Switch Configuration automatically via DHCP/BootP

HINT: This function requires management hardwareversion 2 installed.

Contrary to loading the configuration via a console command, here the IP address of the TFTP server and the name of the configuration file are transmitted using the DHCP protocol. For creating the corresponding command or binary files see chapter *7.2.4 Loading Switch Configuration via Telnet/SSH/V.24 Console*.

In order to be able to use this feature the switch needs to be set to DHCP (factory default). The DHCP server needs to fill two optional fields in the DHCP protocol with the appropriate data. These fields are the 'server host name' field and the 'boot file name' field (see RFC2131). Here the 'sname' and 'file' fields in the protocol header as well as the options 66 and 67 can be used. If no value is transmitted for 'server host name' or 'boot file name', the contents of both fields will be ignored and no action for loading the configuration executed.

HINT: The TFTP download can be deactivated globally to prevent that the switch loads the configuration each time it reboots. This is helpful if the switch should only load the configuration after the first boot, but continuing running as a DHCP client. By adding the CLI command „dhcp tftp-download disable“ in the configurations that is loaded in the first bootp process any additional TFTP download will be disabled. This configuration can also be done later via the Device Manager.

- **server host name**
  Type the IP address of the TFTP server (a.b.c.d) into this field. A DNS name is not acceptable here.
- **boot file name**
  Two procedures are possible:
  - **Entry of a file name:**
    In this case the indicated file will be requested from the TFTP server. If this file is not available from the TFTP server, the switch will boot using the current flash configuration.
    Examples:
    Configuration.cfg
    Configuration.dat
    /Update/Configuration.cfg
    /Update/Configuration.dat
  - **Entry of a directory name:**
    When the name of a directory is entered, a slash '/' is always required at the end.
    Example:
    /
    /Config/

    In this case the switch tries to find different fixed file names in the indicated directory. The sequence of configuration requests is as follows:

    a) NEXANS-XXXXXXXXXXXX.cfg (command file)
    b) NEXANS-XXXXXXXXXXXX.dat (binary file)
    c) Nexans.cfg (command file)
    d) Nexans.dat (binary file)

    Where XXXXXXXXXXXX is the MAC address of the switch.

If none of the files are available on the TFTP server, the switch will continue to run using the flash configuration loaded during booting.

IMPORTANT:
The data regarding the IP address of the TFTP server and the name of the configuration file included in the DHCP packet are analysed only with the first DHCP-Acknowledge packet of the DHCP server after the reboot of the switch and the corresponding configuration file is loaded via TFTP. After expiration of half of the DHCP Lease-Time or by entering the 'dh:cp r:enew‘ console command and the resulting DHCP Request, the data will be ignored in the DHCP Acknowledge.
A renewed loading of the configuration file via DHCP/BOOTP can be triggered as follows:

- By rebooting the switch (e. g. by the ‘rel:oad’ console command).
- By the ‘dh:cp rel:oad-config’ console command (no reboot is triggered here).

IMPORTANT:
When loading a binary file the following parameters are kept:

- Switch Name

The name of the switch can be assigned via 'Host Name' DHCP option 12 if it is necessary.

When loading a cli file the following parameters are kept:

- Switch Name and Location
- IP Address, Gateway and Netmask
- Admin Account Name and Password
- User Account Name and Password
- Password Encryption Mode

If the mentioned parameters should also be replaced, the corresponding console commands can be added to the configuration file.

7.2.6. Reading and Writing the Switch Configuration via PC Console and TFTP

Here a TFTP client is needed for reading or writing the switch configuration on the PC. The 'tftp.exe' tool, which is included in Windows, for example, can be used.

Reading and writing the configuration from a PC is only possible, if the 'Manager Authentication Mode' in the switch is set to {none} (see chapter *10.10. Manager Authentication Mode*)or if prior authentication via SNMP has been performed (see chapter *10.3. Switch Name / Location / Contact / Domain*).

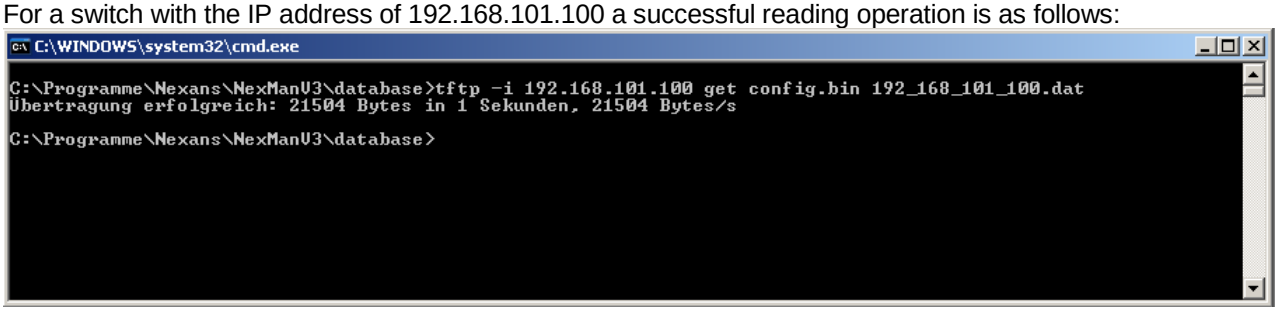
Depending on whether the configuration shall be read or written, the command syntax is as follows:

- **Reading the configuration in binary format:**
  `tftp -i <a.b.c.d> get config.bin a_b_c_d.dat`
- **Writing the configuration in binary format:**
  `tftp -i <IP address> put a_b_c_d.dat config.bin`

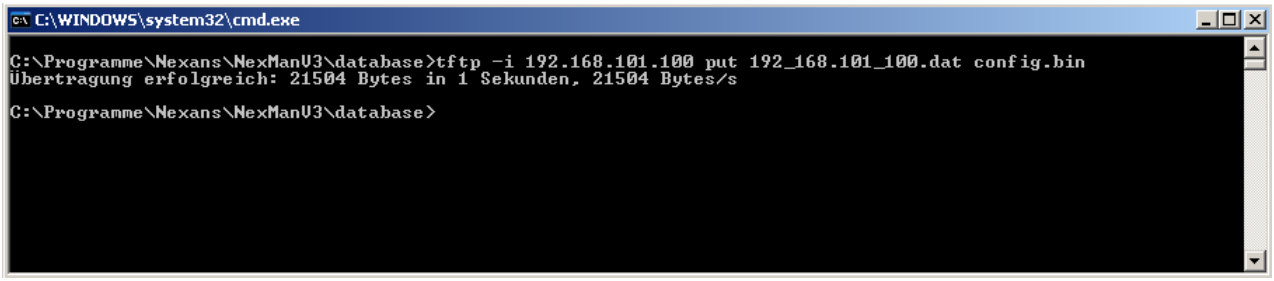
IMPORTANT:
Reading and writing the switch configuration in command line format is only possible via SCP (see chapter *7.2.7 Reading and Writing the Switch Configuration per PC Console and SCP*).

Example:

For a switch with the IP address of 192.168.101.100 a successful reading operation is as follows:



And this is an example of a successful writing operation:



After a successful transfer of the configuration into the switch, this configuration will be applied immediately without rebooting.

IMPORTANT NOTE:
The configuration read via TFTP is in binary format and can thus not be displayed using a text editor. It can only be read by NEXMAN. In order to display and, if necessary, modify this configuration using NEXMAN the configuration file should be copied into the "Database folder" of NEXMAN observing the naming convention indicated above. Afterwards the configuration can be loaded into the switch editor via the NEXMAN right-click menu option "Open Switcheditor from Database".

7.2.7. Reading and Writing the Switch Configuration per PC Console and SCP

NOTE: This feature requires management hardware version HW3 or higher.

The switch configuration can be written via Secure Copy (SCP) protocol to the switch or read by the switch. Secure FTP (SFTP) cannot be used. Under Windows you can use e. g. the “pscp.exe” program, which is included in the SSH/Telnet Client “PuTTY” package (see http://www.putty.org). For Linux operating systems the standard command “scp” is available for this purpose.

7.2.7.1. Reading the CLI Configuration per PC Console and SCP

For reading the configuration in CLI command format, which exclusively contains the parameters deviating from Factory Default, the following syntax applies:

Windows: `pscp -scp -P 50271 <username>@<ip-address>:/cfg <filename>`
Linux: `scp -P 50271 <username>@<ip-address>:/cfg <filename>`

For reading the configuration in CLI command format containing all parameters, the following syntax applies:

Windows: `pscp -scp -P 50271 <username>@<ip-address>:/cfg_all <filename>`
Linux: `scp -P 50271 <username>@<ip-address>:/cfg_all <filename>`

7.2.7.2. Writing the CLI Configuration per PC Console and SCP

For writing the configuration in CLI command format with reset to Factory Default the following syntax applies:

Windows: `pscp -scp -P 50271 <filename> <username>@<ip-address>:/cfg`
Linux: `scp -P 50271 <filename> <username>@<ip-address>:/cfg`

For writing the configuration in CLI command format without reset to Factory Default the following syntax applies:

Windows: `pscp -scp -P 50271 <filename> <username>@<ip-address>:/cfg_no_default`
Linux: `scp -P 50271 <filename> <username>@<ip-address>:/cfg_no_default`

7.2.7.3. Reading the Binary Configuration per PC Console and SCP

For reading the configuration in binary format, the following syntax applies;

Windows: `pscp -scp -P 50271 <username>@<ip-address>:/cfg_bin <filename>`
Linux: `scp -P 50271 <username>@<ip-address>:/cfg_bin <filename>`

7.2.7.4. Writing the Binary Configuration per PC Console and SCP

For writing the configuration in binary format, the following syntax applies;

Windows: `pscp -scp -P 50271 <filename> <username>@<ip-address>:/cfg_bin`
Linux: `scp -P 50271 <filename> <username>@<ip-address>:/cfg_bin`

7.2.7.5. Reading the Customer CLI Configurations per PC Console and SCP

For reading the Customer Default Configuration in CLI command format, the following syntax applies:

Windows: `pscp -scp -P 50271 <username>@<ip-address>:/cfg_custumer_default <filename>`

Linux: `scp -P 50271 <username>@<ip-address>:/cfg_customer_default <filename>`

For reading the Customer Reboot Configuration in CLI command format, the following syntax applies:

Windows: `pscp -scp -P 50271 <username>@<ip-address>:/cfg_customer_reboot <filename>`

Linux: `scp -P 50271 <username>@<ip-address>:/cfg_customer_reboot <filename>`

7.2.7.6. Writing the Customer CLI Configurations per PC Console and SCP

For writng the Customer Default Configuration in CLI command format, the following syntax applies:

Windows: `pscp –scp -P 50271 <filename> <username>@<ip-address>:/cfg_customer_default <filename>`

Linux: `scp -P 50271 <filename> <username>@<ip-address>:/cfg_customer_default`

For writng the Customer Reboot Configuration in CLI command format, the following syntax applies:

Windows: `pscp –scp -P 50271 <filename> <username>@<ip-address>:/cfg_customer_reboot <filename>`

Linux: `scp -P 50271 <filename> <username>@<ip-address>:/cfg_customer_reboot`

IMPORTANT:

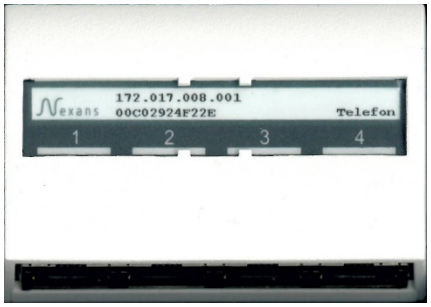
If you upload a CLI configuration the following parameters will be saved in case of a reset with factory default:

- Switch Name and Location
- IP Address, Gateway and Netmask
- Admin Account Name and Password
- User Account Name and Password
- Password Encryption Mode

If wished the upper values can be overwritten by using the respective CLI commands in the configuration file.

7.2.8. Switch Configuration ex Factory

Currently, factory pre-configuration of the switch can only be provided for switches of the GigaSwitch V5 type. These switches are programmed in a separate manufacturing step with a custom configuration and then provided with a head label indicating the IP address, the MAC address and (optionally) the “Phone” text:



For this purpose, the customer needs to make the desired switch configuration available in the form of a CLI command file. This file can easily be created via Nexans Manager in the Device Editor using the “Configure > Read CLI Config (Only with parameters changed from Factory Default)” menu.

Additionally, the following information is needed from the customer:

- First IP address of the desired IP address range. The last digit must be .1 (x.x.x.1).
- Information, whether a memory card shall be installed. In this case the MAC address of the memory card (instead of the MAC address of the switch) will be indicated on the label.
- Information, whether the “Phone” text shall be printed above TP Port 4 on the label.

For each switch configuration, Nexans must assign a different product number, which then must additionally be ordered together with the order for the switches.

7.3. Zero Touch Configuration

On HW5 switches with Zero Touch Configuration (ZTC) the configuration process and the programming of firmware upgrades can be automized. If Zero Touch Configuration is enabled, new switch configurations and firmware will automatically be provided by the Zero Touch Configuration Controller (subsequently reffered as Controller). The Controller is a separate server system or a virtual server on a dedicated computer on the network. Zero Touch Configuration is enabled by default, if the admin account is set to factory default (name: “admin”, password: “nexans”).

On startup the switch checks whether Zero Touch Configuration is enabled. If this is the case, the switch registers at the Controller to get new configurations or firmware. For this purpose, the switch must know the IP address of the Controller that the switch can retrieve in three different ways:

1. via *Nexans*-specific DHCP option 43 (if DHCP is enabled)
2. via DNS server using DHCP options 6 and 15 (if DHCP is enabled)
3. via static Controller IP address configured in the switch

The IP address of the Controller can be an IPv4 address or IPv6 address.

To show the current state of Zero Touch Configuration, DHCP server and DNS server, you can enter the following console command:

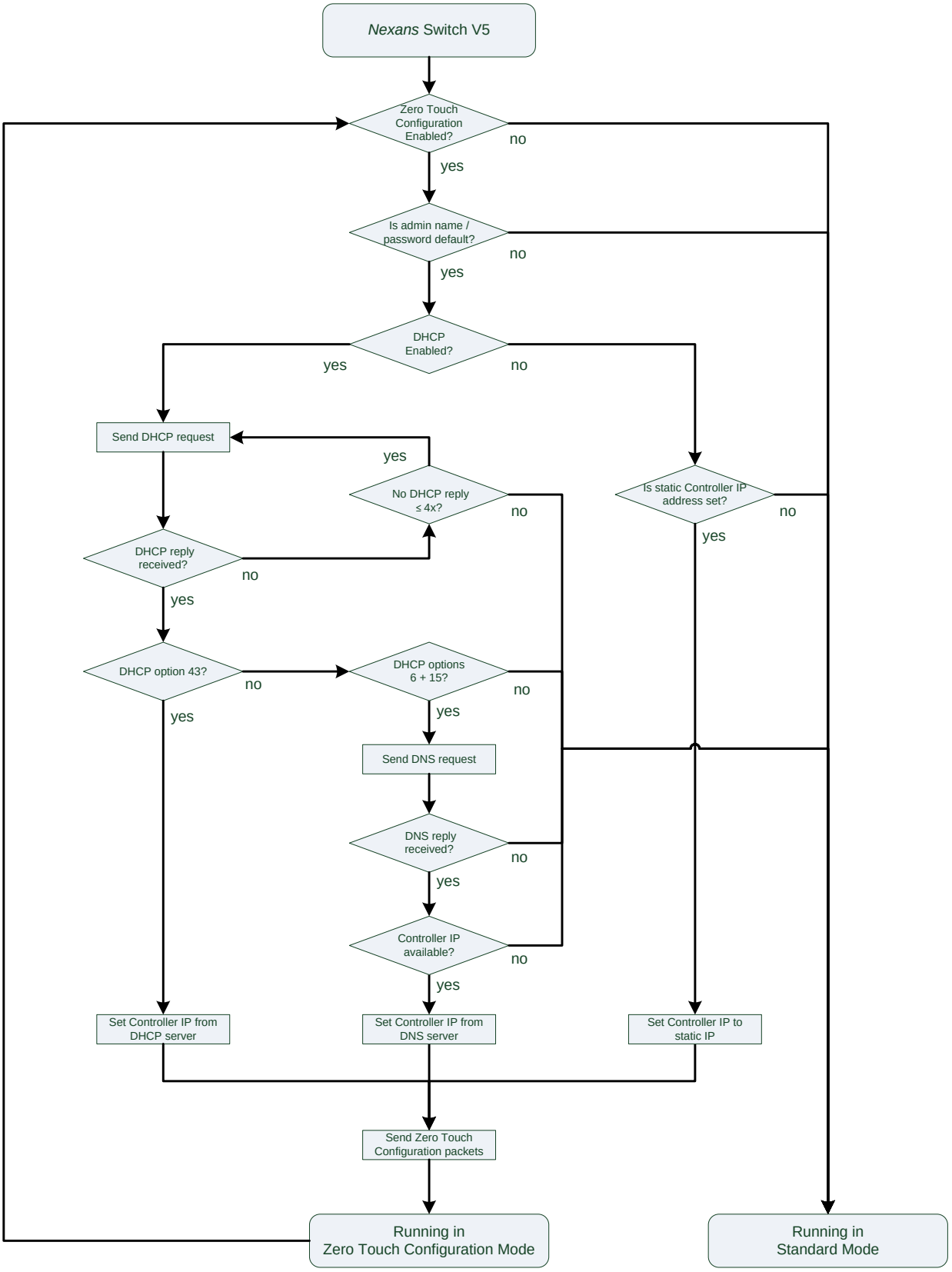
```
sh:ow zero-:touch-config
```

NOTES:

This feature is only available for *Nexans* V5 switches.

This feature requires the NEXMAN Controller. The NEXMAN Controller is a server software that is installed on the Controller and always running in the background.

The general workflow when Zero Touch Configuration is enabled, is depicted in the following flowchart:


Nexans Switch V5
Zero Touch Configuration Enabled?
no
yes
Is admin name / password default?
no
yes
DHCP Enabled?
yes
no
Send DHCP request
yes
No DHCP reply ≤ 4x?
no
DHCP reply received?
no
yes
DHCP option 43?
no
yes
DHCP options 6 + 15?
no
yes
Send DNS request
DNS reply received?
no
yes
Controller IP available?
no
yes
Is static Controller IP address set?
no
yes
Set Controller IP from DHCP server
Set Controller IP from DNS server
Set Controller IP to static IP
Send Zero Touch Configuration packets
Running in Zero Touch Configuration Mode
Running in Standard Mode

7.3.1. Zero Touch Configuration Settings

The following tables contains a summary of all Zero Touch Configuration settings:

Designation in NEXMAN	Default value	Function
Zero Touch Configuration Mode	enabled	With the Zero Touch Configuration Mode this feature can be enabled or disabled.
Controller IP Address	0.0.0.0	The static Controller IPv4 or IPv6 address. This IP address is only used, if DHCP is disabled. With the console command '`sh:ow zero-:touch-config`' the currently active Controller IP address can be checked.

7.3.2. Get Controller IP Address via DHCP Option 43

To get the Controller IP address from a DHCP server, DHCP must be enabled, and on the DHCP server option 43 must be configured as *vendor-encapsulated-option* according to the following *Nexans*-specific text format:

```
0x01 <text length> "NEXANS_cip_<IPv4/IPv6 address>"
```

whereas `0x01` is the code of suboption “Controller IP Address”, and `<text length>` is the length of the subsequent text field without NULL terminator. For some DHCP servers the text length is automatically calculated by the length of the subsequent text field and must not explicitly be declared.

Furthermore, the DHCP server must be configured to send option 43 if the requesting device is a *Nexans* switch. For Nexans switches the *vendor-class-identifier* in DHCP option 60 of the DHCP request starts with fix string “266” (e.g. “266:085”).

Example for a *Linux* DHCP server:

```
# Space for Nexans options 43
option space zero-touch-cfg;
option zero-touch-cfg.controller-ip code 1 = text;

...

# Nexans Switch with Zero Touch Config Controller IPv4 (option 43)
class "nexans-client" {
    match if substring(option vendor-class-identifier, 0, 3) = "266";
    vendor-option-space zero-touch-cfg;
    option zero-touch-cfg.controller-ip "NEXANS_cip_192.168.88.147";
}

# Nexans Switch with Zero Touch Config Controller IPv6 (option 43)
#class "nexans-client" {
#    match if substring(option vendor-class-identifier, 0, 3) = "266";
#    vendor-option-space zero-touch-cfg;
#    option zero-touch-cfg.controller-ip "NEXANS_cip_2000:2000::88:147”;
#}
```

7.3.3. Get Controller IP Address via DHCP Options 6 and 15

To get the Controller IP address from a DNS server, DHCP must be enabled, and on the DHCP server options 6 and 15 must be configured for the DNS server providing the IP address of the Controller. Option 6 must contain the corresponding IP address of the DNS server, and option 15 must contain the name of the domain the DNS server is located in.

Moreover, the DNS server must be configured with the IP address and the computer name of the Controller, and the with the name of the domain. The Controller name must be set to “nexans-controller”.

7.3.4. Static Controller IP Address

The static IP address of the Controller is part of the switch configuration and can be configured via NexMan or CLI. To activate the static IP address of the Controller, DHCP must be disabled and a valid IPv4 or IPv6

address be configured. For details about the switch configuration for Zero Touch Configuration see chapter *9.18 Management > Zero Touch Configuration*.

7.4. Scripting

NOTE: This feature requires management hardware version HW5 or higher.

Event-based, customer-specific configuration changes can be made through Scripting. Based on a pre-defined system event, a list of CLI commands will be started. The list of commands assigned to a certain event is called *CLI Script*. A pre-defined event can be a status change of a port or functional input, or a time-based event.

7.4.1. Script Files

All CLI Scripts to be executed on a pre-defined event are included in a *Script file*. Basically, the format of the Script file is identical to the format of the CLI configuration (see chapter *7.2.1 File Formats of Switch Configuration*). With this solution you can execute every available CLI command.

The Script file is not part of the running configuration and needs to be uploaded separately to the switch, equal to the Customer Reboot/Default Configuration.

A Script file can be up to 128 kB in size and is divided into two parts: The “CLI Script Definitions” part and the “Running CLI Configuration” part.

“CLI Script Definitions” part:

The “CLI Script Definitions” part consists of up to 1024 CLI Script sections, where each section defines one CLI Script with a maximum size of 4 kB. The syntax of a CLI Script section is as follows:

```
#START <CLI Script name>#

<List of CLI commands>

#END <CLI Script name>#
```

Here all CLI commands enclosed by the `START` and `END` tags belong to the CLI Script with the name `<CLI Script name>`. The CLI Script name must be a unique text label.

“Running CLI Configuration” part:

In the “Running CLI Configuration” part the pre-defined events are configured, i.e. a CLI Script is assigned to the corresponding events. One CLI Script can be assigned to one or more events. If multiple CLI Scripts are consecutively assigned to the same event, the last assigned CLI Script will be executed.

For each event that you want to configure, you must add a respective CLI command.

Currently, the following pre-defined events are configurable for CLI Scripts:

Event	Resulting action
Link-Up	Start CLI Script if the link on the configured port(s) is up
Link-Down	Start CLI Script if the link on the configured port(s) is down
Link-Change	Start CLI Script if the link on the configured port(s) has changed from Link-Down to Link-Up or vice versa

IMPORTANT NOTE:

Based on the customer’s needs, we can extend the support for further events in short term on demand. Basically, we can implement a CLI Script assignment for every useful alarm or action event that is available in the Alarm Destination Table (see chapter *10.54. Alarm Destination Table*).

7.4.1.1. Assign CLI Script to Event for Status Change on Ports

To assign a CLI Script to a Link-Up, Link-Down or Link-Change event on one or more ports, you must call the following CLI command:

```
cli-script interface {if-no range} {link-u:p|link-d:own|link-change} assign
<CLI Script name>
```

7.4.1.2. Delete CLI Script from Event for Status Change on Ports

To delete the assigned CLI Script from a Link-Up, Link-Down and Link-Change events on one or more ports, you must call the following CLI command:

```
cli-script interface {if-no range} {link-u:p|link-d:own|link-change} delete
```

7.4.2. Scripting using NEXMAN

Modification and management of the Script file can be performed using Nexans Device Manager (NEXMAN). NEXMAN will store the Script files in the so-called 'Database folder'. For each switch a file of the name `a_b_c_d.script` is created (a_b_c_d is the IP address a.b.c.d of the switch).

Reading and writing the Script file via NEXMAN is done exclusively via SCP. Here the switch is working as SCP server using TCP port 50271. For more information see chapter *7.4.3 Reading and Writing Script File per PC Console and SCP*.

7.4.3. Reading and Writing Script File per PC Console and SCP

A Script file can be written via Secure Copy (SCP) protocol to the switch or read by the switch. Under Windows you can use e. g. the “pscp.exe” program, which is included in the SSH/Telnet Client “PuTTY” package (see http://www.putty.org). For Linux operating systems the standard command “scp” is available for this purpose.

7.4.3.1. Reading Script File per PC Console and SCP

For reading a Script file from the switch the following syntax applies:

Windows: `pscp -scp -P 50271 <username>@<ip-address>:/cli_script <filename>`
Linux: `scp -P 50271 <username>@<ip-address>:/cli_script <filename>`

7.4.3.2. Writing Script File per PC Console and SCP

For writing a Script file to the switch the following syntax applies:

Windows: `pscp -scp -P 50271 <filename> <username>@<ip-address>:/cli_script`
Linux: `scp -P 50271 <filename> <username>@<ip-address>:/cli_script`

NOTE:

To delete Scripting, you must write an empty Script file to the switch.

7.4.4. Scripting Examples

7.4.4.1. Change Switch Name on Link-Up / Link-Down Event

```
# Define CLI Scripts for system events

#START LINK_UP_SCRIPT#
set name Connected Switch
#END LINK_UP_SCRIPT#

#START LINK_DOWN_SCRIPT#
set name Disconnected Switch
#END LINK_DOWN_SCRIPT#


# Assign CLI Scripts to system events on ports

cli-script interface 3 link-up assign LINK_UP_SCRIPT
cli-script interface 3 link-down assign LINK_DOWN_SCRIPT
```

7.4.4.2. Change Admin State and VLANs on Link-Up / Link-Down Event

```
# Define CLI Scripts for system events
```

```
#START SCRIPT_1#
set name SCRIPT_1
interface 5 admin-state enable
interface 6 admin-state disable
interface 2 vlan-id 55
interface 2 voice-vlan-id 100
#END SCRIPT_1#

#START SCRIPT_2#
set name SCRIPT_2
interface 6 admin-state enable
interface 5 admin-state disable
interface 2 vlan-id 1
interface 2 voice-vlan-id 1
#END SCRIPT_2#


# Assign CLI Scripts to system events on ports

cli-script interface 3 link-up assign SCRIPT_1
cli-script interface 3 link-down assign SCRIPT_2
```

7.5. TFTP Authentication using SNMP

The authentication method using SNMP described here does only apply to TFTP transfers via PC console. Principally, reading and writing the configuration and updating the firmware via PC console require prior authentication which, when using NEXMAN, is performed using a proprietary protocol via UDP port 50266.

Alternatively, authentication can also be performed using the SNMP Get or Set request.
The corresponding MIB variable is:

```
iso(1).
 org(3).
  dod(6).
   internet(1).
    private(4).
     enterprises(1).
      nexansActiveNetworkingSystems(266).
       bmSwitchManagement(20).
        bmSwitchAdmin(2).
         adminTftpAcces(17)
```

This variable can have the following values:

```
1) tftpAccessDisable(1)
2) tftpAccessReadOnly(2)
3) tftpAccessReadWrite(3)
```

The 'TFTP Authentication via SNMP' setting allows you to define in which way authentication is permitted via this variable.
The following modes are available:

- Disabled: No authentication possible via SNMP
- Read/Only Authentication only possible for reading the configuration
- Read/Write: Authentication possible for reading/writing the configuration and firmware update

After successful authentication via SNMP only one single TFTP transfer may be performed. After completion of the TFTP transfer the TFTP access is immediately blocked again.

Disabled (Factory Default):
No authentication possible via SNMP.

Read/Only:
With this setting reading the configuration can be authenticated only.
However, authentication can be performed in various ways:
a) SNMP Get request with the correct read/trap community
b) SNMP Set request with the value of tftpAccessReadOnly(2) and the correct write/read community
c) SNMP Set request with the value of tftpAccessReadWrite(3) and the correct write/read community

Read/Write:
With this setting reading and writing the configuration and a firmware update can be authenticated.

Authentication for reading the configuration can be performed in the same ways as described above for 'Read/Only'. However, authentication for writing the configuration and the firmware update can exclusively be performed using an SNMP Set request with the value of tftpAccessReadWrite(3) and using the correct write/read community.

NOTE:
Authentication via SNMP Set request is only possible, if the 'SNMP access mode' is set to {Read/Write}.

8. Resetting to Factory Default

The following resetting commands are available:

- Reboot with Factory Default
- Reboot with Factory Default (Except IP Parameters)
- Reboot without customer reboot settings
- Reboot with customer default settings
- Reset Total Boots Counter
- Reset Total Operation Time
- Reset Local Logging
- Reset Firmware on Memory Card

Reboot (Cold Start)
The switch performs a Cold Start. If a Customer Reboot configuration is available, the current configuration will be overwritten with the Reboot Configuration parameters.

Reboot with Factory Default :
Above all, the factory settings have to be restored when the switch is inadvertently configured incorrectly and can therefore not be accessed by the management procedure. The reset can be made using the configuration switches (see next chapter) or, if the Management can still be reached, using the Management function via the WEB, CLI, SNMP and Manager interfaces.

Reboot with Factory Default (Except IP Parameters):
This command switches all settings, except the IP parameters, to Factory Default.

Reboot without customer reboot settings
If a Customer Reboot Configuration is available, this option will perform a reboot without overwriting the current configuration with the Customer Reboot Configuration parameters.

Reboot with customer default settings
This option will boot the switch using the defined Customer Default Configuration. In this case all parameters are set to Factory Default and then the Customer Default Configuration parameters are loaded.

Reset Total Boots Counter:
This command resets the counter for the number of reboots.
NOTE: It is not possible to delete this counter using the “Reboot with Factory Default” command.

Reset Total Operation Time:
This command resets the indicated Total Operation Time.
NOTE: The Total Operation Time is only supported for switches manufactured from 2009. It is not possible to delete this value using the “Reboot with Factory Default” command.

Reset Local Logging:
This command deletes the local SYSLOG of the switch.

Reset Firmware on Memory Card:
This command deletes the firmware stored on MC.

Reset Total Boots Counter, Port Counters, Total Operation Time, Local Logging and Firmware on Memory Card
This command combines the listed Reset commands.

8.1. Reset to Factory Default Settings via configuration switch

The factory default settings must be restored when the switch is inadvertently configured incorrectly and can therefore not be accessed via the management procedure.

IMPORTANT NOTE:
If the configuration switches have been disabled via the management feature, please proceed as indicated in chapter *3.5. Disabling Configuration Switches*. In case of an enabled configuration switch please proceed as follows:

1	**Booting with Factory Default Settings** Booting the switch via the configuration switches with factory default settings. Detailed procedure see chapter *3.4 Management Configuration Switches and Pushbuttons.*
2	**Check, if the Status-LED on the management module lights up permanently** Notes on the function of the Status-LED see chapter *3.3 Management Status-LED*.
3	**Booting with flash configuration** Booting the switch via the configuration switches with flash configuration. Detailed procedure see chapter *3.4 Management Configuration Switches and Pushbuttons*.
4	**Check, if the Status-LED on the management module lights up permanently** Now the switch has been successfully restored to Factory Default settings.

9. Summary of all State and Configuration Parameters

The following tables contain summaries of all state and configuration parameters. The particular table headlines are identical to tab names of Device-Editor within the Nexans Manager V3.

For each parameter it is indicated how it can be displayed and/or configured in NEXMAN, WEB, Telnet/SSH/V.24 console and SNMP.
Lines containing a '-' mean, that this parameter cannot be displayed and/or configured via the respective interface.

IMPORTANT:
The functions described in this document are not supported by all switch types and/or firmware versions.

The words in the lines have the following meaning:

Chapter:
Indication of the chapter containing detailed information on the function of this parameter.

WEB:
Indication of the link description in the upper browser frame. After clicking on the indicated link the page, on which the respective parameter is listed, will be displayed.

Console Show:
The indicated console command can be used to display the respective state within the Telnet and V.24 console. For configuration parameters the configuration setting currently stored in the flash will be displayed.

Console Set:
The indicated console command can be used to edit the respective configuration parameter within the Telnet and V.24 console.

SNMP OID:
Indication of the respective MIB and of the name of the MIB variable. If a parameter should be available in several MIBs, these MIB's are listed one below the other. The respective MIB should be consulted for the complete OID.

9.1. Notes on the Console Command Syntax

Almost all commands and parameters can be entered in their abbreviated form. The colon (:) designates the minimum number of characters in the command list. The colon is not part of the command and must be omitted in the entry.

The following special characters are used here:

# ...	Command is available on Admin access level only.
> ...	Command is available on Admin and User access levels.
:	Separator for abbreviated entry of the command.
	E.g. for the command 'sh:ow' both 'sh', 'sho' and 'show' may be entered.
{...}	List of alternative parameters. Only one of the parameters listed may be entered.
[...]	This parameter is optional and may be omitted.
(a...b)	Numerical parameter with indication of the admissible min and max values.
<string ...>	String parameter with indication of the admissible number of characters.
<ip-address>	IP address in the a.b.c.d format.

The Telnet console supports a history buffer, which stores the last 10 entered commands. The keys ↑ and ↓ can be used to scroll through the buffer.

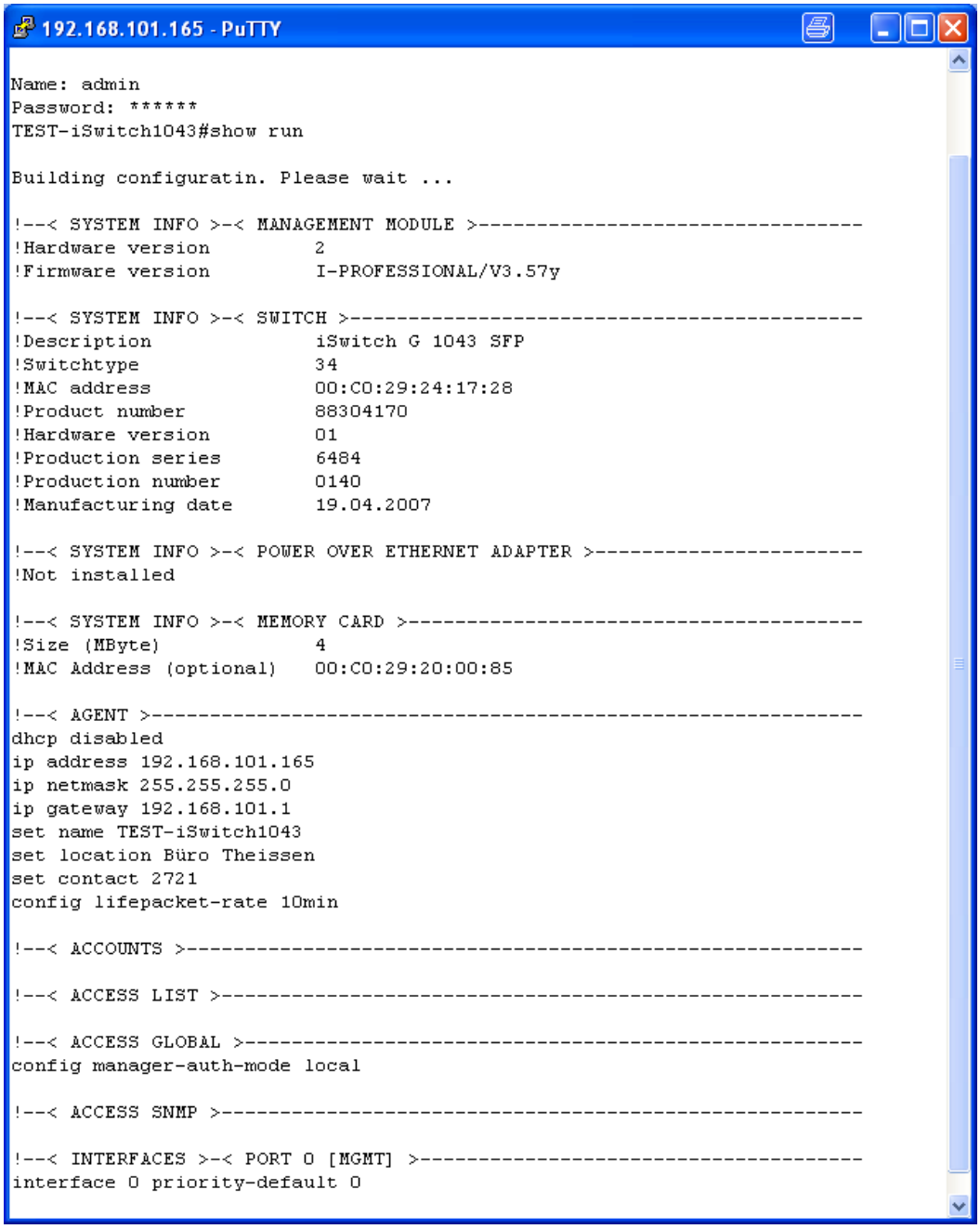
9.2. Display Current Configuration on the Console

The current configuration of the switch can be displayed using the Console command `sh:ow ru:nning-config [a:ll]`.

Without indication of the optional "all" parameter only settings deviating from factory default will be displayed. With indication of the "all" parameter all configuration settings, also those set to factory default, will be displayed.

After sending the command, first the configuration file is created in the memory and then output to the console page by page.

Example:



NOTE: The 'sh:ow ru:nning-config [a:ll]' command requires an installed management hardware version 2.

Alternatively the configuration can also be displayed depending on functional assignment. Here the following commands are available (non-exhaustive listing):

```
# sh:ow con:figuration acce:ss [a:ll]
# sh:ow con:figuration acco:unts [a:ll]
# sh:ow con:figuration al:arm-destinations [a:ll]
```

```
# sh:ow con:figuration ag:ent [a:ll]
> sh:ow con:figuration di:scovery [a:ll]
# sh:ow con:figuration do:t1x [a:ll]
> sh:ow con:figuration g:lobal [a:ll]
> sh:ow con:figuration ig:mp [a:ll]
> sh:ow con:figuration in:terfaces [a:ll]
> sh:ow con:figuration p:riorisation [a:ll]
# sh:ow con:figuration ra:dius [a:ll]
> sh:ow con:figuration re:dundancy [a:ll]
> sh:ow con:figuration sf:p-limits [a:ll]
> sh:ow con:figuration s:ntp [a:ll]
> sh:ow con:figuration v:lan [a:ll]
```

The function of the optional "all" parameter is identical with the command 'sh:ow ru:nning-config [a:ll]'.

9.3. Reset Commands

Designation	Access	
Global Reset Commands		
Reboot	Chapter:	*3.6.1. Booting with Flash Configuration (Normal Mode)*
	WEB:	Switch Setup → Reset Command → Reboot
	Console Set:	`# rel:oad`
	SNMP OID:	`NEXANS-BM-MIB → adminReset → rebootSwitch`
Reboot with Factory Defaults	Chapter:	*8. Resetting to Factory Default*
	WEB:	Switch Setup → Reset Command → Reboot with Factory Defaults
	Console Set:	`# rel:oad f:actory-a:ll`
	SNMP OID:	`NEXANS-BM-MIB → adminReset → rebootToFactoryDefaults`
Reboot with Factory Defaults (Except IP Parameters)	Chapter:	*8. Resetting to Factory Default*
	WEB:	-
	Console Set:	`# rel:oad f:actory-w:thout-ip`
	SNMP OID:	-
Reset Total Boots Counter	Chapter:	*8. Resetting to Factory Default*
	WEB:	Switch Setup → Reset Command → Reset Total Boots Counter
	Console Set:	`# res:et b:oots`
	SNMP OID:	-
Reset Total Operation Time	Chapter:	*8. Resetting to Factory Default*
	WEB:	Switch Setup → Reset Command → Reset Total Operation Time
	Console Set:	`# res:et o:peration-time`
	SNMP OID:	-
Reset all Counters	Chapter:	*10.27. Reset all Port* Counters
	WEB:	Switch Setup → Reset Command → Reset all counters
	Console Set:	`> res:et c:ounter`
	SNMP OID:	`NEXANS-BM-MIB → adminReset → resetCounters`
Renew IP- und VLAN-Parameter	Chapter:	*10.8. Configuration of IP and VLAN Parameters*
	WEB:	Switch Setup → Renew IP- and VLAN Parameter
	Console Set:	`# ren:ew`
	SNMP OID:	`NEXANS-BM-MIB → adminReset → renewIpAndVlanParameter`

Reset Local Logging	Chapter:	*9.25 Alarms > Alarm Destinations*
	WEB:	Local Log → Delete Log
	Console Set:	`# sh:ow l:og delete`
	SNMP OID:	-
Reset Firmware on Memory Card	Chapter:	*4.5 Memory Card Firmware-Update*
	WEB:	Switch Setup → Reset Command → Reset Firmware on Memory Card
	Console Set:	`> res:et f :irmware-memory-card`
	SNMP OID:	-
Port Reset Commands		
Renew Portsecurity	Chapter:	*10.36.5. Portsecurity - Renew Command*
	WEB:	Port State → Setup → Renew Security and Enable Port
	Console Set:	`# in:terface {if-no range} se:curity-mode r:enew`
	SNMP OID:	`NEXANS-BM-MIB → portSecurityAdminState → renew`
Reset PoE Power	Chapter:	*11.1.7. PoE Reset Command*
	WEB:	PoE State → Setup → Reset
	Console Set:	`# in:terface {if-no range} poe-s:etup r:eset`
	SNMP OID:	`NEXANS-BM-MIB → portPoeAdminState → reset`

9.4. State > Global + Link State

Designation	Access	
Global		
Show all Counters	Chapter:	*10.52. Statistic / RMON Counters*
	WEB:	Port State → All Counters
	Console Show:	`> sh:ow cou:nter <if-no>`

	SNMP OID:	`MIB-II → interfaces`
		`IF-MIB → ifXTable`
		`BRIDGE-MIB → dot1dTpPortTable`
		`EtherLike-MIB → dot3StatsTable`
		`RMON-MIB → statistics`

Reset all Counters		
Show Neighbors	Chapter:	*10.70. Link Layer Discovery Protocol (LLDP)* *10.72. Cisco Discovery Protocol (CDP)*
	WEB:	-
	Console Show:	`> sh:ow n:eighbors-table [<if-no>|c:lear-table]`
	SNMP OID:	-
Show SFP Info	Chapter:	*10.25. SFP Info, Diag*
	WEB:	Port+Alarm State
	Console Show:	`> sh:ow sf:p-info [<if-no>]`
	SNMP OID:	-
Show IGMP State	Chapter:	*10.69.1. IGMP Snooping*
	WEB:	-
	Console Show:	`> sh:ow ig:mp`
	SNMP OID:	-

Show STP State	Chapter:	*10.73. Rapid Spanning Tree Protocol (RSTP)* *10.74. Multiple Spanning Tree Protocol (MSTP)*
	WEB:	Spanning Tree State
	Console Show:	`> sh:ow rs:tp` `> sh:ow ms:tp [instance-id]`
	SNMP OID:	-
Cable Diagnostic all TP Ports	Chapter:	*10.23Cable Diagnostic for Twisted-Pair*
	WEB:	Cable Diagnostic
	Console Show:	`> ca:ble-diagnostic {<if-no>|a:ll}`
	SNMP OID:	-
Show MRP State	Chapter:	*10.76. Media Redundancy Protocol (MRP)*
	WEB:	-
	Console Show:	`> sh:ow mr:p`
	SNMP OID:	-
Global State		
Temperature (°C)	Chapter:	*10.29. Switch Temperature*
	WEB:	Info
	Console Show:	`> sh:ow inf:o`
	SNMP OID:	`NEXANS-BM-MIB → infoTemperature`
Internal Voltage 1 (V) Internal Voltage 2 (V)	Chapter:	*10.30. Switch Operating Voltages*
	WEB:	Info
	Console Show:	`> sh:ow inf:o`
	SNMP OID:	`NEXANS-BM-MIB → infoPowerVoltage2500` `NEXANS-BM-MIB → infoPowerVoltage3300`
PoE Input Voltage (V)	Chapter:	*11.1.1. PoE Measured Values*
	WEB:	PoE State
	Console Show:	`> sh:ow p:oe`
	SNMP OID:	`NEXANS-BM-MIB → infoPoeInputVoltage`
System Uptime	Chapter:	*10.28.1. System Uptime*
	WEB:	Info
	Console Show:	`> sh:ow inf:o`
	SNMP OID:	`MIB-II → sysUpTime`
Time from time server	Chapter:	*10.28.3. Network Time Protocol - SNTP*
	WEB:	Info
	Console Show:	`> sh:ow inf:o`
	SNMP OID:	`NEXANS-BM-MIB → infoLastSntpTime`
Active MAC Address	Chapter:	*10.2. Determination of the active MAC Address*
	WEB:	Info
	Console Show:	`> sh:ow inf:o`
	SNMP OID:	`NEXANS-BM-MIB → adminAgentPhysAddress`
Memory Card	Chapter:	*4. Memory Card (MC)*
	WEB:	Info
	Console Show:	`> sh:ow inf:o`
	SNMP OID:	-

Power Input S1 (V)	Chapter: *10.30. Switch Operating Voltages* WEB: Port+Alarm State Console Show: `> sh:ow al:arms` SNMP OID: `NEXANS-BM-MIB → infoS1InputVoltage`
Power Input S2 (V)	Chapter: *10.30. Switch Operating Voltages* WEB: Port+Alarm State Console Show: `> sh:ow al:arms` SNMP OID: `NEXANS-BM-MIB → infoS1InputVoltage`
Industrial State	
Alarm Output M1	Chapter: *10.47. Alarm Outputs for Industrial Switches* WEB: Port+Alarm State Console Show: `> sh:ow al:arms` SNMP OID: `NEXANS-BM-MIB → infoAlarmStateM1`
Alarm Output M2	Chapter: *10.47. Alarm Outputs for Industrial Switches* WEB: Port+Alarm State Console Show: `> sh:ow al:arms` SNMP OID: `NEXANS-BM-MIB → infoAlarmStateM2`
Function Input	Chapter: *10.47. Alarm Outputs for Industrial Switches* WEB: Port+Alarm State Console Show: `> sh:ow al:arms` SNMP OID: -
Port Link State	
Link State	Chapter: *10.21. Link / EEE State* WEB: Port State Console Show: `> sh:ow int:erfaces [<if-no>]` SNMP OID: `NEXANS-BM-MIB → portLinkState`
Link/SFP Alarm State	
Time since last link change	Chapter: *10.28.2. Time Since Last Link* WEB: - Console Show: - SNMP OID: `MIB-II → ifLastChange`
Error Counter	Chapter: *10.26. Error Counter* WEB: Port State Console Show: `> sh:ow int:erfaces` SNMP OID: `NEXANS-BM-MIB → portErrorCounter`
Security State	Chapter: *10.36.4. Portsecurity – Security State* WEB: Port State Console Show: `> sh:ow se:curity` SNMP OID: `NEXANS-BM-MIB → portSecurityForwardingState`
Active Default VLAN	Chapter: *10.31.11. Active Default VLAN-ID* WEB: Port State Console Show: `> sh:ow int:erfaces` SNMP OID: `NEXANS-BM-MIB → portActiveDefaultVlanId`

Active Voice VLAN	Chapter: *10.31.12. Active Voice VLAN-ID* WEB: Port State Console Show: `> sh:ow int:erfaces` SNMP OID: `NEXANS-BM-MIB → portActiveVoiceVlanId`
Active Trunking Mode	Chapter: *10.31.13. Active Trunking Mode* WEB: Port State Console Show: `> sh:ow int:erfaces` SNMP OID: -
Flow Control State	Chapter: *10.44. Flow Control* WEB: Port State Console Show: `sh:ow f:low-control` SNMP OID: -
Redundancy State	Chapter: *10.73. Rapid Spanning Tree Protocol (RSTP)* *10.74. Multiple Spanning Tree Protocol (MSTP)* WEB: Spanning Tree State Console Show: `sh:ow rs:tp` `sh:ow ms:tp` SNMP OID: -

9.5. State > MAC + Security State

Designation	Access
Global	
MAC Table	Chapter: *10.37. MAC Address Table* WEB: - Console Show: `> sh:ow ma:c-address-table d:ynamic [<if-no>|a:ll]` `Show MAC addresses of all User ports only (no Uplink ports). Use option '<if-no>' to show MAC addresses of this port only. Use option 'a:ll' to show MAC addresses of all ports.` SNMP OID: `BRIDGE-MIB → dot1dTpFdbTable`
Ping from Device	Chapter: - WEB: - Console Show: `> pi:ng <ip-address>` SNMP OID: -
Port Security State	
Security State	Chapter: *10.36.4. Portsecurity – Security State* WEB: Port State Console Show: `> sh:ow se:curity` SNMP OID: `NEXANS-BM-MIB → portSecurityForwardingState`
Active Default VLAN-ID	Chapter: *10.31.11. Active Default VLAN-ID* WEB: Port State Console Show: `> sh:ow int:erfaces` SNMP OID: `NEXANS-BM-MIB → portActiveDefaultVlanId`

Active Voice VLAN	Chapter: *10.31.12. Active Voice VLAN-ID* WEB: Port State Console Show: `> sh:ow int:erfaces` SNMP OID: `NEXANS-BM-MIB → portActiveVoiceVlanId`
Allowed MACs Oberflow Address	Chapter: *10.36.3. Portsecurity - Allowed MACs Overflow Address* WEB: Port State → [Failure MAC Address] Console Show: - SNMP OID: `NEXANS-BM-MIB → infoSecurityFailMacAddr`

MAC Address 1
MAC Address 2
MAC Address 3
	Chapter: *10.36.10. Portsecurity - MAC Addresses*
	WEB: Port State → [MAC Addr.]
	Console Show: `> sh:ow se:curity`
	SNMP OID: `NEXANS-BM-MIB → portSecurityMacAddr1`
	`NEXANS-BM-MIB → portSecurityMacAddr2`
	`NEXANS-BM-MIB → portSecurityMacAddr3`

MAC State 1 MAC State 2 MAC State 3	Chapter: *10.36.11. Portsecurity - MAC State* WEB: Port State → (MAC State) Console Show: `> sh:ow se:curity` SNMP OID: -

9.6. State > PoE State

Designation	Access
Port PoE State	
PoE Voltage (V)	Chapter: *11.1.1. PoE Measured Values* WEB: PoE State Console Show: `> sh:ow p:oe` SNMP OID: `NEXANS-BM-MIB → portPoeVoltage`
PoE Current (mA)	Chapter: *11.1.1. PoE Measured Values* WEB: PoE State Console Show: `> sh:ow p:oe` SNMP OID: `NEXANS-BM-MIB → portPoeCurrent`
PoE Power (W)	Chapter: *11.1.1. PoE Measured Values* WEB: PoE State Console Show: `> sh:ow p:oe` SNMP OID: `NEXANS-BM-MIB → portPoePower (in mVA)`
PoE Power class	Chapter: *11.1.1. PoE Measured Values* WEB: PoE State Console Show: `> sh:ow p:oe` SNMP OID: -
Power Supply State	
PoE Input Voltage (V)	Chapter: *11.1.1. PoE Measured Values* WEB: PoE State Console Show: `> sh:ow p:oe` SNMP OID: `NEXANS-BM-MIB → infoPoeInputVoltage`

PoE Input Current (mA)	Chapter: *11.1.1. PoE Measured Values* WEB: PoE State Console Show: `> sh:ow p:oe` SNMP OID: -
PoE Input Power (W)	Chapter: *11.1.1. PoE Measured Values* WEB: PoE State Console Show: `> sh:ow p:oe` SNMP OID: `NEXANS-BM-MIB → infoPoeInputPower (in mVA)`

9.7. State > Radius State

Designation	Access
RADIUS Server State	
Global Authentication Server 1 - 4	Chapter: *10.55. RADIUS Authentication* WEB: - Console Show: `> sh:ow ra:dius` SNMP OID: -
Management Authentication Server 1 - 4	Chapter: *10.55. RADIUS Authentication* WEB: - Console Show: `> sh:ow ra:dius` SNMP OID: -
Accounting Server 1 - 4	Chapter: *10.60. RADIUS Accounting* WEB: - Console Show: `> sh:ow ra:dius` SNMP OID: -

9.8. State > TACACS+ State

Designation	Access
TACACS+ Server State	
Authentication Server 1 - 4	Chapter: *10.61 TACACS+ Authentication* WEB: - Console Show: `> sh:ow ta:cacs+` SNMP OID: -
Authorization Server 1 - 4	Chapter: *10.62 TACACS+ Authorization* WEB: - Console Show: `> sh:ow ta:cacs+` SNMP OID: -
Accounting Server 1 - 4	Chapter: *10.63 TACACS+ Accounting* WEB: - Console Show: `> sh:ow ta:cacs+` SNMP OID: -

9.9. Device Info

Designation	Access
Management Info	
Management Hardwareversion	Chapter: *10.1. Determination of Switch Type and Management Version* WEB: Device Info Console Show: `> sh:ow inf:o` SNMP OID: `NEXANS-BM-MIB → infoMgmtHardwareVersion`
Management Firmware version	Chapter: *10.1. Determination of Switch Type and Management Version* WEB: Device Info Console Show: `> sh:ow inf:o` SNMP OID: `NEXANS-BM-MIB → infoMgmtFirmwareVersion`
Backup Firmware version (HW5 switches only)	Chapter: *10.1. Determination of Switch Type and Management Version* WEB: Device Info Console Show: `> sh:ow inf:o` SNMP OID: -
Switch Info	
Description	Chapter: *10.1. Determination of Switch Type and Management Version* WEB: Device Info Console Show: `> sh:ow inf:o` SNMP OID: `NEXANS-BM-MIB → infoDescr`
Switch type	Chapter: *10.1. Determination of Switch Type and Management Version* WEB: Device Info Console Show: `> sh:ow inf:o` SNMP OID: `NEXANS-BM-MIB → infoType`
MAC Address	Chapter: *10.1. Determination of Switch Type and Management Version* WEB: Device Info Console Show: `> sh:ow inf:o` SNMP OID: `NEXANS-BM-MIB → adminAgentPhysAddress`
Part Number (P/N)	Chapter: *10.1. Determination of Switch Type and Management Version* WEB: Device Info Console Show: `> sh:ow inf:o` SNMP OID: `NEXANS-BM-MIB → infoProductNo`
Switch Hardwareversion	Chapter: *10.1. Determination of Switch Type and Management Version* WEB: Device Info Console Show: `> sh:ow inf:o` SNMP OID: `NEXANS-BM-MIB → infoSwitchHardwareVersion`
Production Lot	Chapter: *10.1. Determination of Switch Type and Management Version* WEB: Info Console Show: `> sh:ow inf:o` SNMP OID: `NEXANS-BM-MIB → infoSerie`
Series Number (S/N)	Chapter: *10.1. Determination of Switch Type and Management Version* WEB: Device Info Console Show: `> sh:ow inf:o` SNMP OID: `NEXANS-BM-MIB → infoSeriesNo`

Manufacturing Date	Chapter: *10.1. Determination of Switch Type and Management Version* WEB: Device Info Console Show: `> sh:ow inf:o` SNMP OID: `NEXANS-BM-MIB → infoManufactureDate`
PoE Adapter Info	
Description	Chapter: *11. Power-over-Ethernet (PoE) Functional Description* WEB: Device Info Console Show: `> sh:ow inf:o` SNMP OID: -
Part Number (P/N)	Chapter: *11. Power-over-Ethernet (PoE) Functional Description* WEB: Device Info Console Show: `> sh:ow inf:o` SNMP OID: -
Adapter Hardwareversion	Chapter: *11. Power-over-Ethernet (PoE) Functional Description* WEB: Device Info Console Show: `> sh:ow inf:o` SNMP OID: -
Production Lot	Chapter: *11. Power-over-Ethernet (PoE) Functional Description* WEB: Device Info Console Show: `> sh:ow inf:o` SNMP OID: -
Series Number (S/N)	Chapter: *11. Power-over-Ethernet (PoE) Functional Description* WEB: Device Info Console Show: `> sh:ow inf:o` SNMP OID: -
Manufacturing Date	Chapter: *11. Power-over-Ethernet (PoE) Functional Description* WEB: Device Info Console Show: `> sh:ow inf:o` SNMP OID: -
Memory Card Info	
Card Type	Chapter: *4. Memory Card (MC)* WEB: Device Info Console Show: `> sh:ow inf:o` SNMP OID: -
Write-Protection (DIP F2) (HW5 iSwitches only)	Chapter: *4. Memory Card (MC)* WEB: Device Info Console Show: `> sh:ow inf:o` SNMP OID: -
MAC Address	Chapter: *4. Memory Card (MC)* WEB: Device Info Console Show: `> sh:ow inf:o` SNMP OID: -

Licence	Chapter:	*4. Memory Card (MC)*
	WEB:	Device Info
	Console Show:	`> sh:ow inf:o`
	SNMP OID:	-

9.10. Port Setup

Designation	Access	
Port Global		
Name	Chapter:	*10.40. Port Name*
	WEB:	Port State
	Console Show:	`> sh:ow con:figuration in:terfaces [a:ll]` `> sh:ow int:erfaces [a:ll]`
	Console Set:	`# in:terface {if-no range} na:me [<string max. 64 chars>]`
	SNMP OID:	`NEXANS-BM-MIB → portName`
Type	Chapter:	*10.41. Port Type*
	WEB:	Port State → Setup
	Console Show:	`> sh:ow con:figuration in:terfaces [a:ll]`
	SNMP OID:	-
Port Link-Setup		
Link Type	Chapter:	*10.20.1. Link Type*
	WEB:	Port State
	Console Show:	`> sh:ow con:figuration in:terfaces [a:ll]`

	Console Set:	`# in:terface {if-no range} link-t:ype {setup}`
		`Valid values for {setup} are:`
		`{up:link-downlink|us:erport|l:oop-protected}`

	SNMP OID:	`NEXANS-BM-MIB → portLinkType`
Admin State	Chapter:	*10.20.2. Admin State*
	WEB:	Port State → Setup
	Console Show:	`> sh:ow con:figuration in:terfaces [a:ll]`
	Console Set:	`# in:terface {if-no range} ad:min-state {e:nable|d:isable}`
	SNMP OID:	`NEXANS-BM-MIB → portAdminState`
Shutdown if no link	Chapter:	*10.20.3 Shutdown Port if no Link*
	WEB:	-
	Console Show:	-

	Console Set:	`# in:terface {if-no range} shutdown-no-link {setup}`
		`Valid values for {setup} are:`
		`{di:sable|o:ne-time|p:ermanent|de:layed-permanent}`

	SNMP OID:	-

Speed/Duplex	Chapter:	*10.20.4. Speed/Duplex*
	WEB:	Port State
	Console Show:	`> sh:ow con:figuration in:terfaces [a:ll]` `> sh:ow int:erfaces`

	Console Set:	`# in:terface {if-no range} sp:eed-duplex {setup}`
		`Valid values for {setup} are:`
		`a:utoneg`
		`e:co`
		`1000f:dx`
		`100f:dx`
		`100h:dx`
		`10f:dx`
		`10h:dx`

	SNMP OID:	`NEXANS-BM-MIB → portSpeedDuplexSetup`
Autocross/ Autopolarity	Chapter:	*10.20.8. Autocrossover/Autopolarity*
	WEB:	Port State
	Console Show:	`> sh:ow con:figuration in:terfaces [a:ll]`
	Console Set:	`# in:terface {if-no range} au:to-cross {e:nable|d:isable}`
	SNMP OID:	`NEXANS-BM-MIB → portAcApSetup`
Remote Fault enable	Chapter:	*10.24. Remote Fault*
	WEB:	Port State → Setup
	Console Show:	`> sh:ow con:figuration in:terfaces [a:ll]`
	Console Set:	`# in:terface {if-no range} re:mote-fault {e:nable|d:isable}`
	SNMP OID:	`NEXANS-BM-MIB → portRemoteFault`
Send Link Alarms	Chapter:	*10.22. Send Link Alarms*
	WEB:	-
	Console Show:	`> sh:ow con:figuration in:terfaces [a:ll]`
	Console Set:	`# in:terface {if-no range} link-a:larm {e:nabled|d:isabled}`
	SNMP OID:	-
Automatic Powersave	Chapter:	*10.20.5. Automatic Powersave*
	WEB:	-
	Console Show:	`> sh:ow con:figuration in:terfaces [a:ll]`

	Console Set:	`# in:terface {if-no range} auto-p:owersave {mode}`
		`Valid values for {mode} are:`
		`{d:isable|t:ime-client|p:oe-time-client}`

	SNMP OID:	-
Energy-Efficient Ethernet Enable	Chapter:	*10.20.6 Energy-Efficient Ethernet (EEE)*
	WEB:	-
	Console Show:	`> sh:ow con:figuration in:terfaces [a:ll]`
	Console Set:	`# in:terface {if-no range} ee:e {e:nable|d:isable}`
	SNMP OID:	-
Extended Powersave Enable	Chapter:	*10.20.7* Extended Powersave
	WEB:	-
	Console Show:	`> sh:ow con:figuration in:terfaces [a:ll]`
	Console Set:	`# in:terface {if-no range} ex:tended-powersave {e:nable|d:isable}`
	SNMP OID:	-

Client Remove Alarm	Chapter: *10.20.9. Client Remove Alarm*
	WEB: -
	Console Show: `> sh:ow con:figuration in:terfaces [a:ll]`
	Console Set: `# in:terface {if-no range} c:lient-remove-alarm {mode}`
	`Valid values for {mode} are:`
	`{d:isabled|l:ink-down-timeout}`
	SNMP OID: -

Link Down Timeout (seconds) (0…60000)	Chapter: *10.20.9. Client Remove Alarm* WEB: - Console Show: `> sh:ow con:figuration in:terfaces [a:ll]` Console Set: `# in:terface {if-no range} c:lient-remove-alarm l:ink-down-timeout (0...60000)` SNMP OID: -
Port Power over Ethernet (PoE)	

Power Setup	Chapter: *11.1.2. PoE Power Setup*
	WEB: PoE State
	Console Show: `> sh:ow con:figuration in:terfaces [a:ll]`
	`> sh:ow p:oe`
	Console Set: `# in:terface {if-no range} poe-s:etup {setup}`
	`Valid values for {setup} are:`
	`{d:isable|o:n-forced|au:to|af:-high-power|`
	`at:-high-power|r:eset}`
	SNMP OID: `NEXANS-BM-MIB → portPoeAdminState`

Powerlimit (W) (0…100)	Chapter: *11.1.3. PoE Power Limit per Port* WEB: PoE State Console Show: `> sh:ow con:figuration in:terfaces [a:ll]` `> sh:ow p:oe` Console Set: `# in:terface {if-no range} poe-l:imit (0...100)` SNMP OID: `NEXANS-BM-MIB → portPoePowerLimit`
Port Security	

Mode	Chapter: *10.36. Portsecurity*
	10.59. Portsecurity with authentication via RADIUS server
	WEB: Port State
	Console Show: `> sh:ow con:figuration in:terfaces [a:ll]`
	`> sh:ow se:curity`
	Console Set: `# in:terface {if-no range} se:curity-mode {setup}`
	`Valid values for {setup} are:`
	`{di:sabled|m:anual|v:endor|learn1|learn2|`
	`auto1|auto2|auto3|radius1|radius2|radius3|`
	`dot1x-o:ne|dot1x-p:c+voice|dot1x-a:ll|`
	`dot1x-m:ulti3|dot1x-s:upplicant}`
	SNMP OID: `NEXANS-BM-MIB → portSecurityAdminState`

MAC Address 1	Chapter: *10.36. Portsecurity* WEB: - Console Show: `> sh:ow con:figuration in:terfaces [a:ll]` `> sh:ow se:curity` Console Set: - SNMP OID: `NEXANS-BM-MIB → portSecurityMacAddr1`

MAC Address 2	Chapter: *10.36. Portsecurity* WEB: - Console Show: `> sh:ow con:figuration in:terfaces [a:ll]` `> sh:ow se:curity` Console Set: - SNMP OID: `NEXANS-BM-MIB → portSecurityMacAddr2`
MAC Address 3	Chapter: *10.36. Portsecurity* WEB: - Console Show: `> sh:ow con:figuration in:terfaces [a:ll]` `> sh:ow se:curity` Console Set: - SNMP OID: `NEXANS-BM-MIB → portSecurityMacAddr3`
Toggle Link	Chapter: *10.59.7. Portsecurity Option {Toggle Link}* WEB: - Console Show: `> sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius l:ink-interrupt i:nterface <if-no>` `{e:nabled|d:isabled}` SNMP OID: -
Renew	Chapter: *10.36.5. Portsecurity - Renew Command* WEB: - Console Set: `in:terface <if-no> se:curity-mode re:new` SNMP OID: `NEXANS-BM-MIB → portSecurityAdminState`
Port Prioritisation	
Default 802.1p Priority Level (Queue)	Chapter: *10.38.2. Prioritization according to IEEE802.1p* WEB: Prioritisation+Limiter Console Show: `> sh:ow con:figuration in:terfaces [a:ll]` Console Set: `# in:terface {if-no range} priority-de:fault` `(priority value=0..7)` SNMP OID: `NEXANS-BM-MIB → portDot1qDefaultPrioValue`
IEEE802.1p Prioritisation enable	Chapter: *10.38.2. Prioritization according to IEEE802.1p* WEB: Prioritisation+Limiter Console Show: `> sh:ow con:figuration in:terfaces [a:ll]` Console Set: `# in:terface {if-no range} priority-do:t1p` `{e:nable|d:isable}` SNMP OID: `NEXANS-BM-MIB → portPrioDot1p`
IEEE802.1p VLAN based priority override enable	Chapter: *10.38.3. IEEE802.1p VLAN based Priority Override* WEB: Prioritisation+Limiter Console Show: `> sh:ow con:figuration in:terfaces [a:ll]` Console Set: `# in:terface {if-no range} priority-v:lan` `{e:nable|d:isable}` SNMP OID: `NEXANS-BM-MIB → portPrioOverride`
Ipv4/IPv6 Prioritisation enable	Chapter: *10.38.4. Prioritization according to IPv4/IPv6* WEB: Prioritisation+Limiter Console Show: `> sh:ow con:figuration in:terfaces [a:ll]` Console Set: `# in:terface {if-no range} priority-i:p` `{e:nable|d:isable}` SNMP OID: `NEXANS-BM-MIB → portPrioIp`

Port LEDs		
Green LED	Chapter:	*10.42. Programming of Port Status-LEDs*
	WEB:	Port State
	Console Show:	`> sh:ow con:figuration in:terfaces [a:ll]`

	Console Set:	`# in:terface {if-no range} led-g:reen {mode}`
		`Valid values for {mode} are:`
		`{l:ink-activity|on|of:f}`

	SNMP OID:	`NEXANS-BM-MIB → portLEDGreen`
Yellow LED	Chapter:	*10.42. Programming of Port Status-LEDs*
	WEB:	Port State
	Console Show:	`> sh:ow con:figuration in:terfaces [a:ll]`

	Console Set:	`# in:terface {if-no range} led-y:ellow {mode}`
		`Valid values for {mode} are:`
		`{f:ull-duplex|poe|on|of:f}`

	SNMP OID:	`NEXANS-BM-MIB → portLEDYellow`
Port Bandwidth Limiter		
RX Bitrate	Chapter:	*10.43. Bandwidth Limiter*
	WEB:	Prioritisation+Limiter
	Console Show:	`> sh:ow con:figuration in:terfaces [a:ll]`

	Console Set:	`# in:terface {if-no range} limit-i:n {setup}`
		`Valid values for {setup} are:`
		`100BM switches:`
		`  {d:isabled|128k|256k|512k|1m|2m|3m|4m}`
		`1000BM switches:`
		`  {d:isabled|128k|256k|512k|1m|2m|4m|8m|`
		`  16m|32m|64m|128m|256m}`

	SNMP OID:	`NEXANS-BM-MIB → portDot1qDefaultPrioValue`
TX Bitrate	Chapter:	*10.43. Bandwidth Limiter*
	WEB:	Prioritisation+Limiter
	Console Show:	`> sh:ow con:figuration in:terfaces [a:ll]`

	Console Set:	`# in:terface {if-no range} limit-o:ut {setup}`
		`Valid values for {setup} are:`
		`100BM switches:`
		`{d:isabled|128k|256k|512k|1m|2m|3m|4m}`
		`1000BM switches:`
		`{d:isabled|128k|256k|512k|1m|2m|4m|8m|`
		`16m|32m|64m|128m|256m}`

	SNMP OID:	`NEXANS-BM-MIB → portDot1qDefaultPrioValue`
Packet Type	Chapter:	*10.43.2. Limiter Packet Type*
	WEB:	Prioritisation+Limiter
	Console Show:	`> sh:ow con:figuration in:terfaces [a:ll]`

	Console Set:	`# in:terface {if-no range} limit-p:acket-type {setup}`
		`Valid values for {setup} are:`
		`{a:ll|l:oop-bcast}`

	SNMP OID:	`NEXANS-BM-MIB → portLimiterPacketType`

9.11. IPv4 / IPv6 Setup

Designation	Access
IPv4 Setup	
DHCP enable	Chapter: *10.8. Configuration of IP and VLAN Parameters* WEB: Switch Setup Console Show: > sh:ow con:figuration ip [a:ll] Console Set: # dh:cp {e:nable|d:isable} SNMP OID: NEXANS-BM-MIB → adminAgentDhcp
DHCP/BOOTP Download Mode	Chapter: *7.2.5 Loading Switch Configuration automatically via DHCP/BootP* WEB: - Console Show: > sh:ow con:figuration ag:ent [a:ll] Console Set: # dh:cp t:ftp-download {e:nable|d:isable} SNMP OID: -
IPv4-Address	Chapter: *10.8. Configuration of IP and VLAN Parameters* WEB: Switch Setup Console Show: > sh:ow con:figuration ip [a:ll] > sh:ow d:hcp Console Set: # ip a:ddress <ip-address> SNMP OID: NEXANS-BM-MIB → adminAgentIpAddress MIB-II → ipAdEntAddr (Read/Only)
Netmask	Chapter: *10.8. Configuration of IP and VLAN Parameters* WEB: Switch Setup Console Show: > sh:ow con:figuration ip [a:ll] > sh:ow d:hcp Console Set: # ip n:etmask <ip-address> SNMP OID: NEXANS-BM-MIB → adminAgentNetmask MIB-II → ipAdEntNetMask (Read/Only)
Gateway	Chapter: *10.8. Configuration of IP and VLAN Parameters* WEB: Switch Setup Console Show: > sh:ow con:figuration ip [a:ll] > sh:ow d:hcp Console Set: # ip g:ateway <ip-address> SNMP OID: NEXANS-BM-MIB → adminAgentDefRouterIpAddress MIB-II → ipRouteNextHop (Read/Only)
DHCP Server	Chapter: *10.8. Configuration of IP and VLAN Parameters* WEB: - Console Show: > sh:ow d:hcp Console Set: - SNMP OID: NEXANS-BM-MIB → adminAgentDhcpServerIpAddress

IPv6 Setup	
IPv6 Access Mode	Chapter: *10.8. Configuration of IP and VLAN Parameters* WEB: Switch Setup Console Show: `> sh:ow con:figuration ip [a:ll]` Console Set: `ip v6 access-m:ode {mode} Valid values for {mode} are: {di:sabled|s:tatic-address|au:to-stateless|pr:ivacy-auto-stateless|dh:cpv6}` SNMP OID:
IPv6 Link Local Address	Chapter: *10.8. Configuration of IP and VLAN Parameters* WEB: Switch Setup Console Show: `> sh:ow con:figuration ip [a:ll]` Console Set: `n/a` SNMP OID:
IPv6-Address	Chapter: *10.8. Configuration of IP and VLAN Parameters* WEB: Switch Setup Console Show: `> sh:ow con:figuration ip[a:ll]` Console Set: `# ip v6 {ad:dress|g:ateway} <ipv6-address>` SNMP OID:
Subnet Prefix Length	Chapter: *10.8. Configuration of IP and VLAN Parameters* WEB: Switch Setup Console Show: `> sh:ow con:figuration ip[a:ll]` Console Set: `# ip v6 {s:ubnet-prefix} (0...128)` SNMP OID:
Gateway Address	Chapter: *10.8. Configuration of IP and VLAN Parameters* WEB: Switch Setup Console Show: `> sh:ow con:figuration ip[a:ll]` Console Set: `# ip v6 {ad:dress|g:ateway} <ipv6-address>` SNMP OID:
DHCP Server Address	Chapter: *10.8. Configuration of IP and VLAN Parameters* WEB: - Console Show: `> sh:ow d:hcp` Console Set: - SNMP OID:

9.12. Management > Agent

Designation	**Access**
Reset Action	
Reboot (Cold Start)	Chapter: *3.6.1. Booting with Flash Configuration (Normal Mode)* WEB: Switch Setup → Reset Command → Reboot Console Set: `# rel:oad` SNMP OID: `NEXANS-BM-MIB → adminReset → rebootSwitch`
Reboot with Factory Default	Chapter: *8. Resetting to Factory Default* WEB: Switch Setup → Reset Command → Reboot with Factory Default Console Set: `# rel:od factory-a:ll|` SNMP OID: `NEXANS-BM-MIB → adminReset → rebootToFactoryDefaults`

Reboot with Factory Default (Except IP Parameters)	Chapter: *8. Resetting to Factory Default* WEB: Switch Setup → Reset Command → Reboot with Factory Default Console Set: `# rel:od factory-w:ithout-ip` SNMP OID: -
Reboot without customer reboot settings	Chapter: *8. Resetting to Factory Default* WEB: - Console Set: `# rel:oad w:ithout-cust-reboot` SNMP OID: -
Reboot with customer default settings	Chapter: *8. Resetting to Factory Default* WEB: - Console Set: `# rel:oad c:ust-default` SNMP OID: -
Reset Total Boots Counter	Chapter: *8. Resetting to Factory Default* WEB: Switch Setup → Reset Command → Reset Total Boots Counter Console Set: `# res:et b:oots` SNMP OID: -
Reset Port Counters	Chapter: *10.27. Reset all Port Counters* WEB: Switch Setup → Reset Command → Reset all counters Console Set: `> res:et c:ounter` SNMP OID: `NEXANS-BM-MIB → adminReset → resetCounters`
Reset Total Operation Time	Chapter: *8. Resetting to Factory Default* WEB: Switch Setup → Reset Command → Reset Total Operation Time Console Set: `# res:et o:peration-time` SNMP OID: -
Reset Local Logging	Chapter: *8. Resetting to Factory Default* WEB: Local Log → Delete Log Console Set: `# sh:ow l:og [delete]` SNMP OID: -
Reset Firmware on Memory Card	Chapter: *4.5 Memory Card Firmware-Update* WEB: Switch Setup → Reset Command → Reset Firmware on Memory Card Console Set: `> res:et f :irmware-memory-card` SNMP OID: -
Reset Total Boots Counter, Port Counters, Total Operation Time, Local Logging and Firmware on Memory Card	Chapter: *8. Resetting to Factory Default* WEB: - Console Set: `# N/A` SNMP OID: -
Switch to backup firmware	Chapter: *7.1.1 Dual Firmware Storage* WEB: - Console Set: `# rel:oad b:ackup-firmware` SNMP OID: -

Memory Card Mode	Chapter: *4.6 Memory Card Mode* WEB: - Console Set: `# co:nfig me:mory-card-mode {e:nabled|d:isabled|permanent-disabled| a:es-256-enabled|f:w-aes256-enabled}` SNMP OID: -
Name Setup	
Name (0...50 chars)	Chapter: *10.3. Switch Name / Location / Contact / Domain* WEB: Name Setup Console Show: `> sh:ow con:figuration ag:ent [a:ll]` Console Set: `# se:t n:ame [<string max. 50 chars>]` SNMP OID: `MIB-II → sysName`
Location (0...50 chars)	Chapter: *10.3. Switch Name / Location / Contact / Domain* WEB: Name Setup Console Show: `> sh:ow con:figuration ag:ent [a:ll]` Console Set: `# se:t l:ocation [<string max. 50 chars>]` SNMP OID: `MIB-II → sysLocation`
Contact (0...50 chars)	Chapter: *10.3. Switch Name / Location / Contact / Domain* WEB: Name Setup Console Show: `> sh:ow con:figuration ag:ent [a:ll]` Console Set: `# se:t c:ontact [<string max. 50 chars>]` SNMP OID: `MIB-II → sysContact`
Domain (0...50 chars)	Chapter: *10.3. Switch Name / Location / Contact / Domain* WEB: Name Setup Console Show: `> sh:ow con:figuration ag:ent [a:ll]` Console Set: `# se:t d:omain [<string max. 50 chars>]` SNMP OID: -
Layer-2 Functions	
Life Packet Rate	Chapter: *10.45 Layer-2 Discovery Functios* WEB: - Console Show: `> sh:ow con:figuration ag:ent [a:ll]` Console Set: `# co:nfig li:fepacket-rate {1min|10min|1h|10h|d:isabled}` SNMP OID: -
Basic Configurator	Chapter: *10.45.2 Disable Basic Configurator* WEB: - Console Show: `> sh:ow con:figuration ag:ent [a:ll]` Console Set: `# co:nfig b:asic-configurator {e:nable|d:isable}` SNMP OID: -

9.13. Management > Local Accounts

Designation	Access
Admin Account Setup (Read/Write)	
Admin Name	Chapter: *10.5. Admin/User Accounts for Management Access* WEB: Local Accounts → Admin Account Setup Console Show: `# sh:ow con:figuration acco:unts [a:ll]` Console Set: `# se:t admin n:ame <string 1...14 chars>` `# se:t admin n:ame <hash-string>` SNMP OID: -
Admin Password	Chapter: *10.5. Admin/User Accounts for Management Access* WEB: Local Accounts → Admin Account Setup Console Show: `# sh:ow con:figuration acco:unts [a:ll]` Console Set: `# se:t admin p:assword <string 1...14 chars>` `# se:t admin p:assword <hash-string>` SNMP OID: -
Extended Admin Account Setup (Read/Write)	

Admin 1…5 Name	Chapter: *10.5. Admin/User Accounts for Management Access*
	WEB: -
	Console Show: `# sh:ow con:figuration acco:unts [a:ll]`
	Console Set: `# se:t admin-x n:ame <string 1...14 chars>`
	`# se:t admin-x n:ame <hash-string>`
	`Allowed admin-x accounts are {admin-1|admin-2|admin-3|admin-4|admin-5}`
	SNMP OID: -

Admin 1…5 Password	Chapter: *10.5. Admin/User Accounts for Management Access*
	WEB: -
	Console Show: `# sh:ow con:figuration acco:unts [a:ll]`
	Console Set: `# se:t admin-x p:assword <string 1...14 chars>`
	`# se:t admin-x p:assword <hash-string>`
	`Allowed admin-x accounts are {admin-1|admin-2|admin-3|admin-4|admin-5}`
	SNMP OID: -

Admin 1 Access Rights	Chapter: *10.5. Admin/User Accounts for Management Access* WEB: - Console Show: `# sh:ow con:figuration acco:unts [a:ll]` Console Set: `# se:t admin-1 a:ccess-rights {rw-a:ll|rw-w:eb-port-monitor-only}` SNMP OID: -
User Account Setup (Read/Only)	
User Name	Chapter: *10.5. Admin/User Accounts for Management Access* WEB: Local Accounts → User Account Setup Console Show: `# sh:ow con:figuration acco:unts [a:ll]` Console Set: `# se:t u:ser n:ame <string 1...14 chars>` `# se:t u:ser n:ame <hash-string>` SNMP OID: -

User Password	Chapter: *10.5. Admin/User Accounts for Management Access* WEB: Local Accounts → User Account Setup Console Show: `# sh:ow con:figuration acco:unts [a:ll]` Console Set: `# se:t u:ser p:assword <string 1...14 chars>` `# se:t u:ser p:assword <hash-string>` SNMP OID: -
Password Encryption	
Password Encryption Mode	Chapter: *10.6. Password Encryption* WEB: - Console Show: `# sh:ow con:figuration acco:unts [a:ll]` Console Set: `# se:t p:assword-encryption { st:andard|m:d5-hash| sha-:hash|sha2:56-hash|d:es}` SNMP OID: -
Password strength checker	
Password strength checker	Chapter: *10.7 Passwort Strength* WEB: Local Accounts → Password strength checker Console Show: `# sh:ow con:figuration acco:unts [a:ll]` Console Set: `# se:t password-s:trength {e:nabled |d:isable}` SNMP OID: -
Minimum password length	Chapter: *10.7 Passwort Strength* WEB: Local Accounts → Password strength checker Console Show: `# sh:ow con:figuration acco:unts [a:ll]` Console Set: `# se:t password-l:ength {8...14 }` SNMP OID: -

9.14. Management > Access Global

Global Access	
Access policy	Chapter: *10.18 Global Access / Access* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# co:nfig g:lobal-security m:ode {e:nabled| d:isabled}` SNMP OID:
Accesslist Setup	

Accesslist Mode	Chapter: *10.19. Access List / Access List Mode*
	WEB: -
	Console Show: `# sh:ow con:figuration acce:ss [a:ll]`
	Console Set: `# co:nfig ac:cesslist-mode {mode}`
	`Valid values for {mode} are:`
	`{d:isabled|m:anager-only|s:nmp-only|a:ll}`
	SNMP OID: `NEXANS-BM-MIB → adminMgmtAccessList`

Accesslist IPv4	Chapter:	*10.19. Access List / Access List Mode*
	WEB:	-
	Console Show:	`# sh:ow con:figuration acce:ss [a:ll]`

	Console Set:	`# a:ccesslist (1..16) <ip-addr-1> <ip-addr-2> {mode}`
		`Valid values for {mode} are:`
		`{read-w:rite|read-o:nly|n:one}`

	SNMP OID:	-
Accesslist IPv6	Chapter:	*10.19. Access List / Access List Mode*
	WEB:	-
	Console Show:	`# sh:ow con:figuration acce:ss [a:ll]`
	Console Set:	`# ip v6 access-l:ist (1..8) <ipv6-addr-1> <ipv6-addr-2>` `{access-mode} Valid values for {access-mode} are: {read-w:rite|read-o:nly|n:one}`
	SNMP OID:	-
Manager Setup		
Manager authentication mode	Chapter:	*10.10. Manager Authentication Mode*
	WEB:	-
	Console Show:	`# sh:ow con:figuration acce:ss [a:ll]`

	Console Set:	`# co:nfig ma:nager-auth-mode {mode}`
		`Valid values for {mode} are:`
		`{n:one|l:ocal|r:adius|b:oth-radius-local|d:isabled }`

	SNMP OID:	-
Console Setup		
Telnet authentication mode	Chapter:	*10.48. Telnet Console Authentication Mode*
	WEB:	-
	Console Show:	`# sh:ow con:figuration acce:ss [a:ll]`

	Console Set:	`# co:nfig tel:net-auth-mode {mode}`
		`Valid values for {mode} are:`
		`{l:ocal|r:adius|both-r:adius-local|t:acacs+|`
		`both-t:acacs+-local|d:isable-telnet}`

	SNMP OID:	-
SSHv2 authentication mode	Chapter:	*10.49. SSHv2 Console Authentication Mode*
	WEB:	-
	Console Show:	`# sh:ow con:figuration acce:ss [a:ll]`

	Console Set:	`# co:nfig ss:h-auth-mode {mode}`
		`Valid values for {mode} are:`
		`{l:ocal|r:adius|both-r:adius-local|t:acacs+|`
		`both-t:acacs+-local|d:isable-ssh}`

	SNMP OID:	-
SCP authentication mode	Chapter:	*10.50 SCP Authentication Mode*
	WEB:	-
	Console Show:	`# sh:ow con:figuration acce:ss [a:ll]`

	Console Set:	`# co:nfig sc:p-auth-mode {setup}`
		`Sets the SCP authentication mode or disables the SCP interface.`
		`Valid values for {setup} are:`
		`{u:se-ssh-mode|l:ocal|r:adius|both-r:adius-local|`
		`t:acacs+|both-t:acacs+-local|d:isable}`

	SNMP OID:	-

V.24 authentication mode	Chapter: *10.14. V.24 Console Authentication Mode*
	WEB: -
	Console Show: `# sh:ow con:figuration acce:ss [a:ll]`
	Console Set: `# co:nfig v:24-auth-mode {mode}`
	`Valid values for {mode} are:`
	`{l:ocal|r:adius|both-r:adius-local|t:acacs+|`
	`both-t:acacs+-local|d:isable-v24}`
	SNMP OID: -

Console password mode	Chapter: *10.15. Console Password Mode* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# co:nfig co:nsole-password-mode {i:nvisible|v:isible}` SNMP OID: -
Encrypt passwords in CLI	Chapter: *10.16 Encrypt Password* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `co:nfig console-e:ncryption {d:isabled|e:nabled}` SNMP OID: -
Console logout time (seconds)	Chapter: *10.17 Console logout time* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `co:nfig console-l:ogout-timeout (5...65535)` SNMP OID: -
WEB Setup	

Refresh Rate for State pages	Chapter: -
	WEB: Switch Setup
	Console Show: `# sh:ow con:figuration acce:ss [a:ll]`
	Console Set: `# co:nfig web-r:efresh-rate {setup}`
	`Valid values for {setup} are:`
	`{d:isabled|5:sec|10:sec|30:sec}`
	SNMP OID: -

HTTP authentication mode	Chapter: *10.11.1. HTTP Authentication Mode* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# co:nfig web-a:uth-mode {l:ocal|r:ead-only|d:isable-web}` SNMP OID: -
HTTP TCP port	Chapter: *10.11.2. HTTP TCP Port* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# co:nfig web-t:cp-port (1...65535)` SNMP OID: -

HTTPS authentication mode	Chapter: *10.12.1. HTTPS Authentication Mode*
	WEB: -
	Console Show: `# sh:ow con:figuration acce:ss [a:ll]`
	Console Set: `# co:nfig web-h:ttps-auth-mode {setup}`
	`Valid values for {setup} are:`
	`{l:ocal|re:ad-only|d:isable-https}`
	SNMP OID: -

HTTPS TCP port	Chapter: *10.12.2. HTTPS TCP Port* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# co:nfig https-t:cp-port (1...65535)` SNMP OID: -
HTTPS Allowed TLS Versions	Chapter: *10.12.3. HTTPS Allowed TLS Versions* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# co:nfig tls {a:ll|1.1|1.2}` SNMP OID: -
TFTP Setup	

TFTP authentication via SNMP	Chapter: *7.5 TFTP Authentication using SNMP*
	WEB: -
	Console Show: `# sh:ow con:figuration acce:ss [a:ll]`
	Console Set: `# co:nfig tf:tp-auth-via-snmp {setup}`
	`Valid values for {setup} are:`
	`{d:isabled|read-write|read-only}`
	SNMP OID: -

DIP Switches Setup	
Fixed IP	Chapter: *3.5. Disabling Configuration Switches* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# co:nfig dip-fi:xes-ip-mode {e:nabled|d:isabled}` SNMP OID: -
Factory Reset	Chapter: *3.5. Disabling Configuration Switches* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# co:nfig dip-fa:ctory-reset-mode {e:nabled|d:isabled}` SNMP OID: -

9.15. Management > Access SNMP

Designation	Access
SNMP Global Setup	

SNMP protocol version	Chapter: *10.53.1. SNMP Protocol Version*
	WEB: -
	Console Show: `# sh:ow con:figuration acce:ss [a:ll]`
	Console Set: `# co:nfig snmp-p:rotocol-version {setup}`
	`Valid values for {setup} are:`
	`{v1-o:nly|v2-o:nly|v1-a:nd-v2|v3-auth-m:d5|`
	`v3-priv-auth-m:d5|v3-aes-auth-m:d5|v3-auth-s:ha|`
	`v3-priv-auth-s:ha|v3-aes-auth-s:ha|`
	`v3-n:o-priv-with-v1-v2-read-only|`
	`v3-w:ith-v1-v2-read-only}`
	SNMP OID: -

SNMP access mode	Chapter: *10.53.2. SNMP Access Mode*
	WEB: -
	Console Show: `# sh:ow con:figuration acce:ss [a:ll]`
	Console Set: `# co:nfig snmp-a:ccess-mode {mode}`
	`Valid values for {mode} are:`
	`{read-w:rite|read-o:nly|d:isable-snmp}`
	SNMP OID: -

SNMPv1/v2 Setup	
Read/Only community (0…15 chars)	Chapter: *10.53.3. SNMPv1/v2c Communities* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# snm:p c:ommunity r:ead-trap <string 1...15 chars>` SNMP OID: -
Read/Write Community (0…15 chars)	Chapter: *10.53.3. SNMPv1/v2c Communities* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# snm:p c:ommunity w:rite-read <string 1...15 chars>` SNMP OID: -
Trap Community (0…15 chars)	Chapter: *10.53.3. SNMPv1/v2c Communities* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# snm:p c:ommunity t:rap <string 1...15 chars>` SNMP OID: -

SNMPv1 MAC table mode	Chapter: *10.53.4. SNMPv1 MAC Table Mode*
	WEB: -
	Console Show: `# sh:ow con:figuration acce:ss [a:ll]`
	Console Set: `# co:nfig snmp-m:ac-table-mode {mode}`
	`Valid values for {mode} are:`
	`{a:ll-ports|u:ser-ports-only}`
	SNMP OID: `NEXANS-BM-MIB → adminSnmpMacTableMode`

SNMPv3 Global Setup	
Engine ID (max 64 chars / 32 bytes, leavy empty to use default MAC based Engine ID)	Chapter: *10.53.5. SNMPv3 Engine ID* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# snm:p v:3 e:ngine-id` `[<string max. 64 chars (32 bytes)>]` SNMP OID: -
SNMPv3 Read/Write Account Setup	
Read/Write username (max 32 chars)	Chapter: *10.53.6. SNMPv3 User Setup* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# snm:p v:3 u:sername w:rite-read` `[<string max. 32 chars>]` SNMP OID: -

Read/Write password (8…32 chars)	Chapter: *10.53.6. SNMPv3 User Setup* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# snm:p v:3 p:assword w:rite-read [<string max. 32 chars>]` SNMP OID: -
Privacy password (8…32 chars)	Chapter: *10.53.6. SNMPv3 User Setup* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# snm:p v:3 pr:ivacy-password w:rite-read [<string max. 32 chars>]` SNMP OID: -
SNMPv3 Read/Only Account Setup	
Read/Only username (max 32 chars)	Chapter: *10.53.6. SNMPv3 User Setup* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# snm:p v:3 u:sername r:ead [<string max. 32 chars>]` SNMP OID: -
Read/Only password (8…32 chars)	Chapter: *10.53.6. SNMPv3 User Setup* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# snm:p v:3 p:assword r:ead [<string max. 32 chars>]` SNMP OID: -
Privacy password (8…32 chars)	Chapter: *10.53.6. SNMPv3 User Setup* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# snm:p v:3 pr:ivacy-password r:ead [<string max. 32 chars>]` SNMP OID: -
SNMPv3 Flexible Account Setup	
Flexible access mode (max 32 chars)	Chapter: *SNMPv3 User Setup* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# snm:p v:3 f:lexible-access {r:ead|w:rite-read} [<string max. 32 chars>]` SNMP OID: -
Username (max 32 chars)	Chapter: *SNMPv3 User Setup* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# snm:p v:3 u:sername f:lexible [<string max. 32 chars>]` SNMP OID: -

Authentication password (8…32 chars)	Chapter: *SNMPv3 User Setup* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# snm:p v:3 p:assword f:lexible [<string 8...32 chars>]` SNMP OID: -
Privacy password (8…32 chars)	Chapter: *10.53.6. SNMPv3 User Setup* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# snm:p v:3 pr:ivacy-password f:lexible [<string max. 32 chars>]` SNMP OID: -
SNMPv3 Trap Account Setup	
Username (max 32 chars)	Chapter: *10.53.6. SNMPv3 User Setup* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# snm:p v:3 u:sername t:rap [<string max. 32 chars>]` SNMP OID: -
Authentication password (8…32 chars)	Chapter: *10.53.6. SNMPv3 User Setup* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# snm:p v:3 pa:ssword t:rap [<string max. 32 chars>]` SNMP OID: -
Privacy password (8…32 chars)	Chapter: *10.53.6. SNMPv3 User Setup* WEB: - Console Show: `# sh:ow con:figuration acce:ss [a:ll]` Console Set: `# snm:p v:3 pr:ivacy-password t:rap [<string max. 32 chars>]` SNMP OID: -

9.16. Management > Access IEC 61850

Designation	Access
IEC 61850 Global Setup	
IEC 61850 access mode	Chapter: *10.79 IEC61850 protocol support* WEB: - Console Show: `> sh:ow con:figuration ie:c61850 [a:ll]` Console Set: `# ie:c61850 a:ccess-mode {d:isable|read-w:rite|read-o:nly}` SNMP OID: -

9.17. Management > Banner

Designation	Access
Banner Setup	
Banner	Chapter: *10.4 Banner* WEB: - Console Show: `> sh:ow con:figuration ba:nner` Console Set: `# se:t ba:nner t:ext (1...12) <string 0...80 chars>` SNMP OID: -

9.18. Management > Zero Touch Configuration

Designation	Access
Zero Touch Configuration Setup	
Zero Touch Configuration Mode	Chapter: *7.3 Zero Touch Configuration* WEB: - Console Show: `> sh:ow con:figuration ip [a:ll]` Console Set: `# zero-:touch-config m:ode {d:isabled|e:nabled}` SNMP OID: -
Controller IP	Chapter: *7.3 Zero Touch Configuration* WEB: - Console Show: `> sh:ow con:figuration ip [a:ll]` Console Set: `# zero-:touch-config c:ontroller-ip <ip-addr>` SNMP OID: -
Zero Touch Configuration State	Chapter: *7.3 Zero Touch Configuration* WEB: - Console Show: `# sh:ow zero-:touch-config` Console Set: - SNMP OID: -

9.19. Management > Scripting

Designation	Access
Scripting Setup	
Script File Content	Chapter: *7.4 Scripting* WEB: - Console Show: `> sh:ow cli-script [{n:o-pause|d:elete}]` Console Set: `# cli-script interface {if-no range} {link-u:p|link-d:own|link-change} assign <CLI Script name>` `# cli-script interface {if-no range} {link-u:p|link-d:own|link-change} delete` SNMP OID: -

9.20. Global

Designation	Access
LED Setup	
Global LED Mode	Chapter: *10.33 Global LED Mode* WEB: - Console Show: `> sh:ow con:figuration g:lobal [a:ll]` Console Set: `# co:nfig le:d-global-mode {s:tandard|on|off-a:ll|off-e:xcept-mgmt|r:ed-blue-blinking|g:reen-blinking}` SNMP OID: `NEXANS-BM-MIB → adminLedGlobalMode`
Portmirror / Portmonitor Setup	
VLAN Portmirror	Chapter: *10.32. VLAN Portmirror* WEB: - Console Show: `> sh:ow con:figuration g:lobal [a:ll]` Console Set: `# co:nfig mi:rror {e:nable|d:isable}` SNMP OID: `NEXANS-BM-MIB → adminSwitchPortMirror`
Portmonitor → Mode	Chapter: *10.34. Portmonitor* WEB: Port Monitor Console Show: `> sh:ow con:figuration g:lobal [a:ll]` Console Set: `# co:nfig mo:nitor m:ode {d:isabled|r:x-only|t:x-only|b:oth}` SNMP OID: -
Portmonitor → Source-Port	Chapter: *10.34. Portmonitor* WEB: Port Monitor Console Show: `> sh:ow con:figuration g:lobal [a:ll]` Console Set: `# co:nfig mo:nitor s:ource <if-no>` SNMP OID: -
Portmonitor → Destination-Port	Chapter: *10.34. Portmonitor* WEB: Port Monitor Console Show: `> sh:ow con:figuration g:lobal [a:ll]` Console Set: `# co:nfig mo:nitor d:estination <if-no>` SNMP OID: -
Switch Engine Setup	
Address Ageing (1...68 Minuten)	Chapter: *10.39. Address Ageing Time* of the Forwarding Table WEB: - Console Show: `> sh:ow con:figuration g:lobal [a:ll]` Console Set: `# co:nfig ag:eing-time (1..68)` SNMP OID: `NEXANS-BM-MIB → adminAddrAgingTimeMinutes`
Flow Control enable	Chapter: *10.44. Flow Control* WEB: - Console Show: `> sh:ow con:figuration g:lobal [a:ll]` Console Set: `# co:nfig f:low-control d:isable|a:uto` SNMP OID: -

9.21. VLAN > VLAN-Table

Designation	Access
VLAN Table Global Setup	
VLAN Table Mode	Chapter: *10.31.2. VLAN Mode* WEB: Switch Setup Console Show: `> sh:ow con:figuration v:lan [a:ll]` Console Set: `# v:lan-table m:ode {mode}` `Valid values for {mode} are: {s:tatic|e:nhanced-static|2:56-static|d:ynamic| p:ort-based}` SNMP OID: `NEXANS-BM-MIB → adminSwitchVlanTableMode`
Tagging Ethertype	Chapter: *10.31.6. Tagging Ethertype (Q-in-Q)* WEB: - Console Show: `> sh:ow con:figuration g:lobal [a:ll]` Console Set: `# co:nfig ta:gging-ethertype {mode}` `Valid values for {mode} are: {81:00-default|91:00|92:00}` SNMP OID: -
Fabric Attach Authentication Key	Chapter: *10.31.3 Fabric Attach* WEB: - Console Show: `> sh:ow con:figuration v:lan [a:ll]` Console Set: `# v:lan-table f:a-auth-key [<string 1...32 chars>]` SNMP OID: -
VLAN Table	
VLAN-ID (1...4095)	Chapter: *10.31.1. VLAN Table* WEB: VLAN Table Console Show: `> sh:ow con:figuration v:lan [a:ll]` Console Set: `# v:lan-table a:dd (1...4095) [string max. 50 chars]` `# v:lan-table d:elete (1...4095)` SNMP OID: `NEXANS-BM-MIB → vlanId`
VLAN Name (0...50 chars)	Chapter: *10.31.1. VLAN Table* WEB: VLAN Table Console Show: `> sh:ow con:figuration v:lan [a:ll]` Console Set: `# v:lan-table a:dd (1...4095) [string max. 50 chars]` SNMP OID: `NEXANS-BM-MIB → vlanDescr`
MGMT	Chapter: *10.31.10 Port VLAN Tagging* WEB: VLAN Table Console Show: `> sh:ow con:figuration v:lan [a:ll]` Console Set: - SNMP OID: `Q-BRIDGE-MIB → dot1qVlanStaticEgressPorts` `Q-BRIDGE-MIB → dot1qVlanStaticUntaggedPorts`

1…*n* (*n* = number of ports)	Chapter:	*10.31.10 Port VLAN Tagging*
	WEB:	VLAN Table
	Console Show:	`> sh:ow con:figuration v:lan [a:ll]`
	Console Set:	`# in:terface {if-no range} vl:an-id {vlan-id range} {t:ag|u:ntag|r:emove}`
	SNMP OID:	`Q-BRIDGE-MIB → dot1qVlanStaticEgressPorts` `Q-BRIDGE-MIB → dot1qVlanStaticUntaggedPorts`
IEEE802.1p VLAN based priority override value	Chapter:	*10.38.3. IEEE802.1p VLAN based Priority Override*
	WEB:	VLAN Table
	Console Show:	`> sh:ow con:figuration v:lan [a:ll]`
	Console Set:	`# v:lan-table p:rio-override (1...4095) {disable|0..7)}`
	SNMP OID:	`NEXANS-BM-MIB → vlanPrioOverride`
Fabric Attach SPBM I-SID	Chapter:	*10.31.3 Fabric Attach*
	WEB:	VLAN Table
	Console Show:	`> sh:ow con:figuration v:lan [a:ll]`
	Console Set:	`# v:lan-table i:-sid {vlan-id} (0|1...16777215)`
	SNMP OID:	-

9.22. VLAN > VLAN Setup

Designation	Access	
VLAN Port Setup		
Default VLAN-ID (1…4095, 0 disables VLAN)	Chapter:	*10.31.8. Port Default VLAN-ID*
	WEB:	Port State
	Console Show:	`> sh:ow con:figuration v:lan [a:ll]`
	Console Set:	`# in:terface {if-no range} vl:an-id (0|1...4095)`
	SNMP OID:	`NEXANS-BM-MIB → portDefaultVlanId`
Voice-VLAN-ID (1…4095, 0 disables VLAN)	Chapter:	*10.31.9. Port Voice VLAN-ID*
	WEB:	Port State
	Console Show:	`> sh:ow con:figuration v:lan [a:ll]`
	Console Set:	`# in:terface {if-no range} vo:ice-vlan-id (0|1...4095)`
	SNMP OID:	`NEXANS-BM-MIB → portVoiceVlanId`
Trunking Mode	Chapter:	*10.31.7. Port Trunking Mode*
	WEB:	Port State
	Console Show:	`> sh:ow con:figuration v:lan [a:ll]`

	Console Set:	`# in:terface {if-no range} t:runking-mode {mode}`
		`Valid values for {mode} are:`
		`{di:sable|do:t1q|n:otag|h:ybrid}`

	SNMP OID:	`NEXANS-BM-MIB → portTrunkingMode`
Port Isolation	Chapter:	*10.31.5 Per-Port VLAN Port Isolation*
	WEB:	-
	Console Show:	`> sh:ow con:figuration v:lan [a:ll]`
	Console Set:	`# in:terface {if-no range} po:rt-vlan-isolation {e:nable|d:isable}`
	SNMP OID:	-

VLAN Port Global Setup		
VLAN Port Isolation	Chapter:	*10.31.4. Global VLAN Port Isolation*
	WEB:	-
	Console Show:	`> sh:ow con:figuration v:lan [a:ll]`
	Console Set:	`# v:lan-table p:ort-isolation {d:isable|u:ser-ports|s:elected-ports}`
	SNMP OID:	-
VLAN Security Setup		
RADIUS Unsecure VLAN-ID (1…4095)	Chapter:	*10.31.15. RADIUS Unsecure VLAN-ID*
	WEB:	VLAN Table
	Console Show:	`> sh:ow con:figuration v:lan [a:ll]`
	Console Set:	`# rad:ius u:nsecure-vlan (1...4095)`
	SNMP OID:	`NEXANS-BM-MIB → adminUnsecureVlanId`
RADIUS Guest VLAN-ID (0…4095)	Chapter:	*10.31.16. RADIUS Guest VLAN-ID*
	WEB:	VLAN Table
	Console Show:	`> sh:ow con:figuration v:lan [a:ll]`
	Console Set:	`# rad:ius g:uest-vlan (0...4095)`
	SNMP OID:	-
RADIUS Inaccessible VLAN-ID (1…4095)	Chapter:	*10.31.17. RADIUS Inaccessible VLAN-ID*
	WEB:	VLAN Table
	Console Show:	`> sh:ow con:figuration v:lan [a:ll]`
	Console Set:	`# rad:ius i:naccessible-vlan (0...4095)`
	SNMP OID:	-
IEEE802.1X Authentication Failure VLAN-ID (0…4095)	Chapter:	*10.31.18. IEEE802.1X Authentication Failure VLAN-ID*
	WEB:	VLAN Table
	Console Show:	`> sh:ow con:figuration v:lan [a:ll]`
	Console Set:	`# do:t1x a:uthentication f:ailure-vlan-id (0...4095)`
	SNMP OID:	-

9.23. Discovery

Designation	**Access**	
Link-Layer-Discovery-Protocol Setup (IEEE802.1AB)		
LLDP Mode	Chapter:	*10.70. Link Layer Discovery Protocol (LLDP)*
	WEB:	-
	Console Show:	`> sh:ow con:figuration di:scovery [a:ll]`

	Console Set:	`# co:nfig lldp-mo:de {setup}`
		`Valid values for {setup} are:`
		`{d:isabled|fi:lter-disabled|e:nabled|fo:rward-enabled}`

	SNMP OID:	-

TX Message Interval (seconds)	Chapter: *10.70. Link Layer Discovery Protocol (LLDP)* WEB: - Console Show: `> sh:ow con:figuration di:scovery [a:ll]` Console Set: `# co:nfig lldp-i:nterval (5..32678)` SNMP OID: -
TX Holdtime Multiplier	Chapter: *10.70. Link Layer Discovery Protocol (LLDP)* WEB: - Console Show: `> sh:ow con:figuration di:scovery [a:ll]` Console Set: `# co:nfig lldp-mu:ltiplier (2..10)` SNMP OID: -
LLDP MED - Network Policy Voice (TIA-1057)	
Layer 2 Voice priority value	Chapter: *10.71. LLDP for Media Endpoint Devices (LLDP-MED)* WEB: - Console Show: `> sh:ow con:figuration di:scovery [a:ll]` Console Set: `# co:nfig lldp-me:d layer2-p:riority (0..7)` SNMP OID: -
Layer 3 Voice DSCP value	Chapter: *10.71. LLDP for Media Endpoint Devices (LLDP-MED)* WEB: - Console Show: `> sh:ow con:figuration di:scovery [a:ll]` Console Set: `# co:nfig lldp-me:d dscp-p:riority (0..63)` SNMP OID: -
LLDP MED - Network Policy Voice Signaling (TIA-1057)	
Layer 2 Voice Signaling priority value	Chapter: *10.71. LLDP for Media Endpoint Devices (LLDP-MED)* WEB: - Console Show: `> sh:ow con:figuration di:scovery [a:ll]` Console Set: `# co:nfig lldp-me:d layer2-s:ig-priority (0..7)` SNMP OID: -
Layer 3 Voice Signaling DSCP value	Chapter: *10.71. LLDP for Media Endpoint Devices (LLDP-MED)* WEB: - Console Show: `> sh:ow con:figuration di:scovery [a:ll]` Console Set: `# co:nfig lldp-me:d dscp-s:ig-priority (0..63)` SNMP OID: -
LLDP MED – Location Indentification – Civic Address LCI (TIA-1057)	
Building (25)	Chapter: *10.71. LLDP for Media Endpoint Devices (LLDP-MED)* WEB: - Console Show: `> sh:ow con:figuration di:scovery [a:ll]` Console Set: `# co:nfig lldp-me:d lo:cation-id b:uilding [<string 1...50 chars>]` SNMP OID: -
Unit (26)	Chapter: *10.71. LLDP for Media Endpoint Devices (LLDP-MED)* WEB: - Console Show: `> sh:ow con:figuration di:scovery [a:ll]` Console Set: `# co:nfig lldp-me:d lo:cation-id u:nit [<string 1...50 chars>]` SNMP OID: -

Place Type (29)	Chapter: *10.71. LLDP for Media Endpoint Devices (LLDP-MED)* WEB: - Console Show: `> sh:ow con:figuration di:scovery [a:ll]` Console Set: `# co:nfig lldp-me:d lo:cation-id p:lace-type [<string 1...50 chars>]` SNMP OID: -
Cisco-Discovery-Protocol Setup (IEEE802.1AB)	
CDP Mode	Chapter: *10.72. Cisco Discovery Protocol (CDP)* WEB: - Console Show: `> sh:ow con:figuration di:scovery [a:ll]` Console Set: `# co:nfig cdp-m:ode {d:isabled|e:nabled|f:orward-enabled}` SNMP OID: -
TX Message Interval (seconds)	Chapter: *10.72. Cisco Discovery Protocol (CDP)* WEB: - Console Show: `> sh:ow con:figuration di:scovery [a:ll]` Console Set: `# co:nfig cdp-i:nterval (5..255)` SNMP OID: -
TX Holdtime (seconds)	Chapter: *10.72. Cisco Discovery Protocol (CDP)* WEB: - Console Show: `> sh:ow con:figuration di:scovery [a:ll]` Console Set: `# co:nfig cdp-h:oldtime (10..255)` SNMP OID: -

9.24. Prioritisation

Designation	Access
Prioritisation Global Setup	

Priority Scheme	Chapter: *10.38.1 Prioritization Scheme*
	WEB: -
	Console Show: `> sh:ow con:figuration p:riorisation [a:ll]`
	Console Set: `# co:nfig priority-s:cheme {setup}`
	`Valid values for {setup} are:`
	`s:trict`
	`w:eighted-fair`
	`mixed-strict-q3`
	`mixed-strict-q2:-and-q3`
	SNMP OID: -

Priority Setup IEEE802.1p	
Priority Setup: 802.1p	Chapter: *10.38.2. Prioritization according to IEEE802.1p* WEB: 802.1q Priority Console Show: `> sh:ow con:figuration p:riorisation [a:ll]` Console Set: `# co:nfig priority-d:ot1p (priority value=0..7) (queue=0..3)` SNMP OID: -

Priority Setup IPv4/IPv6		

Priority Setup:
IPv4-DSCP-Diffserv
IPv4-TOS
IPv6-Traffic-Class
	Chapter:
	WEB:
	Console Show:
	Console Set:
	SNMP OID:
		10.38.4. Prioritization according to IPv4/IPv6
		IPv4/Ipv6 Priority
		`> sh:ow con:figuration p:riorisation [a:ll]`
		`# co:nfig priority-i:p (priority value=0..63) (queue=0..3)`
		-

9.25. Alarms > Alarm Destinations

Designation	**Access**
Alarm Destination Table	
Test Traps/Syslog	Chapter: *10.54. Alarm Destination Table* WEB: - Console Set: `# te:st-traps-syslog` SNMP OID: -

Syslog Severity	Chapter: *10.54. Alarm Destination Table*
	WEB: -
	Console Show: `# sh:ow con:figuration al:arms [a:ll]`
	Console Set:
	`# tr:ap-syslog s:everity {event-type} {severity-type}`
	`Valid values for {severity-type} are:`
	`0:-emergency`
	`1:-alert`
	`2:-critical`
	`3:-error`
	`4:-warning`
	`5:-notice`
	`6:-info`
	`7:-debug`
	SNMP OID: -

Local Logging Mode	Chapter: *10.54. Alarm Destination Table* WEB: - Console Show: `# sh:ow con:figuration al:arms [a:ll]` Console Set: `# tr:ap-syslog l:ocal-log m:ode {o:verwrite|s:top|d:isable}` SNMP OID: -
Syslog Facility	Chapter: *10.54. Alarm Destination Table* WEB: - Console Show: `# sh:ow con:figuration al:arms [a:ll]` Console Set: `# tr:ap-syslog f:acility (1...31)` SNMP OID: -

Destination Type	Chapter: *10.54. Alarm Destination Table*
	Console Show: `# sh:ow con:figuration al:arms [a:ll]`
	Console Set:
	`# tr:ap-syslog t:ype (1...8) {destination-type}`
	`Valid values for {destination-type} are:`
	`snmp-trap-v1`
	`snmp-trap-v2`
	`snmp-trap-v3`
	`remote-sy:slog`
	`remote-sw:itch-alarm`
	`l:ocal-syslog`
	SNMP OID: -

IPv4/IPv6 Address	Chapter: *10.54. Alarm Destination Table* Console Show: `# sh:ow con:figuration al:arms [a:ll]` Console Set: `# tr:ap-syslog d:estination (1...8) {i:p-addr|d:isable} [<ip>]` SNMP OID: -

Event Type	Chapter: *10.54. Alarm Destination Table*
	Console Show: `# sh:ow con:figuration al:arms [a:ll]`
	Console Set:
	`# tr:ap-syslog e:vent (1...8) {event-type} {e:nable|d:isable}`
	`Valid values for {event-type} are:`
	`a:ll`
	`c:old-start`
	`link-u:p`
	`link-d:own`
	`link-c:hange`
	`new-m:ac-address`
	`te:mperatur-fail`
	`e:rror-counter-fail`
	`b:roadcast-fail`
	`poe-v:oltage-fail`
	`poe-s:witch-overload`
	`poe-p:ort-overload`
	`m:gmt-auth-fail`
	`por:t-secu-fail`
	`a:ctive-loop-detect`
	`radius-m:gmt-auth-reject`
	`radius-p:ort-secu-reject`
	`alarm1`
	`alarm2`
	`new-r:oot`
	`to:pology-change`
	`i:nternal-voltage-fail`
	`tf:tp-message`
	`s:fp-event`
	`cl:ient-remove-alarm`
	`internal-m:gmt-warning`
	`f:unction-input-alarm`
	`con:figuration-changed`
	`port-e:rror-disabled`
	SNMP OID: -

9.26. Alarms > Global Alarms

Temperature Alarm Setup	
Low Alarm Limit (°C)	Chapter: *10.29. Switch Temperature* WEB: - Console Show: `# sh:ow con:figuration al:arms [a:ll]` Console Set: `# co:nfig temp-l:ow-alarm (-40..20)` SNMP OID: -
High Alarm Limit (°C)	Chapter: *10.29. Switch Temperature* WEB: - Console Show: `# sh:ow con:figuration al:arms [a:ll]` Console Set: `# co:nfig temp-h:igh-alarm (30..100)` SNMP OID: -

Overtemperature Powersave Action	Chapter: *10.29.2. Temperature Powersave Function* WEB: - Console Show: `# sh:ow con:figuration al:arms [a:ll]` Console Set: `# co:nfig o:vertemp-action {d:isable|s:peed-eco}` SNMP OID: -
PoE Input Alarm Setup	

PoE Power Source	Chapter: *11.1.6 PoE Power Source*
	WEB: PoE → Power Supply
	Console Show: `# sh:ow con:figuration al:arms [a:ll]`
	Console Set: `# co:nfig poe-po:wer-source {setup}`
	`Valid values for {setup} are:`
	`{af:-uplink|2:x-class2-af-uplink|at:-uplink|`
	`1:x-class4-at-uplink|e:xternal}`
	SNMP OID: -

PoE Input Powerlimit (W)	Chapter: *11.1.4. PoE Input Power Limit* WEB: PoE → Power Supply Console Show: `# sh:ow con:figuration al:arms [a:ll]` Console Set: `# co:nfig poe-li:mit (1..100)` SNMP OID: `NEXANS-BM-MIB → adminSwitchPoEPowerLimit`
PoE Input Voltage Low Alarm Limit (V)	Chapter: *11.1.5. PoE Input Voltage Alarm Limits* WEB: PoE → Power Supply Console Show: `> sh:ow con:figuration g:lobal [a:ll]` Console Set: `# co:nfig poe-lo:w-alarm-voltage (0..48)` SNMP OID: -
PoE Input Voltage Upper Alarm Limit (V)	Chapter: *11.1.5. PoE Input Voltage Alarm Limits* WEB: PoE → Power Supply Console Show: `> sh:ow con:figuration g:lobal [a:ll]` Console Set: `# co:nfig poe-up:per-alarm-voltage (49..57)` SNMP OID: -

9.27. Alarms > Alarm Inputs

Function Input Setup	
Function Input 1..4 Name	Chapter: *10.46.1 Function Input Alarm Mode* WEB: - Console Show: # Console Set: `# co:nfig io-input-n:ame {1..4} [<string max 32 chars>]` SNMP OID: -

Function Input 1..4 Remote Alarm Mode	Chapter: *10.46.1 Function Input Alarm Mode*
	WEB: -
	Console Show: `# sh:ow con:figuration al:arms [a:ll]`
	Console Set: `# co:nfig io-input-r:emote-alarm {1..4} m:ode {setup}`
	`Valid values for {setup} are:`
	`{d:isabled|shorted-o:nly|shorted-c:lear|`
	`open-o:nly|open-c:lear|`
	`clear-o:pened-ouput-alarms|`
	`clear-s:horted-ouput-alarms}`
	SNMP OID: -

Function Input 1..4 Remote Alarm Group	Chapter: *10.46.1 Function Input Alarm Mode* WEB: - Console Show: `# sh:ow con:figuration al:arms [a:ll]` Console Set: `# co:nfig io-input-r:emote-alarm {1..4} g:roup (0..255)` SNMP OID: -

9.28. Alarms > Alarm Inputs for 160X

Function Input Setup	
Input Name	Chapter: *10.46.1 Function Input Alarm Mode* WEB: - Console Show: `#` Console Set: `# co:nfig io-input-n:ame {1..4} [<string max 32 chars>]` `Sets name for io input.` SNMP OID: -

Remote Alarm Mode	Chapter: *10.46.1 Function Input Alarm Mode*
	WEB: -
	Console Show: `# sh:ow con:figuration al:arms [a:ll]`
	Console Set: `# co:nfig io-input-r:emote-alarm {1..4} m:ode {setup}`
	`Sets mode for io input remote alarms.`
	`Valid values for {setup} are:`
	`{d:isabled|shorted-o:nly|shorted-c:lear|`
	`open-o:nly|open-c:lear}`
	SNMP OID: -

Remote Alarm Group	Chapter: *10.46.1 Function Input Alarm Mode*
	WEB: -
	Console Show: `# sh:ow con:figuration al:arms [a:ll]`
	Console Set: `# co:nfig io-input-r:emote-alarm`
	`{1..4} g:roup (0...255)`
	`Sets destination group for io input remote alarms.`
	SNMP OID: -

9.29. Alarms > Alarm Outputs

Industrial Alarm Output Setup	
Alarm Output M1 Name	Chapter: *10.47. Alarm Outputs for Industrial Switches* WEB: Alarm Setup Console Show: `# sh:ow con:figuration al:arms [a:ll]` Console Set: `# co:nfig alarm1 name [<string max 32 chars>]` SNMP OID: -

Alarm Output M1 Mode	Chapter: *10.47. Alarm Outputs for Industrial Switches*
	WEB: Alarm Setup
	Console Show: `# sh:ow con:figuration al:arms [a:ll]`
	Console Set:
	`# co:nfig alarm1 {mode}`
	`Valid values for {mode} are:`
	`{li:nk-down|on:-forced|of:f-forced|s1-:power|`
	`s2-:power|s1s2:-power|op:en-func-input|`
	`sh:orted-func-input|remote-f:unc-input|`
	`remote-a:larm-table|lo:cal-alarm-table}`
	SNMP OID: -

Remote Alarm Group M1	Chapter: *10.47. Alarm Outputs for Industrial Switches* WEB: - Console Show: `# sh:ow con:figuration al:arms [a:ll]` Console Set: `# co:nfig alarm1 remote-g:roup (0...255)` SNMP OID: -
Alarm Output M2 Name	Chapter: *10.47. Alarm Outputs for Industrial Switches* WEB: Alarm Setup Console Show: `# sh:ow con:figuration al:arms [a:ll]` Console Set: `# co:nfig alarm2 name [<string max 32 chars>]` SNMP OID: -

Alarm Output M2 Mode	Chapter: *10.47. Alarm Outputs for Industrial Switches*
	WEB: Alarm Setup
	Console Show: `# sh:ow con:figuration al:arms [a:ll]`
	Console Set:
	`# co:nfig alarm2 {mode}`
	`Valid values for {mode} are:`
	`{li:nk-down|on:-forced|of:f-forced|s1-:power|`
	`s2-:power|s1s2:-power|op:en-func-input|`
	`sh:orted-func-input|remote-f:unc-input|`
	`remote-a:larm-table|lo:cal-alarm-table}`
	SNMP OID: -

Remote Alarm Group M2	Chapter: *10.47. Alarm Outputs for Industrial Switches* WEB: - Console Show: `# sh:ow con:figuration al:arms [a:ll]` Console Set: `# co:nfig alarm2 remote-g:roup (0...255)` SNMP OID: -

Industrial Link Down Alarms		
Link Down Alarm M1	Chapter:	*10.47. Alarm Outputs for Industrial Switches*
	WEB:	Industrial Alarm
	Console Show:	`# sh:ow con:figuration al:arms [a:ll]`
	Console Set:	`# in:terface {if-no range} alarm1 {e:nable|d:isable}`
	SNMP OID:	-
Link Down Alarm M2	Chapter:	*10.47. Alarm Outputs for Industrial Switches*
	WEB:	Industrial Alarm
	Console Show:	`# sh:ow con:figuration al:arms [a:ll]`
	Console Set:	`# in:terface {if-no range} alarm2 {e:nable|d:isable}`
	SNMP OID:	-

9.30. Alarms > SFP Alarms

SFP Alarms Limits Setup		
Laser Bias Current (mA) Upper Limit	Chapter:	*10.25. SFP Info, Diagnostic and Alarms*
	WEB:	-
	Console Show:	`# sh:ow con:figuration al:arms [a:ll]`
	Console Set:	`# in:terface {if-no range} sfp-b:ias-current-limit (0..1000)`
	SNMP OID:	`NEXANS-BM-MIB → sfpAlarmTxBiasCurrentUpperLimit`
TX Output Power (uW) Lower Limit	Chapter:	*10.25. SFP Info, Diagnostic and Alarms*
	WEB:	-
	Console Show:	`# sh:ow con:figuration al:arms [a:ll]`
	Console Set:	`# in:terface {if-no range} sfp-t:x-power-limit (0..1000)`
	SNMP OID:	`NEXANS-BM-MIB → sfpAlarmTxOutputPowerLowerLimit`
RX Input Power (uW) Lower Limit	Chapter:	*10.25. SFP Info, Diagnostic and Alarms*
	WEB:	-
	Console Show:	`# sh:ow con:figuration al:arms [a:ll]`
	Console Set:	`# in:terface {if-no range} sfp-r:x-power-limit (0..1000)`
	SNMP OID:	`NEXANS-BM-MIB → sfpAlarmRxInputPowerLowerLimit`

9.31. Security > Security Setup

Portsecurity Global Setup	

Portsecurity Failure Action	Chapter: *10.36.1. Portsecurity Failure Action*
	WEB: -
	Console Show: `> sh:ow con:figuration g:lobal [a:ll]`
	Console Set: `# co:nfig se:curity-action {mode}`
	`Valid values for {mode} are:`
	`{d:isable-port|t:rap-syslog-only|i:mmediately-disable}`
	SNMP OID: -

Re-enable time for Security-Disabled ports	Chapter: *10.36.1. Portsecurity Failure Action* WEB: - Console Show: `> sh:ow con:figuration g:lobal [a:ll]` Console Set: `# co:nfig r:e-enable s:ecurity-disable (0...60000)` SNMP OID: -
Re-enable time for Loop-Disabled ports	Chapter: *10.36.1. Portsecurity Failure Action* WEB: - Console Show: `> sh:ow con:figuration g:lobal [a:ll]` Console Set: `# co:nfig r:e-enable l:oop-disable (0...60000)` SNMP OID: -
Voice VLAN Authentication Mode	Chapter: *10.36.2. Portsecurity - Voice VLAN Authentication Mode* WEB: - Console Show: `> sh:ow con:figuration g:lobal [a:ll]` Console Set: `# co:nfig vo:ice-auth-mode {e:nable|b:ypass}` SNMP OID: -
Portsecurity Address Ageing Setup	
Ageing time (minutes)	Chapter: *10.36.12. Portsecurity - MAC Address Ageing* WEB: - Console Show: `> sh:ow con:figuration g:lobal [a:ll]` Console Set: `# co:nfig au:to-ageing (0|1..255)` SNMP OID: -
Portsecurity ageing time for PC behind IP-Phone (minutes)	Chapter: *10.36.12. Portsecurity - MAC Address Ageing* WEB: - Console Show: `> sh:ow con:figuration g:lobal [a:ll]` Console Set: `# co:nfig pc:-behind-phone-ageing (0|1..255)` SNMP OID: -
Portsecurity ageing time for 'Allowed MACs Overflow Address (minutes)	Chapter: *10.36.12. Portsecurity - MAC Address Ageing* WEB: - Console Show: `> sh:ow con:figuration g:lobal [a:ll]` Console Set: `# co:nfig al:lowed-mac-overflow-ageing (0|1..255)` SNMP OID: -

9.32. Security > RADIUS Global Authentication

Designation	Access
Authentication Server Setup	
Server 1 Address Server 2 Address Server 3 Address Server 4 Address	Chapter: *10.55. RADIUS Authentication* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius se:rver-ip (1|2|3|4) <ip-address>` SNMP OID: -
Authentication UDP Port (1...65535)	Chapter: *10.55. RADIUS Authentication* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius au:th po:rt (1...65535)` SNMP OID: -
Shared secret (0…50 chars)	Chapter: *10.55. RADIUS Authentication* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius au:th s:ecret [<string max 50 chars>]` SNMP OID: -
Request timeout (1...255 sec.)	Chapter: *10.55. RADIUS Authentication* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius t:imeout (1...255)` SNMP OID: -
Request retries (0...255)	Chapter: *10.55. RADIUS Authentication* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius ret:ries (0...255)` SNMP OID: -

VLAN attribute	Chapter: *10.55. RADIUS Authentication*
	WEB: -
	Console Show: `# sh:ow con:figuration ra:dius [a:ll]`
	Console Set:
	`# rad:ius v:lan-attribut {setup}`
	`Valid values for {setup} are:`
	`{v:endor-specific|tunnel-i:d|tunnel-d:escr|`
	`tunnel-b:oth|i:gnore-all}`
	SNMP OID: -

Cisco device-traffic-class mode	Chapter: *10.55. RADIUS Authentication*
	WEB: -
	Console Show: `# sh:ow con:figuration ra:dius [a:ll]`
	Console Set:
	`# rad:ius c:isco-tc-voice-mode {setup}`
	`Valid values for {setup} are:`
	`{s:et-voice-vlan-only|a:llow-access}`
	SNMP OID: -

Server request algorithm	Chapter: *10.55. RADIUS Authentication* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius req:uest-mode {s:trict-priority|r:ound-robin|p:arallel}` SNMP OID: -
MAC Bases Portsecurity	
MAC address separator (0…1 character)	Chapter: *10.55. RADIUS Authentication* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius ma:c-separator [<string max 1 char>]` SNMP OID: -
Portsecurity password (0…50 chars) (Default = 'port')	Chapter: *10.55. RADIUS Authentication* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius au:th pa:ssword <string 1 to 14 char>` SNMP OID: -

Startup VLAN-ID	Chapter: *10.55. RADIUS Authentication*
	WEB: -
	Console Show: `# sh:ow con:figuration ra:dius [a:ll]`
	Console Set: `# rad:ius st:artup-vlan`
	`Valid values for {setup} are:`
	`{u:nsecure-vlan|d:efault-vlan|`
	`block-u:nsecure-vlan|block-d:efault-vlan}`
	SNMP OID: -

Portsecurity realm (0…50 chars)	Chapter: *10.55. RADIUS Authentication* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius rea:lm p:ort [<string max 50 char.>]` SNMP OID: -
Management Authentication	
Management realm (0…50 chars)	Chapter: *10.55. RADIUS Authentication* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius rea:lm m:gmt [<string max 50 char.>]` SNMP OID: -
Global Realm Setup	
Realm location	Chapter: *10.55. RADIUS Authentication* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius rea:lm l:ocation {p:refix|s:uffix}` SNMP OID: -

Realm separator (0…50 character)	Chapter: *10.55. RADIUS Authentication* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius rea:lm s:eparator [<string max 1 char>]` SNMP OID: -

9.33. Security > RADIUS Management Authentication

Designation	Access
Authentication Server Setup	
Management Authentication Mode	Chapter: *10.55. RADIUS Authentication* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius mg:mt-auth m:ode {g:lobal-auth-settings|m:gmt-auth-settings}` SNMP OID: -
Server 1 Address Server 2 Address Server 3 Address Server 4 Address	Chapter: *10.55. RADIUS Authentication* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius mg:mt-auth s:erver-ip (1|2|3|4) <ip-address>` SNMP OID: -
Authentication UDP Port (1...65535)	Chapter: *10.55. RADIUS Authentication* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius mg:mt-auth a:uth p:ort (1...65535)` SNMP OID: -
Shared secret (0…50 chars)	Chapter: *10.55. RADIUS Authentication* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius mg:mt-auth a:uth s:ecret [<string max 50 chars>]` SNMP OID: -
Request timeout (1...255 sec.)	Chapter: *10.55. RADIUS Authentication* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius mg:mt-auth t:imeout (1...255)` SNMP OID: -
Request retries (0...255)	Chapter: *10.55. RADIUS Authentication* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius mg:mt-auth r:etries (0...255)` SNMP OID: -

9.34. Security > RADIUS Accounting

Designation	Access
Accounting Enable	
IEEE802.1X accounting enable	Chapter: *10.60. RADIUS Accounting* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius ac:counting do:t1x {e:nable|d:isable}` SNMP OID: -
MAC based accounting enable	Chapter: *10.60. RADIUS Accounting* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius ac:counting m:ac-based {e:nable|d:isable}` SNMP OID: -
Accounting Server Setup	
Server 1 Address Server 2 Address Server 3 Address Server 4 Address	Chapter: *10.60. RADIUS Accounting* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius ac:counting ser:ver-ip (1|2|3|4) <ip-address>` SNMP OID: -
Authentication UDP Port (1...65535)	Chapter: *10.60. RADIUS Accounting* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius ac:counting p:ort (1...65535)` SNMP OID: -
Shared secret (0…50 chars)	Chapter: *10.60. RADIUS Accounting* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius ac:counting sec:ret [<string max 50 chars>]` SNMP OID: -
Request timeout (1...255 sec.)	Chapter: *10.60. RADIUS Accounting* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius ac:counting t:imeout (1...255)` SNMP OID: -
Request retries (0...255)	Chapter: *10.60. RADIUS Accounting* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius ac:counting r:etries (0...255)` SNMP OID: -

Accounting Options	
Alive packets enable	Chapter: *10.60. RADIUS Accounting* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius ac:counting sen:d-alive-packets {e:nable|d:isable}` SNMP OID: -
Alive packets interval (1...240 minutes)	Chapter: *10.60. RADIUS Accounting* WEB: - Console Show: `# sh:ow con:figuration ra:dius [a:ll]` Console Set: `# rad:ius ac:counting a:live-packets-intervall (1...240)` SNMP OID: -

User-Name for 802.1X	Chapter: *10.60. RADIUS Accounting*
	WEB: -
	Console Show: `# sh:ow con:figuration ra:dius [a:ll]`
	Console Set: `# rad:ius ac:counting u:ser-name-dot1x {setup}`
	`Valid values for {setup} are:`
	`{e:ap-identity|u:ser-name|c:hargeable-user-identity}`
	SNMP OID: -

Discover IP Address	Chapter: *10.60. RADIUS Accounting*
	WEB: -
	Console Show: `# sh:ow con:figuration ra:dius [a:ll]`
	Console Set: `# rad:ius ac:counting di:scover-ip-address {setup}`
	`Valid values for {setup} are:`
	`{d:isable|f:ramed-ip-address}`
	SNMP OID: -

9.35. Security > IEEE802.1X

Designation	Access
IEEE802.1X Global Setup	
IEEE802.1X Transparency	Chapter: *10.35. IEEE802.1X Transparency* WEB: - Console Show: `# sh:ow con:figuration do:t1x [a:ll]` Console Set: `# dot:1x t:ransparency {e:nable|d:isable}` SNMP OID: -
IEEE802.1X Authenticator Setup	
Re-Authentication enabled	Chapter: *10.59. Portsecurity with authentication via RADIUS server* WEB: - Console Show: `# sh:ow con:figuration do:t1x [a:ll]` Console Set: `# do:t1x rea:uthentication {e:nable|d:isable}` SNMP OID: -

Re-Authentication initial delay (seconds) (0…65535) (Set to 0 to use Re-authentication interval)	Chapter: *10.59. Portsecurity with authentication via RADIUS server* WEB: - Console Show: `# sh:ow con:figuration do:t1x [a:ll]` Console Set: `# do:t1x rea:uthentication d:elay (0...65535)` SNMP OID: -
Re-Authentication interval (seconds) (1…65535)	Chapter: *10.59. Portsecurity with authentication via RADIUS server* WEB: - Console Show: `# sh:ow con:figuration do:t1x [a:ll]` Console Set: `# do:t1x rea:uthentication interval (1...65535)` SNMP OID: -
Re-Authentication Inaccessible VLAN Mode	Chapter: *10.59. Portsecurity with authentication via RADIUS server* WEB: - Console Show: `# sh:ow con:figuration do:t1x [a:ll]` Console Set: `# do:t1x rea:uthentication ina:ccessible-mode {m:ove|s:tay}` SNMP OID: -
Quiet Time after Auth. fails (seconds) (1…65535)	Chapter: *10.59. Portsecurity with authentication via RADIUS server* WEB: - Console Show: `# sh:ow con:figuration do:t1x [a:ll]` Console Set: `# do:t1x q:uiet-time (1...65535)` SNMP OID: -
Client request timeout (seconds) (1…65535)	Chapter: *10.59. Portsecurity with authentication via RADIUS server* WEB: - Console Show: `# sh:ow con:figuration do:t1x [a:ll]` Console Set: `# do:t1x req:uest t:imeout (1...65535)` SNMP OID: -
Client request retries (0…255)	Chapter: *10.59. Portsecurity with authentication via RADIUS server* WEB: - Console Show: `# sh:ow con:figuration do:t1x [a:ll]` Console Set: `# do:t1x req:uest r:tries (0...255)` SNMP OID: -
Max. Authentication retries (0…255)	Chapter: *10.59. Portsecurity with authentication via RADIUS server* WEB: - Console Show: `# sh:ow con:figuration do:t1x [a:ll]` Console Set: `# do:t1x a:uthentication r:etries (0...255)` SNMP OID: -

Radius MAC Bypass	Chapter: *10.59. Portsecurity with authentication via RADIUS server*
	WEB: -
	Console Show: `# sh:ow con:figuration do:t1x [a:ll]`
	Console Set: `#dot:1x m:ac-bypass {setup}`
	`Valid values for {setup} are:`
	`{d:isable|e:nable|s:ingle|fallback-e:nable|fallback-s:ingle|immediate-e:nable|immediate-s:ingle|immediate-fallback-e:nable|immediate-fallback-s:ingle}`
	SNMP OID: -

MAC bypass Quiet Time	Chapter: *10.59. Portsecurity with authentication via RADIUS server* WEB: - Console Show: `# sh:ow con:figuration do:t1x [a:ll]` Console Set: `# dot:1x m:ac-bypass q:uiet-time (0...65535)` SNMP OID: -
EAP packets within Voice-VLAN	Chapter: *10.59.8. Portsecurity Option {EAP Packets within Voice-VLAN}* WEB: - Console Show: `# sh:ow con:figuration do:t1x [a:ll]` Console Set: `# do:t1x v:oice-vlan-eap-packets {t:agged|u:ntagged)` SNMP OID: -
IEEE802.1X Supplicant Setup	
MD5 Name (0…50 chars)	Chapter: *10.59.9. Portsecurity Modus {IEEE802.1X Supplicant}* WEB: - Console Show: `# sh:ow con:figuration do:t1x [a:ll]` Console Set: `# do:t1x s:upplicant n:ame [<string max 50 chars>]` SNMP OID: -
MD5 Password (0…50 chars)	Chapter: *10.59.9. Portsecurity Modus {IEEE802.1X Supplicant}* WEB: - Console Show: `# sh:ow con:figuration do:t1x [a:ll]` Console Set: `# do:t1x s:upplicant p:assword [<string max 50 chars>]` SNMP OID: -

9.36. Security > TACACS+ Authentication

Designation	Access
Authentication Server Setup	
Server 1 Address Server 2 Address Server 3 Address Server 4 Address	Chapter: *10.61 TACACS+ Authentication* WEB: - Console Show: `# sh:ow con:figuration t:acacs+ [a:ll]` Console Set: `# ta:cacs+ authe:ntication ser:ver-ip (1...4) {<ip-address>|di:sable}` SNMP OID: -
Authentication TCP Port (1...65535)	Chapter: *10.61 TACACS+ Authentication* WEB: - Console Show: `# sh:ow con:figuration t:acacs+ [a:ll]` Console Set: `# ta:cacs+ authe:ntication p:ort (1...65535)` SNMP OID: -
Shared secret (0…50 chars)	Chapter: *10.61 TACACS+ Authentication* WEB: - Console Show: `# sh:ow con:figuration t:acacs+ [a:ll]` Console Set: `# ta:cacs+ authe:ntication sec:ret [<string max 50 chars>]` SNMP OID: -

Request timeout (1...255 sec.)	Chapter: *10.61 TACACS+ Authentication* WEB: - Console Show: `# sh:ow con:figuration t:acacs+ [a:ll]` Console Set: `# ta:cacs+ authe:ntication t:imeout (1...255)` SNMP OID: -
Server request algorithm	Chapter: *10.61 TACACS+ Authentication* WEB: - Console Show: `# sh:ow con:figuration t:acacs+ [a:ll]` Console Set: `# ta:cacs+ authe:ntication req:uest-mode {s:trict-priority|r:ound-robin|p:arallel}` SNMP OID: -

9.37. Security > TACACS+ Authorization

Designation	Access
Authorization Server Setup	
Authorization Mode	Chapter: *10.62 TACACS+ Authorization* WEB: - Console Show: `# sh:ow con:figuration t:acacs+ [a:ll]` Console Set: `# ta:cacs+ autho:rization m:ode {authe:ntication-settings|autho:rization-settings}` SNMP OID: -
Command Authorization	Chapter: *10.62 TACACS+ Authorization* WEB: - Console Show: `# sh:ow con:figuration t:acacs+ [a:ll]` Console Set: `# ta:cacs+ autho:rization c:ommands {d:isabled|e:enabled}` SNMP OID: -
Server 1 Address Server 2 Address Server 3 Address Server 4 Address	Chapter: *10.62 TACACS+ Authorization* WEB: - Console Show: `# sh:ow con:figuration t:acacs+ [a:ll]` Console Set: `# ta:cacs+ autho:rization ser:ver-ip (1...4) {<ip-address>|di:sable}` SNMP OID: -
Authorization TCP Port (1...65535)	Chapter: *10.62 TACACS+ Authorization* WEB: - Console Show: `# sh:ow con:figuration t:acacs+ [a:ll]` Console Set: `# ta:cacs+ autho:rization p:ort (1...65535)` SNMP OID: -
Shared secret (0…50 chars)	Chapter: *10.62 TACACS+ Authorization* WEB: - Console Show: `# sh:ow con:figuration t:acacs+ [a:ll]` Console Set: `# ta:cacs+ autho:rization sec:ret [<string max 50 chars>]` SNMP OID: -

Request timeout (1...255 sec.)	Chapter: *10.62 TACACS+ Authorization* WEB: - Console Show: `# sh:ow con:figuration t:acacs+ [a:ll]` Console Set: `# ta:cacs+ autho:rization t:imeout (1...255)` SNMP OID: -
Server request algorithm	Chapter: *10.62 TACACS+ Authorization* WEB: - Console Show: `# sh:ow con:figuration t:acacs+ [a:ll]` Console Set: `# ta:cacs+ autho:rization req:uest-mode {s:trict-priority|r:ound-robin|p:arallel}` SNMP OID: -

9.38. Security > TACACS+ Accounting

Designation	Access
Accounting Server Setup	
Accounting Mode	Chapter: *10.63 TACACS+ Accounting* WEB: - Console Show: `# sh:ow con:figuration t:acacs+ [a:ll]` Console Set: `# ta:cacs+ ac:counting m:ode {d:isabled| au:thentication-settings|ac:counting-settings}` SNMP OID: -
Server 1 Address Server 2 Address Server 3 Address Server 4 Address	Chapter: *10.63 TACACS+ Accounting* WEB: - Console Show: `# sh:ow con:figuration t:acacs+ [a:ll]` Console Set: `# ta:cacs+ ac:counting ser:ver-ip (1...4) {<ip-address>|di:sable}` SNMP OID: -
Accounting TCP Port (1...65535)	Chapter: *10.63 TACACS+ Accounting* WEB: - Console Show: `# sh:ow con:figuration t:acacs+ [a:ll]` Console Set: `# ta:cacs+ ac:counting p:ort (1...65535)` SNMP OID: -
Shared secret (0…50 chars)	Chapter: *10.63 TACACS+ Accounting* WEB: - Console Show: `# sh:ow con:figuration t:acacs+ [a:ll]` Console Set: `# ta:cacs+ ac:counting sec:ret [<string max 50 chars>]` SNMP OID: -
Request timeout (1...255 sec.)	Chapter: *10.63 TACACS+ Accounting* WEB: - Console Show: `# sh:ow con:figuration t:acacs+ [a:ll]` Console Set: `# ta:cacs+ ac:counting t:imeout (1...255)` SNMP OID: -

Server request algorithm	Chapter: *10.63 TACACS+ Accounting* WEB: - Console Show: `# sh:ow con:figuration t:acacs+ [a:ll]` Console Set: `# ta:cacs+ ac:counting req:uest-mode {s:trict-priority|r:ound-robin|p:arallel}` SNMP OID: -

9.39. Security > Access Control List

Designation	Access
Access Control List Mode	
Enable Static	Chapter: *10.68.6 Static ACLs* WEB: - Console Show: `# sh:ow con:figuration acl` `sh:ow acl stati:c` Console Set: `# acl s:tatic {e:nable|d:isable}` SNMP OID: -
Enable Dynamic	Chapter: *10.68.7 Dynamic ACLs* WEB: - Console Show: `# sh:ow acl d:ynamic` Console Set: `# acl dy:namic {e:nable|d:isable}` SNMP OID: -
Show ACL State	Chapter: *10.68.9 ACL Status* WEB: - Console Show: `# sh:ow acl statu:s` Console Set: `# -` SNMP OID: -

Access Control List Commands	

Access Control List Commands	Chapter: *10.68.4 ACL Definition*
	10.68.3 ACL Rules Definition
	WEB: -
	Console Show: `# sh:ow con:figuration acl`
	`sh:ow acl stati:c`
	Console Set: `# acl {s:tatic|dy:namic} c:lear`
	`acl {c:reate|de:lete} [<string max. 64 chars>] (max. 64 ACLs allowed)`
	`acl {a:dd|r:emove} [<string max. 64 chars>] r:ule (1..200)`
	`in:terface {if-no range} ac:l a:dd [<string max. 64 chars>]`
	`in:terface {if-no range} ac:l r:emove [<string max. 64 chars>]`
	`ru:le c:reate (1..200) v:lan {a:ny|(1..4094)} {p:ermit|d:eny} ipv4 p:rotocol {a:ny|(1..YYY)} source {a:ny|<ip-addr>[/ (1..32)]} destination {a:ny|<ip-addr>[/(1..32)]}`
	`ru:le c:reate (1..200) v:lan {a:ny|(1..4094)} {p:ermit|d:eny} ipv4 p:rotocol {t:cp|u:dp} s:ource {a:ny|<ip-addr>[/(1..32)]} p:ort {a:ny|(1..YYY)} d:estination {a:ny|<ip-addr>[/(1..32)]} p:ort {a:ny|(1..YYY)}`
	`ru:le c:reate (1..200) v:lan {a:ny|(1..4094)} {p:ermit|d:eny} ipv4 a:ny`
	`ru:le c:reate (1..200) v:lan {a:ny|(1..4094)} {p:ermit|d:eny} ipv6 p:rotocol {a:ny|(1..YYY)} d:estination {a:ny|<ipv6-addr>[/(1..32)]}`
	`ru:le c:reate (1..200) v:lan {a:ny|(1..4094)} {p:ermit|d:eny} ipv6 p:rotocol {t:cp|u:dp} d:estination {a:ny|<ipv6-addr>[/(1..32)]} p:ort {a:ny|(1..YYY)}`
	`ru:le c:reate (1..200) v:lan {a:ny|(1..4094)} {p:ermit|d:eny} ipv6 a:ny`
	`ru:le c:reate (1..200) v:lan {a:ny|(1..4094)} {p:ermit|d:eny} mac e:type {a:ny|(1..YYY)} s:ource {a:ny | <mac-addr>[/ (1..48)]} d:estination {a:ny | <mac-addr>[/(1..48)]}`
	`ru:le d:elete (1..200)`
	SNMP OID: -

9.40. Multicasts

Designation	**Access**
IGMP Snooping Setup	
IGMP Snooping enable	Chapter: *110.69.1. IGMP Snooping* WEB: - Console Show: `> sh:ow con:figuration ig:mp [a:ll]` Console Set: `# ig:mp s:nooping {e:nable|d:isable}` SNMP OID: -

Snoop Table Ageing Time (seconds)	Chapter: *110.69.1. IGMP Snooping* WEB: - Console Show: `> sh:ow con:figuration ig:mp [a:ll]` Console Set: `# ig:mp s:nooping a:geing (10...65535)` SNMP OID: -
Accept IGMP Version 1/2/3	Chapter: *110.69.1. IGMP Snooping* WEB: - Console Show: `> sh:ow con:figuration ig:mp [a:ll]` Console Set: `# ig:mp s:nooping v:ersion {1|2|3|mld-v1|mld-v2} {e:nable|d:isable}` SNMP OID: -
Accept MLD Version 1/2	Chapter: *110.69.1. IGMP Snooping* WEB: - Console Show: `> sh:ow con:figuration ig:mp [a:ll]` Console Set: `# ig:mp s:nooping v:ersion {1|2|3|mld-v1|mld-v2} {e:nable|d:isable}` SNMP OID: -
Immediate Leave Mode	Chapter: *110.69.1. IGMP Snooping* WEB: - Console Show: `> sh:ow con:figuration ig:mp [a:ll]` Console Set: `# ig:mp s:nooping l:eave-mode {accept-u:ser-ports|accept-a:ll|i:gnore-all}` SNMP OID: -
Clear Snoop Tables	Chapter: *110.69.1. IGMP Snooping* WEB: - Console Set: `# ig:mp s:nooping c:lear-tables` SNMP OID: -
IGMP Querier Setup	
IGMP Querier enable	Chapter: *10.69.2. IGMP Querier* WEB: - Console Show: `> sh:ow con:figuration ig:mp [a:ll]` Console Set: `# ig:mp q:uerier {e:nable|d:isable}` SNMP OID: -
Query interval (seconds)	Chapter: *10.69.2. IGMP Querier* WEB: - Console Show: `> sh:ow con:figuration ig:mp [a:ll]` Console Set: `# ig:mp q:uerier i:nterval (10...3600)` SNMP OID: -
IGMP State	
IGMP State	Chapter: *10.69.2. IGMP Querier* WEB: - Console Show: `> sh:ow con:figuration ig:mp [a:ll]` SNMP OID: -

9.41. Time Client > SNTP Setup

Designation	Access
SNTP Client Setup	
Client enabled	Chapter: *10.28.3. Network Time Protocol - SNTP* WEB: - Console Show: `> sh:ow con:figuration s:ntp [a:ll]` Console Set: `# snt:p st:atus {e:nable|d:isable}` SNMP OID: -
Time server IP 1	Chapter: *10.28.3. Network Time Protocol - SNTP* WEB: - Console Show: `> sh:ow con:figuration s:ntp [a:ll]` Console Set: `# snt:p se:rver-ip {<ip-address>|di:sable}` SNMP OID: -
Time server IP 2	Chapter: *10.28.3. Network Time Protocol - SNTP* WEB: - Console Show: `> sh:ow con:figuration s:ntp [a:ll]` Console Set: `# snt:p server-ip-2 {<ip-address>|di:sable}` SNMP OID: -
Server request interval (seconds)	Chapter: *10.28.3. Network Time Protocol - SNTP* WEB: - Console Show: `> sh:ow con:figuration s:ntp [a:ll]` Console Set: `# snt:p i:nterval (0..65535)` SNMP OID: -
SNTP protocoll version (1...4)	Chapter: *10.28.3. Network Time Protocol - SNTP* WEB: - Console Show: `> sh:ow con:figuration s:ntp [a:ll]` Console Set: `# snt:p v:ersion (1..4)` SNMP OID: -
Accept SNTP broadcasts	Chapter: *10.28.3. Network Time Protocol - SNTP* WEB: - Console Show: `> sh:ow con:figuration s:ntp [a:ll]` Console Set: `# snt:p b:roadcast {e:nable|d:isable}` SNMP OID: -
UTC local offset (minutes)	Chapter: *10.28.3. Network Time Protocol - SNTP* WEB: - Console Show: `> sh:ow con:figuration s:ntp [a:ll]` Console Set: `# snt:p o:ffset (-720..720)` SNMP OID: -
Summer time correction	Chapter: *10.28.3. Network Time Protocol - SNTP* WEB: - Console Show: `> sh:ow con:figuration s:ntp [a:ll]` Console Set: `# snt:p su:mmertime {d:isabled|e:st}` SNMP OID: -

Manual Time Request	Chapter: *10.28.3. Network Time Protocol - SNTP* WEB: - Console Set: `# snt:p r:equest-now` SNMP OID: -

9.42. Time Client > Powersave Setup

Designation	Access
Powersave Times	

End time hour	Chapter: *10.20.5. Automatic Powersave*
	WEB: -
	Console Show: `> sh:ow con:figuration s:ntp [a:ll]`
	Console Set: `# snt:p p:ower-save {day} e:nd-time (0...23)`
	`Valid values for {day} are:`
	`{su:nday|mo:nday|tu:esday|we:dnesday|th:ursday|`
	`fr:iday|sa:turday}`
	SNMP OID: -

End time hour	Chapter: *10.20.5. Automatic Powersave*
	WEB: -
	Console Show: `> sh:ow con:figuration s:ntp [a:ll]`
	Console Set: `# snt:p p:ower-save {day} s:tart-time (0...23)`
	`Valid values for {day} are:`
	`{su:nday|mo:nday|tu:esday|we:dnesday|th:ursday|`
	`fr:iday|sa:turday}`
	SNMP OID: -

9.43. Redundancy Spanning Tree

Designation	Access
RSTP Global Setup	
Spanning Tree Global enable	Chapter: *10.73.2. RSTP - Global configuration parameters* WEB: - Console Show: `> sh:ow con:figuration re:dundancy [a:ll]` Console Set: `# rs:tp m:ode {e:nabled|d:isabled}` SNMP OID: -
Protocol version	Chapter: *10.73.2. RSTP - Global configuration parameters* WEB: - Console Show: `> sh:ow con:figuration re:dundancy [a:ll]` Console Set: `# rs:tp v:ersion {r:stp-stp|s:tp-only}` SNMP OID: `RSTP-MIB → dot1dStpVersion`

CIST Bridge priority	Chapter:	*10.73.2. RSTP - Global configuration parameters*
	WEB:	-
	Console Show:	`> sh:ow con:figuration re:dundancy [a:ll]`
	Console Set:	`# rs:tp p:riority (0..61440)`
	SNMP OID:	`BRIDGE-MIB → dot1dStpPriority`
Forward Delay (seconds)	Chapter:	*10.73.2. RSTP - Global configuration parameters*
	WEB:	-
	Console Show:	`> sh:ow con:figuration re:dundancy [a:ll]`
	Console Set:	`# rs:tp f:orward-delay (4..30)`
	SNMP OID:	`BRIDGE-MIB → dot1dStpBridgeForwardDelay`
Max. age/hops	Chapter:	*10.73.2. RSTP - Global configuration parameters*
	WEB:	-
	Console Show:	`> sh:ow con:figuration re:dundancy [a:ll]`
	Console Set:	`# rs:tp a:ge-time-max (6..50)`
	SNMP OID:	`BRIDGE-MIB → dot1dStpBridgeMaxAge`
Hello time (seconds)	Chapter:	*10.73.2. RSTP - Global configuration parameters*
	WEB:	-
	Console Show:	`> sh:ow con:figuration re:dundancy [a:ll]`
	Console Set:	`# rs:tp h:ello-time (1..10)`
	SNMP OID:	`BRIDGE-MIB → dot1dStpBridgeHelloTime`
Transmit hold count	Chapter:	*10.73.2. RSTP - Global configuration parameters*
	WEB:	-
	Console Show:	`> sh:ow con:figuration re:dundancy [a:ll]`
	Console Set:	`# rs:tp t:x-hold-count (1..10)`
	SNMP OID:	`RSTP-MIB → dot1dStpTxHoldCount`
Re-enable time for BPDU-Disabled ports	Chapter:	*10.73.2. RSTP - Global configuration parameters*
	WEB:	-
	Console Show:	`> sh:ow con:figuration re:dundancy [a:ll]`
	Console Set:	`# co:nfig r:e-enable b:pdu-disable (0...60000)`
	SNMP OID:	-
Debugging Mode	Chapter:	*10.73.2. RSTP - Global configuration parameters*
	WEB:	-
	Console Show:	`> sh:ow con:figuration re:dundancy [a:ll]`
	Console Set:	`# de:bug s:tp lo:cal {e:nabled|d:isabled}`
	SNMP OID:	-
RSTP Port Setup		
Spanning Tree Port Mode	Chapter:	*10.73.3. RSTP - Port configuration parameters*
	WEB:	-
	Console Show:	`> sh:ow con:figuration re:dundancy [a:ll]`

	Console Set:	`# rs:tp i:nterface <if-no> mo:de {setup}`
		`Enables or disables spanning tree for this port.`
		`Valid values for {setup} are:`
		`{e:nable|l:oop-protect-enable|d:isable|b:pdu-disable}`

	SNMP OID:	`BRIDGE-MIB → dot1dStpPortEnable`

Priority	Chapter: *10.73.3. RSTP - Port configuration parameters* WEB: - Console Show: `> sh:ow con:figuration re:dundancy [a:ll]` Console Set: `# rs:tp i:nterface <if-no> pr:iority (0..240)` SNMP OID: `BRIDGE-MIB → dot1dStpPortEnable`

Path cost mode	Chapter: *10.73.3. RSTP - Port configuration parameters*
	WEB: -
	Console Show: `> sh:ow con:figuration re:dundancy [a:ll]`
	Console Set: `# rs:tp i:nterface <if-no> pa:th co:st-mode {mode}`
	`Valid values for {mode} are:`
	`{r:stp-auto|s:tp-auto|m:anual}`
	SNMP OID: -

Manual path cost	Chapter: *10.73.3. RSTP - Port configuration parameters* WEB: - Console Show: `> sh:ow con:figuration re:dundancy [a:ll]` Console Set: `# rs:tp i:nterface <if-no> pa:th ma:nual-cost (1..200000000)` SNMP OID: `RSTP-MIB → dot1dStpPortAdminPathCost`

Edge port	Chapter: *10.73.3. RSTP - Port configuration parameters*
	WEB: -
	Console Show: `> sh:ow con:figuration re:dundancy [a:ll]`
	Console Set: `# rs:tp i:nterface <if-no> ad:min-edge-port {mode}`
	`Valid values for {mode} are:`
	`{n:o|y:es-portfast}`
	SNMP OID: `RSTP-MIB → dot1dStpPortAdminEdgePort`

Point to Point link	Chapter: *10.73.3. RSTP - Port configuration parameters* WEB: - Console Show: `> sh:ow con:figuration re:dundancy [a:ll]` Console Set: `# rs:tp i:nterface <if-no> po:int-to-point {y:es|n:o|a:uto}` SNMP OID: `RSTP-MIB → dot1dStpPortAdminPointToPoint`
RSTP Global Status	
Bridge Status	Chapter: *10.73.4. RSTP - Global state parameters* WEB: - Console Show: `> sh:ow rs:tp` SNMP OID: -
Root Bridge ID	Chapter: *10.73.4. RSTP - Global state parameters* WEB: - Console Show: `> sh:ow rs:tp` SNMP OID: `BRIDGE-MIB → dot1dStpDesignatedRoot`
Root Port	Chapter: *10.73.4. RSTP - Global state parameters* WEB: - Console Show: `> sh:ow rs:tp` SNMP OID: `BRIDGE-MIB → dot1dStpRootPort`
Root Cost	Chapter: *10.73.4. RSTP - Global state parameters* WEB: - Console Show: `> sh:ow rs:tp` SNMP OID: `BRIDGE-MIB → dot1dStpRootCost`

Learned Max Age	Chapter: *10.73.4. RSTP - Global state parameters* WEB: - Console Show: `> sh:ow rs:tp` SNMP OID: `BRIDGE-MIB → dot1dStpMaxAge`
Learned Hello Time	Chapter: *10.73.4. RSTP - Global state parameters* WEB: - Console Show: `> sh:ow rs:tp` SNMP OID: `BRIDGE-MIB → dot1dStpHelloTime`
Learned Forward Delay	Chapter: *10.73.4. RSTP - Global state parameters* WEB: - Console Show: `> sh:ow rs:tp` SNMP OID: `BRIDGE-MIB → dot1dStpForwardDelay`
Topology Changes	Chapter: *10.73.4. RSTP - Global state parameters* WEB: - Console Show: `> sh:ow rs:tp` SNMP OID: `BRIDGE-MIB → dot1dStpTopChanges`
Time since last Topology Change	Chapter: *10.73.4. RSTP - Global state parameters* WEB: - Console Show: `> sh:ow rs:tp` SNMP OID: `BRIDGE-MIB → dot1dStpTimeSinceTopologyChange`
RSTP Port Status	
State	Chapter: *10.73.5. RSTP - Port state parameters* WEB: Port State Console Show: `> sh:ow rs:tp` SNMP OID: `BRIDGE-MIB → dot1dStpPortState`
Path Cost	Chapter: *10.73.5. RSTP - Port state parameters* WEB: - Console Show: `> sh:ow rs:tp` SNMP OID: `BRIDGE-MIB → dot1dStpPortPathCost` `BRIDGE-MIB → dot1dStpPortPathCost32`
Designated Root	Chapter: *10.73.5. RSTP - Port state parameters* WEB: - Console Show: `> sh:ow rs:tp` SNMP OID: `BRIDGE-MIB → dot1dStpPortDesignatedRoot`
Designated Cost	Chapter: *10.73.5. RSTP - Port state parameters* WEB: - Console Show: `> sh:ow rs:tp` SNMP OID: `BRIDGE-MIB → dot1dStpPortDesignatedCost`
Designated Bridge	Chapter: *10.73.5. RSTP - Port state parameters* WEB: - Console Show: `> sh:ow rs:tp` SNMP OID: `BRIDGE-MIB → dot1dStpPortDesignatedBridge`
Designated Port	Chapter: *10.73.5. RSTP - Port state parameters* WEB: - Console Show: `> sh:ow rs:tp` SNMP OID: `BRIDGE-MIB → dot1dStpPortDesignatedPort`

Port Role	Chapter: *10.73.5. RSTP - Port state parameters* WEB: - Console Show: `> sh:ow rs:tp` SNMP OID: -
Edge Port	Chapter: *10.73.5. RSTP - Port state parameters* WEB: - Console Show: `> sh:ow rs:tp` SNMP OID: `RSTP-MIB → dot1dStpPortOperEdgePort`
Point-to-Point Link	Chapter: *10.73.5. RSTP - Port state parameters* WEB: - Console Show: `> sh:ow rs:tp` SNMP OID: `RSTP-MIB → dot1dStpPortOperPointToPoint`
Spanning Tree Protocol detected	Chapter: *10.73.5. RSTP - Port state parameters* WEB: - Console Show: `> sh:ow rs:tp` SNMP OID: -

9.44. Redundancy > Multiple Spanning Tree

Designation	Access
Multiple Spanning Tree - Indentifier Setup	
MSTP Name	Chapter: *10.74.2. MSTP - Indentifier Setup* WEB: - Console Show: `> sh:ow con:figuration re:dundancy [a:ll]` Console Set: `# rs:tp ms:tp n:ame <string 1...32 chars>` SNMP OID: -
MSTP Revision	Chapter: *10.74.2. MSTP - Indentifier Setup* WEB: - Console Show: `> sh:ow con:figuration re:dundancy [a:ll]` Console Set: `# rs:tp ms:tp r:evision (1...65535)` SNMP OID: -
Multiple Spanning Tree - Instance Setup	
Instance ID Offset	Chapter: *10.74.3. MSTP - Instance Setup* WEB: - Console Show: `> sh:ow con:figuration re:dundancy [a:ll]` Console Set: `# rs:tp ms:tp i:nstance-id o:ffset (0...4000)` SNMP OID: -

Instance ID	Chapter: *10.74.3. MSTP - Instance Setup* WEB: - Console Show: `> sh:ow con:figuration re:dundancy [a:ll]` Console Set: `# rs:tp ms:tp i:nstance-id (1...4094) a:dd-vlan (1...4094)[-(1...4094)]` `# rs:tp ms:tp i:nstance-id (1...4094) d:elete` SNMP OID: -
Bridge Priority	Chapter: *10.74.3. MSTP - Instance Setup* WEB: - Console Show: `> sh:ow con:figuration re:dundancy [a:ll]` Console Set: `# s:tp ms:tp i:nstance-id (1...4094) p:riority (0..61440)` SNMP OID: -

9.45. Redundancy > Link Aggregation

Designation	Access
Link Aggregation - Global Setup	
Link Aggregation global enable	Chapter: *10.75.2 Link Aggregation - Global Setup* WEB: - Console Show: `> sh:ow con:figuration re:dundancy [a:ll]` Console Set: `# li:nk-aggr mo:de {e:nabled|d:isabled}` SNMP OID: -
Link Aggregation Protocol Timeout	Chapter: *10.75.2 Link Aggregation - Global Setup* WEB: - Console Show: `> sh:ow con:figuration re:dundancy [a:ll]` Console Set: `# li:nk-aggr t:imeout {s:low|f:ast}` SNMP OID: -
Link Aggregation – Group Setup	
Mode	Chapter: *10.75.3 Link Aggregation – Group Setup* WEB: - Console Show: `> sh:ow li:nk-aggr` Console Set: `# li:nk-aggr g:roup (1...8) m:ode {s:tatic|l:acp|dis:able|del:ete}` SNMP OID: -
Name	Chapter: *10.75.3 Link Aggregation – Group Setup* WEB: - Console Show: `> sh:ow li:nk-aggr` Console Set: `# li:nk-aggr g:roup (1...8) n:ame [<string max. 15 chars>]` SNMP OID: -

Member Ports	Chapter: *10.75.3 Link Aggregation – Group Setup* WEB: - Console Show: `> sh:ow li:nk-aggr` Console Set: `# li:nk-aggr g:roup (1...8) a:dd-port <if-no>` `# li:nk-aggr g:roup (1...8) d:elete-port <if-no>` SNMP OID: -

9.46. Redundancy > MRP

Designation	Access
Media Ring Redundancy - Global Setup	
MRP global enable	Chapter: *10.76. Media Redundancy Protocol (MRP)* WEB: - Console Show: `> sh:ow con:figuration re:dundancy [a:ll]` Console Set: `# mrp mo:de {e:nabled|d:isabled}` SNMP OID: -
Max. Recovery Time	Chapter: *10.76. Media Redundancy Protocol (MRP)* WEB: - Console Show: > sh:ow mr:p Console Set: # mrp ma:x-recovery-time {200|500} SNMP OID: -
Media Ring Redundancy - Instance Setup	
Admin Role	Chapter: *10.76. Media Redundancy Protocol (MRP)* WEB: - Console Show: `> sh:ow mr:p` Console Set: `# mrp i:nstance (0...4) ro:le {d:isabled|m:anager|p:riority-manager|c:lient}` SNMP OID: -
Domain-ID	Chapter: *10.76. Media Redundancy Protocol (MRP)* WEB: - Console Show: `> sh:ow mr:p` Console Set: `# mrp i:nstance (0...4) d:omain-id (0...255)` SNMP OID: -
VLAN-ID	Chapter: *10.76. Media Redundancy Protocol (MRP)* WEB: - Console Show: `> sh:ow mr:p` Console Set: `# mrp i:nstance (0...4) v:lan (0...4095)` SNMP OID: -
Ring Port 1	Chapter: *10.76. Media Redundancy Protocol (MRP)* WEB: - Console Show: `> sh:ow mr:p` Console Set: `# mrp i:nstance (0...4) ring-if-1 <if-no>` SNMP OID: -

Ring Port 2	Chapter: *10.76. Media Redundancy Protocol (MRP)* WEB: - Console Show: `> sh:ow mr:p` Console Set: `# mrp i:nstance (0...4) ring-if-2 <if-no>` SNMP OID: -
Media Ring Redundancy – MRP to Spanning Tree network coupling	
MRP to STP coupling Mode:	Chapter: *10.76 Media Redundancy Protocol (MRP)* WEB: - Console Show: `> sh:ow mr:p` Console Set: `# mrp s:tp-coupling-m:ode {d:isable|f:unc-input-1|a:larm-m1}` SNMP OID: -
MRP to STP coupling Port:	Chapter: *10.76 Media Redundancy Protocol (MRP)* WEB: - Console Show: `> sh:ow mr:p` Console Set: `# mrp stp-coupling-i:nterface {d:isable|<if-no>}` SNMP OID: -

9.47. Redundancy > Zeroloss

Zeroloss	
Zeroloss global enable	Chapter: 10.68 Zeroloss WEB: - Console Show: `> sh:ow z:eroloss` Console Set: `# z:eroloss m:ode {e:nabled|d:isabled}` SNMP OID: -
Zeroloss Port Setup	Chapter: 10.68 Zeroloss WEB: - Console Show: > sh:ow z:eroloss Console Set: # z:eroloss i:nterface <if-no> r:ole {r:ingport|u:serport|d:isabled} SNMP OID: -
Zeroloss Port Setup	Chapter: 10.68 Zeroloss WEB: - Console Show: > sh:ow z:eroloss Console Set: # z:eroloss i:nterface <if-no> e:thertype (0x8800...0xFFF) SNMP OID: -

9.48. DHCP Relay / Snooping

Designation	Access
DHCP Snooping	
DHCP Snooping	Chapter: *10.78.2 DHCP Snooping – Global Setup* WEB: - Console Show: `> sh:ow con:figuration dhcp-s:nooping [a:ll]` Console Set: `# dh:cp s:nooping mo:de {e:nabled|d:isabled}` SNMP OID: -
DHCP Snooping	Chapter: *10.78.2 DHCP Snooping – Global Setup* WEB: - Console Show: `> sh:ow con:figuration dhcp-s:nooping [a:ll]` Console Set: `# co:nfig r:e-enable d:hcp-snoop-disable (0...60000)` SNMP OID: -
DHCP Relay Agent - Global Setup	
DHCP Relay Agent global enable	Chapter: *0* *DHCP Relay* Agent WEB: - Console Show: `> sh:ow d:hcp r:elay` Console Set: `# dh:cp rela:y mo:de {e:nabled|d:isabled}` SNMP OID: -

10. Switch Features

10.1. Determination of Switch Type and Management Version

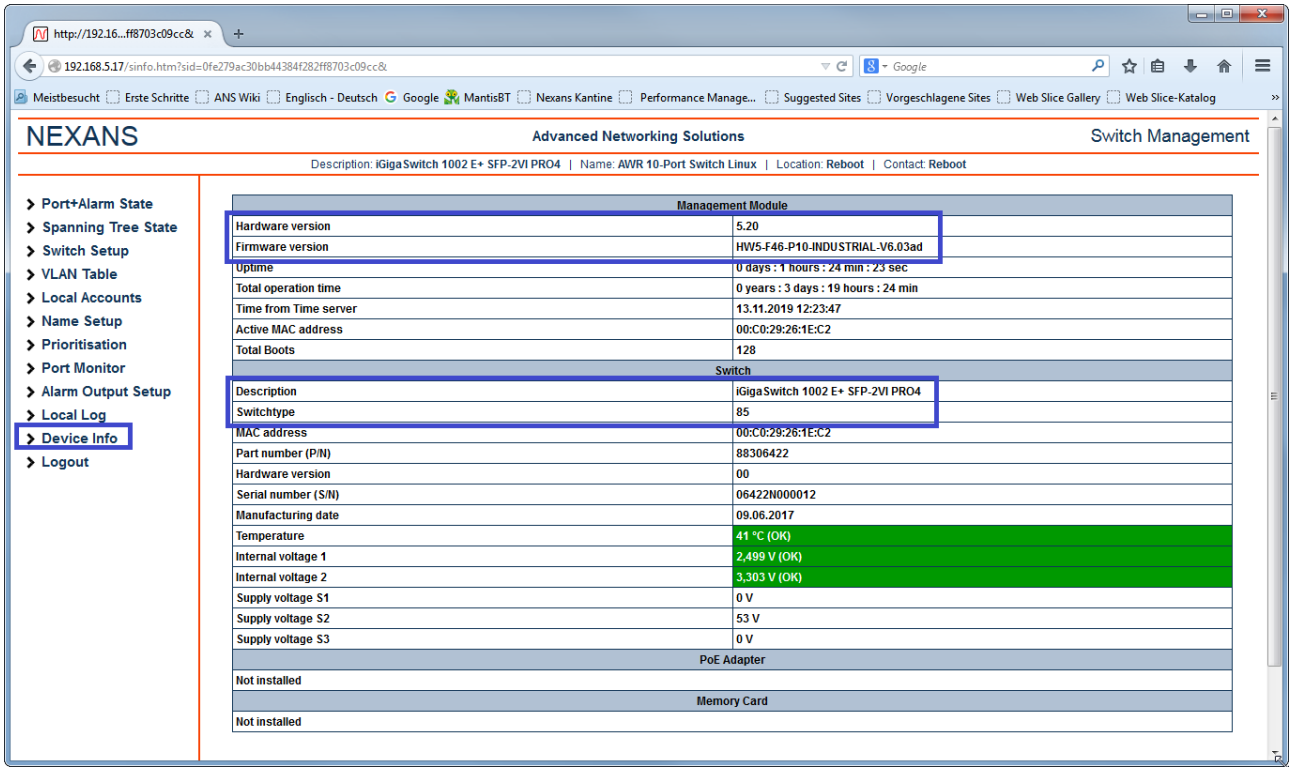
The current switch type and the installed management firmware and hardware version can be verified via WEB, Telnet/SSH/V.24 console, SNMP and NEXMAN. Chapter *2. Switch* contains a list of all supported switch types.

NOTE:

On HW5 switches two firmware versions are parallelly stored on different boot partitions. When a firmware update is installed, the currently running firmware is saved as backup, and the installed firmware becomes the new running firmware (see chapter *7.1.1 Dual Firmware Storage*). Thus, for HW5 switches in addition to the running firmware version the backup firmware version that is located on the other boot partition is also shown in CLI and Manager.

10.1.1. Query via WEB

Menu Device Info:



10.1.2. Query via SNMP

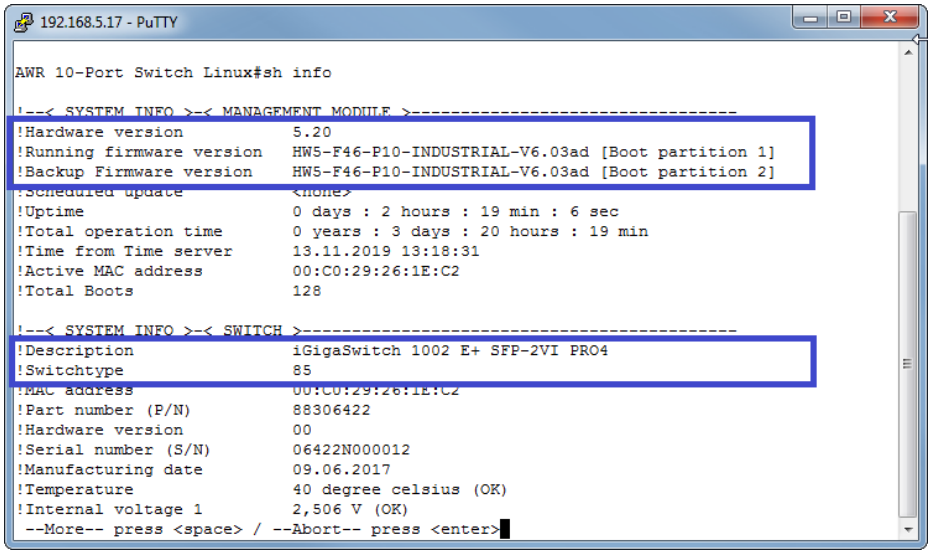
InfoType or infoMgmtFirmwareVersion SNMP variable in the Private MIB

SNMP-OID = private(4)
enterprises(1)
nexansActiveNetworkingSystems(266)
bmSwitchManagement(20)
bmSwitchInfo(1)
→ infoType(2)
→ infoMgmtHardwareVersion (8)
→ infoMgmtFirmwareVersion (9)

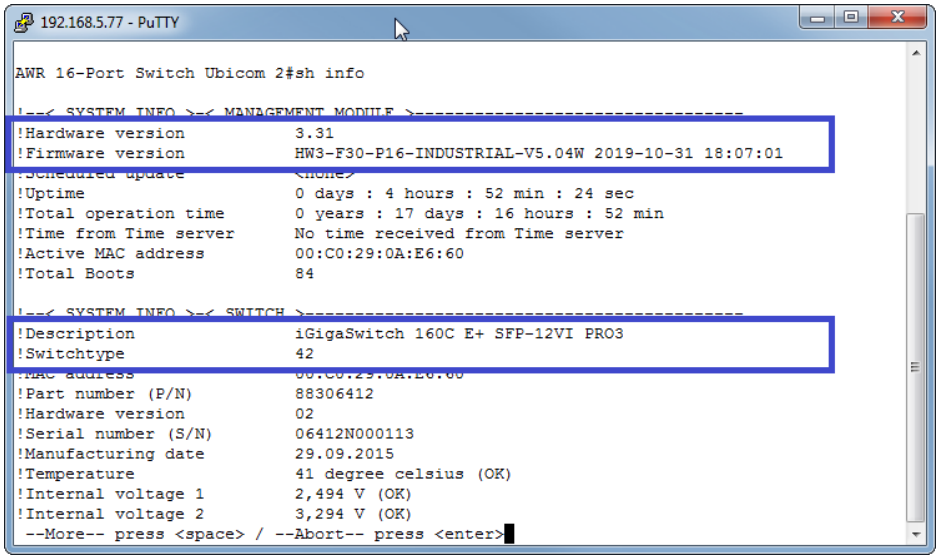
10.1.3. Query via CLI/SSH/V.24 Console

Command `show info`:

For HW5 switches in addition to parameter “Firmware Version” the parameter “Backup Firmware Version” for the backup firmare is also shown. In this case the string “Firmware version” is replaced by “Running firmware version”, and the corresponding boot partition (1 or 2) of both versions is displayed behind the version string in square brackets:



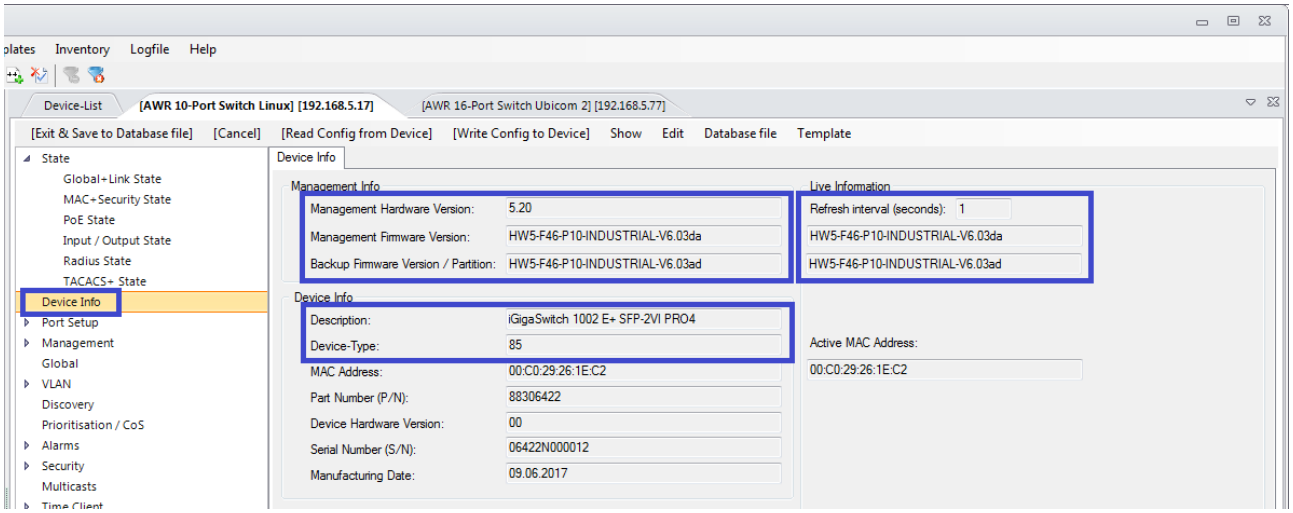
For HW3 switches and for firmware versions older than V6.01ef only the parameter “Firmware version” is shown beside the parameters “Switchtype” and “Hardware version”:



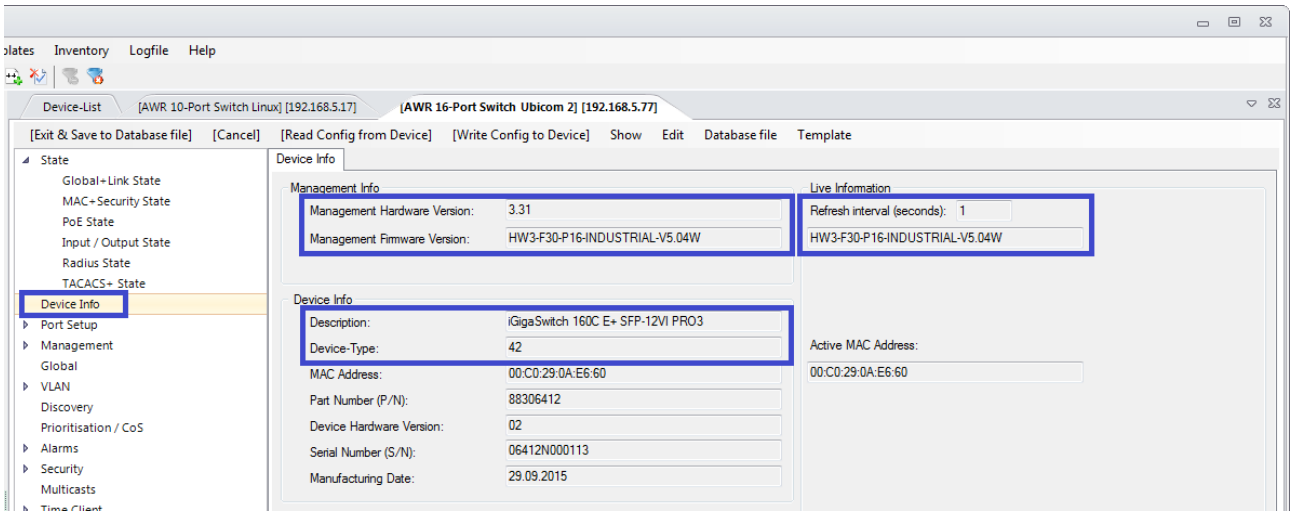
10.1.4. Query via NEXMAN

Tab <u>Device Info</u>:

For HW5 switches in addition to parameter “Management Firmware Version” the parameter “Backup Firmware Version” for the backup firmware is also shown as Management Info and as Live Information.



For firmare versions older than V6.01ef and for HW3 switches only the parameter “Management Firmware Version” is shown beside the parameters “Device-Type” and “Management Hardware Version”:



10.2. Determination of the active MAC Address

The MAC address via which the Management Agent is addressable in the network is called 'Active MAC Address'. For cable-duct and desk switches this is principally the MAC address printed onto the device label.

For industrial switches, however, this can also be the MAC address of an inserted memory card (see chapter *4. Memory Card (MC)*). Since the MAC address of the memory card is only taken over when booting the switch, the display of the active MAC address shows unambiguously the currently used MAC address.

NOTE: If the switch was booted with the fixed IP address, it will principally send and receive using the fixed MAC address 00:C0:29:01:FF:FF. However, the MAC address which would be active in the normal operating mode will be indicated as the active MAC address.

10.3. Switch Name / Location / Contact / Domain

In the switch the following information is permanently stored:

- Name
- Location
- Contact
- Domain

Name:
This is the central name of switch. It has the following additional functions:

- It is entered as 'hostname' with DHCP (details see *5.3. IP Address Configuration via DHCP*).
- It is displayed in the NEXMAN switch list and can be used as a sorting criterion.
- It is displayed in the Telnet and V.24 console prompt.

Location:
Here for example the installation location of the switch can be entered.

Contact:
For indicating a contact address and/or the phone number of the administrator in charge.

Domain:
For indicating a global domain name.

10.4. Banner

It is possible to define up to 12 lines with max. 80 chars. The banner will be shown before logging in the CLI or Web interface. The following characters are allowed:
a...z A...Z 0...9. , ; ! " # $ ^ ~ @ * : + - _ / \ | ( ) [ ] { }

10.5. Admin/User Accounts for Management Access

On principal there are two different access levels for Web, Telnet/SSH/V.24 console and NEXMAN available:
- Admin account: full read/write access to all settings
- User account: read-only access only

The factory default settings are:
- for Admin account: Name = admin Password = nexans
- for Admin-1…5: Deactivated
- for User account: Name = user Password = nexans

If a wrong login name or a wrong password is entered, an error message will be displayed for Telnet/SSH/V.24 console and NEXMAN, while for WEB the empty login window will be displayed again.

For the Admin-1 account, the following additional access rights can be configured:
- Read/Write for all parameters
- Read/Only for all parameters except Port-Monitor on WEB

Read/Write for all parameters:
The Admin-1 account has full read/write access rights.

Read/Only for all parameters except Port-Monitor on WEB:
The Admin-1 account has basically only read/only rights, with one exception:

The port monitor setting for "Mode" and "Source Port" can be configured via the WEB interface. The "destination port" cannot be changed and must therefore be pre-configured by an Admin account with full read/write access rights.

The following ASCII characters are allowed for Name/Password and are checked in WEB, CLI and Manager input masks:

a-z A-Z 0-9 . , ; ! " ' % # $ & ^ ~ @ * : + - = _ / \ | ( ) [ ] { } < >

The only exceptions are the following not supported ASCII characters:

? (ASCII 63) Can't be used because in CLI console “?” is always interpreted as help command

` (ASCII 96) User must press keys <shift + `> + <space> to enter this character, which is not practical

10.6. Password Encryption

The local passwords for the Admin and User accounts can be saved in two ways:
- Standard proprietary procedure

- DES DES Encryption
- MD5 Hash modified MD5 hash algorithm
- SHA1-Hash modified SHA1-Hash algorithm
- SHA256-Hash modified SHA256-Hash algorithm

Standard (factory default):
The local passwords are saved according to a proprietary encryption procedure in FLASH. For a hacker who knows the algorithm, it would be possible to recover the passwords.

DES:
This procedure converts the passwords into encrypted DES values. This setting is required, if the Manager Authentication Mode has been set to “Local via SNMPv3” and if simultaneously CLI configurations, which shall contain encrypted passwords, shall be loaded.

MD5 Hash:
SHA1-Hash:
SHA256-Hash:
In both procedure the password is converted into a irreversiblen hash value and is saved in flash:
MD5 is using the following formula:
`Hash = "!" + base64(md5(<Clear-text password>))`
SHA1 is using the following algorithm for salting:
`Hash = "&" + base64(sha1(<Clear-text password> xor 0x0102..)`
SHA256 is using the followingder algorithm:
`Hash = "#" + base64(sha256(<Clear-text password>)`

If this algorithm is applied, e. g. to the "nexans" factory default password, the following hash value results:
`!/Ri3qIUkshmf/Sn6UPkxfQ==`

It is the special property of a hash value that it is practically impossible to calculate the original password from thi Hash.. However, the precondition is that the password has a sufficient complexity and a minimum length of 8 chars. If we have higher requirements it is usefull to use at least 12 chars.

As soon as the Encryption Mode is changed from Standard to DES or MD5 Hash, SHA1 or SHA256-Hash, the passwords saved in the flash will automatically be converted into their hash values. If you only want to change one of these passwords, you enter the plain text password into the Manager, in WEB or into the CLI console and then the switch and/or Manager will convert this password into an MD5 or SHA1 hash.

If the "Password Encryption Mode" is changed from MD5-, SHA1- or SHA256-Hash to another „Password Encryption Mode“ all passwords willl be set to Facory-Default.

On the CLI console you can also enter directly the corresponding hash value instead of the plain text password. This is particularly useful, if you want to create CLI scripts which shall also contain the passwords. If the Encryption Mode is set to Standard and you configure one of the passwords as a hash value via the CLI Console, the Encryption Mode is automatically changed to MD5, SHA1 or DES Hash.

Via the "show config accounts all" or "show running-config all" Console commands or in the Manager on the "Manangement > Accounts" tab it is possible to read the hash or DES values in order to use them for a script, if necessary.

10.7. Passwort Strength Checker

By enabling the password strength checker only secure passwords for the admin and user account are accepted. Passwords that have the following criteria are classified as safe passwords:

8…14 characters with at least

1 lower letter: (a-z)
1 upper letter (A-Z)
1 digit: (0-9)
1 special character: (. , ; ! “ # $ ^ ~ @ * : + - _ / \ | ( ) [ ] { } < >)

In the field minimum password length there is the possibility to define a minimum password length for the secure passwords. The length can be from 8 to 14 chars. The requirements will not be changed.

To activate the password strength checker via the NEXMAN it is necessary to define a secure Admin and User password before writing the configuration to the device. If there is a unsecure password defined you will be asked to define a secure password.

If there is an unsecure password active while logging in via CLI or WEB you must set a new secure password before you can configure the switch. If you are logged in with the User Account you are only able to change define a secure password for the User Account. Also this is necessary after the login.

10.8. Configuration of IP and VLAN Parameters

Changes to the configuration of IP and VLAN parameters via Telnet/SSH/V.24 console, Web or SNMP do not take immediate effect, but only after execution of the command {Renew IP- and VLAN-Parameter}.

Thus, it is possible to enter all desired changes to the IP and VLAN settings first, before they are being activated. This prevents an incomplete configuration from bringing the switch into an undefined state.

For detailed information on setting the IP and VLAN parameters see chapters *5. IP Address Configuration* and *10.31 VLAN Support*.

10.9. ARP Table

The ARP table of the switch management can exclusively be displayed and/or deleted using the CLI. The corresponding command is:

```
sh:ow ar:p-table [d:elete]
```

10.10. Manager Authentication Mode

The following authentication modes can be set in the switch for NEXMAN access:

• SCP – Use SCP authentication mode setting:	Authentication via SCP
• UDP/TFTP – No authentication (Ignores Username and Password)	No authentication
• UDP/TFTP – Local Accounts	Local authentication
• UDP/TFTP – Radius Only	Authentication through the RADIUS server only
• UDP/TFTP – Radius first, then Local Accounts	Authentication through RADIUS. If no server response, local authentication.
• SNMPv3 – Local Accounts	Local authentication via SNMPv3
• Disable Manager access	Manager access via UDP, TFTP and SNMPv3 is completely disabled

SCP – Use SCP authentication mode setting:
The authentication mode that is defined as the SCP authentication mode at the console setup is used.

UDP/TFTP – No authentication (Ignores Username and Password):
With this setting the switch does not expect any authentication for access via NEXMAN. Moreover, in this mode direct access to the switch is possible via TFTP programme. Before putting the switch into operation, it is among others possible to perform a firmware update or downgrade without entering a password. owever, for security reasons a different mode should be enabled when the switch is later operated in the network. Upon access via NEXMAN an additional warning is displayed in the log window informing on the unsecure mode.
NOTE:
If {none} is selected, access through NEXMAN can only be restricted via the access list (see chapter *10.19. Access List / Access List Mode)*.

UDP/TFTP – Local Accounts:
A name and password each for Admin and User access is stored in the switch (see chapter *10.5. Admin/User Accounts for Management*). These data are used for authentication of NEXMAN access and compared with the entered login name and login password.

UDP/TFTP – Radius Only:
UDP/TFTP – Radius first, then Local Accounts:
These modes are only supported by firmware versions with RADIUS functionality. See chapter *10.57. RADIUS Manager Authentication Modes*

SNMPv3 – Local Accounts:
By using this mode the local defined passwords will be used for the authentication. The authentication and file transfer will only be done via SNMPv3.

Disable Manager access:
Manager access via UDP and TFTP is completely disabled. This setting can only be configured via the **'config manager-auth-mode disable'** CLI command.

10.11. HTTP Setup

Basic notes on configuring the unit via WEB browser can be found in Chapter *6.2. Switch Configuration via Web Browser (HTTP/HTPS)*.

10.11.1. HTTP Authentication Mode

The following modes can be selected for HTTP access:
- Local: Local authentication
- Read/Only: Local authentication, only Read/Only access permitted
- HTTP disabled: HTTP interface disabled

Local (factory default):
A name and password each for Admin and User access is stored in the switch (see chapter *10.5. Admin/User Accounts for Management*). These are the factory default data for authentication during HTTP login and are compared with the entered login name and login password.

Read/Only:
Here the local names and passwords are used, just as with the {local} setting. However, on principal only read-only access is permitted.
NOTE: Only read-only access is granted, also after login with the correct Admin name/password.

HTTP disabled:
The HTTP interface is disabled. The switch will reject any connection setup on the TCP port of the Web interface.

NOTE:
When the user enters the wrong name or password three times, all WEB interfaces (HTTP and HTTPS) will be locked for 60 seconds.

10.11.2. HTTP TCP Port

The TCP port for HTTP access can be configured in the range 1 ... 65535. By factory default, the port 80 is set.

10.12. HTTPS Setup

Basic notes on configuring the unit via WEB browser can be found in Chapter *6.2. Switch Configuration via Web Browser (HTTP/HTPS)*.

10.12.1. HTTPS Authentication Mode

The following modes can be selected for HTTPS access:

- Local: Local authentication
- Read/Only: Local authentication, only Read/Only access permitted
- HTTPS disabled: HTTPS interface disabled

Local (factory default):
A name and password each for Admin and User access is stored in the switch (see chapter *10.5. Admin/User Accounts for Management*). These are the factory default data for authentication during web login and are compared with the entered login name and login password.

Read/Only:
Here the local names and passwords are used, just as with the {local} setting. However, on principal only read-only access is permitted.
NOTE: Only read-only access is granted, also after login with the correct Admin name/password.

HTTPS disabled:
The HTTPS interface is disabled. The switch will reject any connection setup on the TCP port 443 of the HTTP interface.

NOTE:
When the user enters the wrong name or password three times, all WEB interfaces (HTTP and HTTPS) will be locked for 60 seconds.

10.12.2. HTTPS TCP Port

The TCP port for HTTPS access can be configured in the range 1 ... 65535. By factory default, the port 443 is set.

10.12.3. HTTPS Allowed TLS Versions

The minimum allowed TLS version for HTTPS access can be configured to ensure a desired security level. The requirement is that the used WEB Browser also supports the configured TLS version.

The following settings are available:

- Allow TLS 1.0 and higher
- Allow TLS 1.1 and higher
- Allow TLS 1.2 and higher

10.13. V.24 Console Interface

Configuration using the V.24 console interface is supported by industrial switches and desk switches of type 'GigaSwitch'.

For a detailed summary of valid console commands see Chapter *9. Summary of all State and Configuration Parameters*.

For a description of the configuration using the V.24 console see Chapter *6.3. Switch Configuration via V.24*

10.14. V.24 Console Authentication Mode

Six different authentication modes can be selected for the V.24 console:

- Local: Local authentication
- V.24 disabled: V.24 console interface disabled
- Radius only: Authentication through the RADIUS server only
- Radius first, then local: Authentication through RADIUS. If no server response, local authentication.
- TACACS+ only: Authentication through the TACACS+ server only
- TACACS+ first, then local: Authentication through TACACS+. If no server response, local authentication.

Local (factory default):
A name and password each for Admin and User access is stored in the switch (see chapter *10.5.*

Admin/User Accounts for Management). They are the factory default data for authentication during Telnet login and will be compared with the entered login name and login password.

V.24 disabled:
The V.24 console interface is disabled.

Radius Only:
Radius first, then local:
These modes are only supported by firmware versions with RADIUS functionality. See chapter *10.56. RADIUS Console Authentication Mode.*

TACACS+ Only:
TACACS+ first, then local:
These modes are only supported by firmware versions with TACACS+ functionality. See chapter *10.64 TACACS+ Console Authentication Modes.*

10.15. Console Password Mode

The Console Password Mode can be used to specify whether the Telnet und V.24 console password shall be displayed or not upon entry. This is quite useful, e.g. when one-time passwords are used with RADIUS servers and the entered password can only be used once.

The following settings are possible:
- Invisible (Default)
- Visible

10.16. Encrypt Password Mode

With the “show running-config” CLI command the SNMPv1/v2 communities, SNMP v3 passwords, RADIUS secrets and TACACS+ secrets can optionally be output in an encrypted form. The encrypted values can then be used as input values for configuring the corresponding parameters.

10.17. Console logout time

Sets the inactivity timeout for the command line interface usage.

10.18. Global Access / Access Policy

By enabling the access policy only secure protocols for the access via CLI, WEB, SNMP and Manager are allowed, and the Manager Authentication Mode is set to ‘SNMPv3’. At the same time the password strength checker is enabled and the password encryption mode is set to MD5, see Chapter 10.7 Passwort Strength .
Unsecure protocols are:
TELNET, HTTP, SNMPv1, SNMPv2 and SNMPv3 without SHA-Auth. , Encryption and manager access via UDP/TFTP.
Secure protocols are still available:
SSHv2, HTTPS, and SNMPv3 with SHA-Auth. and DES-Encryption.Manager access via SNMPv3 and SCP

On industrial switches this mode can be activated via DIP switch 3 (F1) at the backside or the frontside switch F1. If the DIP switch is set to on the access policy cannot be deactivated by management access.

10.19. Access List / Access List Mode

You can define in an **Access List** which IP addresses can access the management of the switch. A total of 16 IP ranges can be indicated and each entry can be assigned read/write or read/only rights. If a single IP address is to be entered instead of a range, the Stop IP Address field is left empty.

The firmware versions with SNMP support will additionally send an Authentication Failure Event which contains the invalid IP address, if an unauthorized access is detected. Moreover, the IP address is entered in the SNMP variable infoMgmtAuth and can be requested via SNMP.

Via the **Accesslist Mode** you can define the access type for the list.

The following settings are possible:

- Disabled
- Enabled for Manager access only
- Enabled for SNMP access only
- Enabled for all access:

Disabled:
The access list is ignored.

Enabled for Manager access only:
The access list is enabled for exclusive access via NEXMAN.
If the Manager Authentication Mode is set to {Local}, {Radius only} or {Radius first, then local}, both the login name/password must be correct, and the IP address of the management PC must be entered in the access list in order to allow access via NEXMAN.

Enabled for SNMP access only:
The access list is exclusively enabled for access via SNMP.
For SNMP access both the SNMP community must be correct, and the IP address of the management PC must be entered in the access list. Otherwise the SNMP agent will reply with an 'Authentication Failure'.

Enabled for all access:
This mode applies the access list to all access attempts (NEXMAN, SNMP, Telnet and Web):
NEXMAN: If the 'Manager Authentication Mode' is set to {Local}, {Radius-only} or {Radius-first, then local}, both the login name/password must be correct and the IP address of the management PC must be entered in the access list in order to allow access via NEXMAN.
SNMP: For SNMP access both the SNMP community must be correct and the IP address of the management PC must be entered in the access list. Otherwise the SNMP agent will respond with an Authentication Failure.
Telnet: For Telnet access both the login name/password must be correct, and the IP address of the management PC must be entered in the access list.
Web: For Web access both the login name/password must be correct, and the IP address of the management PC must be entered in the access list.

10.20. Link Setup

The following Link Setup parameters can be configured separately for each port:
- Link Type
- Admin State
- Speed/Duplex
- Autocross/Autopolarity

10.20.1. Link Type

The Link Type parameter defines the function of the connected link. The following settings are possible:
- Userport
- Userport with active Loop Protection
- Uplink / Downlink

Userport:
This setting should be selected, if a permanently installed terminal is connected to the respective port.

Userport with active Loop Protection:
This setting should be selected, if different terminals are connected to a switch and there is the risk of (inadvertently or maliciously) short-circuiting two ports so that a loop could occur in the network. Moreover, loops caused by downstream hubs or switches are detected.

On the relevant ports special loop protection packets are then periodically sent, and it is checked whether these packets are received on the same or a different port. If the loop protection packets are received via an Uplink port or User port with active Loop Protection, a loop is present, and the port is switched off. In addition, the Admin Status 'Disabled by Loop Detection' is displayed (for further information see chapter *10.20.2.Admin State*).

Switched-off ports can optionally be reactivated automatically after an adjustable "Re-Enable Time for Loop-Disabled Ports". The time can be configured in the range of 1 to 60 000 seconds.

IMPORTANT:

To reliably detect loops, the management VLAN must not be enabled on the corresponding ports.

NOTE:
This function will cause an additional quiet time of about 5 seconds after a Link-Up. During this time the switch is already sending Loop Protection packets, however, any other traffic will be blocked, to prevent a temporary loop in case of a short-circuit.

NOTE:
This function can only be activated if Spanning Tree Global is deactivated or Spanning Tree is deactivated for the respective port.

Uplink / Downlink:
All ports serving as an uplink to the central core switch or as a downlink to the subsequent switch should be set to this Link Type.
In this case the following characteristics apply to these ports:
a) The port cannot be disabled, neither manually nor automatically by management. If the port is already disabled, it will be automatically enabled again.
b) The Console command `sh:ow m:ac-address-table d:ynamic` will not display the addresses of these ports. If you want to display the addresses of these ports, too, the Console command must be extended by the `a:ll` option.
c) No Port Broadcast Failure events will be transmitted for these ports, since usually the broadcasts of almost all terminals are received on the uplink. This would lead to unnecessary and misleading events.

10.20.2. Admin State

Via Admin State the port can be completely disabled. If a security function is enabled for the respective port, the port can also be disabled via management.

The following table shows the possible statuses:

Admin State	
Designation	**Function**
Enabled	The port is enabled and transmits a link signal.
Disabled	The port was manually disabled by the administrator and does not send a link signal.
Disabled by Security Violation	The port was automatically disabled via the activated Portsecurity function. An additional Portsecurity-Failure event is sent, if the port was automatically disabled.
Disabled by Loop Detection	The port was automatically disabled, because the activated Active Loop Protection has detected a loop. An additional Port-Loop-Detected event is sent, if the port was automatically disabled.
Disabled by BPDU Detection	The port was automatically disabled, because for the respective port the “Disabled (BPDU disables Port)” Spanning Tree mode is configured and a Spanning Tree BPDU was received on this port. In case of an automatic disablement in addition a “Port-Error-Disabled” event is sent.
Disabled by Ring Loop Protection	The port was automatically disabled, because for the respective port the “Enabled (Ring Loop Protection)” Spanning Tree mode is configured, and a loop was detected in the ring. In case of an automatic disablement in addition a “Port-Error-Disabled” event is sent.
Disabled by DHCP Snooping	The port was automatically disabled, because DHCP Snooping is enabled and for the respective port the “Userport” or “Userport with Active Loop Protection” link type is configured and a DHCP packet was received from a DHCP server on this port. In case of an automatic disablement in addition a “Port-Error-Disabled” event is sent.

10.20.3. Shutdown Port if no Link

This command allows you to automatically disable the port in case of a missing link signal. If no link is available at the moment of testing, the respective port will be permanently disabled. This is done by switching the Admin State to “Disabled”. This setting will be kept also after rebooting the switch.

The following settings are possible:
- Disabled
- Check Link one time
- Check Link permanently
- Check Link permanently delayed

Disabled:
The port will not be automatically disabled.

Check Link one time:
The link is checked only once, i. e. immediately after setting this value. Afterwards the setting is switched back to “Disabled” again.
This command makes particular sense for CLI scripts or master configurations, in order not to disable all connected ports for security reasons.

Check Link permanently:
Here the link is permanently monitored and the port disabled within a few milliseconds after detecting a missing link signal. If a disabled port is switched on again using the Management feature, unless a link is established within a period of 5 seconds the port will be set to “Disabled” again. With this setting the port will be disabled after a reboot (also, if the link was established before rebooting).

Check Link permanently delayed:

Here the link is permanently monitored and the port disabled within a few milliseconds after detecting a missing link signal. Alternatively the disablement can be delayed by activating the “Client Remove Alarm” for the respective port. In this case the desired disablement delay is set via the “Link Down Timeout” item. If the “Client Remove Alarm” is enabled when the disablement occurs, in addition a “Client Remove Alarm” is sent.
If a disabled port is switched on again using the Management feature, within 5 seconds a link signal must be received, or the port will be disabled again.
Furthermore, after a reboot the link signal will be checked with 30 second delay. Among others this feature will prevent the port from being disabled after a firmware update.

10.20.4. Speed/Duplex

The Speed/Duplex setting defines the acceptable data rate and the duplex mode of the respective port.
The following table indicates the supported modes:

Speed/Duplex	
Designation	**Function**
Autoneg	Auto-negotiation: automatic detection of data rate and duplex mode.
ECO 10/100	Autonegotiation, but no 1 Gbps links will be allowed. This setting is exclusively supported by gigabit ports to reduce power consumption. This makes sense, e. g. for terminal units which support a gigabit link, but for which a data rate of 100 Mbps is sufficient. Ports which are operated unnecessarily on a 1 Gbps link will need an additional power of about 0.5 Watt at the switch and at the terminal unit. This mode can be enabled/disabled time-controlled, to reduce power consumption during the night or at weekends (see Chapter *10.14.4. Automatic Powersave).* Additionally, all ports with a 1 Gbps link can automatically be switched into this ECO mode in case of excess temperature (see Chapter *10.29.2. Temperature Powersave Function).* NOTE: This mode is supported by certain switch types only.
ECO 10/100 (Powersave)	Same function as 'ECO 10/100', but the ECO mode was automatically disabled, because an automatic Powersave function is enabled for this port. For detailed information see Chapter *10.20.5. Automatic Powersave.*

ECO 10/100 (Overtemp.)	Same function as 'ECO 10/100', but the ECO mode was automatically disabled, because the temperature of the switch has exceeded the set upper limit. For detailed information see Chapter *10.29.2. Temperature Powersave Function.*
1000 FDX	Fixed setting: 1 Gbps - full duplex In spite of the fixed setting, the Autonegotiation function for speed and flow-control will always be executed.
1000 FDX (Autoneg. disabled)	Fixed setting: 1 Gbps - full duplex This mode is required, if the Fiber Uplink is connected to an older unit (e. g. Fiber Converter). In this case the Autonegotiation functions for speed and flow control are disabled, because Autonegotiation might not be supported by legacy units.
100 FDX	Fixed setting: 100 Mbps - full duplex
100 HDX	Fixed setting: 100 Mbps - half duplex
10 FDX	Fixed setting: 10 Mbps - full duplex
10 HDX	Fixed setting: 10 Mbps - half duplex

IMPORTANT:
Please observe the basic principle that both the switch port and the remote side (terminal or core switch) should have identical settings, e.g. both set to {Autoneg} or both set to {100FDX}.

NOTE:
The supported settings depend on the port type. Example: Fiber-optic ports never support auto-negotiation.

10.20.5. Automatic Powersave

This function allows you to automatically reduce the power consumption of the port.

The following setting is available:
- Set Speed/Duplex to 'ECO 10/100' by Time Client
- Set PoE Setup to 'Off' by Time Client
- Set Speed/Duplex to 'ECO 10/100' by Time Client: Twisted pair ports supporting the 'ECO 10/100' Speed/Duplex mode can be switched time-controlled into this mode. This requires the port to be set to 'Autoneg' and the Time Client to receive a valid time from the Time Server.

Set PoE Setup to 'Off' by Time Client:
For ports witch support PoE (Power over Ethernet) the PoE voltage can be shut down time controlled. This will only take affect if the port is not set to 'Off' and the time client receives a valid time from the time server.

Time is controlled globally for all ports set accordingly. The times for each day of the week can be set separately via the Powersave setup of the Time Client.

The following parameters can be configured:
- Start time hour
- End time hour

Start time hour:
This is the time (in full hours) at which all twisted pair ports set to the ‘Autoneg’ Speed/Duplex Mode will automatically be set to the 'ECO 10/100 (Powersave)' Speed/Duplex Mode.

End time hour:
This is the time (in full hours) at which all twisted pair ports set to the ‘ECO 10/100 (Powersave)’ Speed/Duplex Mode will automatically be set to the 'Autoneg' Speed/Duplex Mode.

IMPORTANT:
If the time value is set to ‘0’, the time will be ignored. If you want to enable the Powersave feature, e. g. for the weekend, you only need to set the 'Start Time' for Friday (e. g. 18 hours) and the 'End Time' (e. g. 8 hours) for Monday. For Saturday and Sunday all times can be left set to ‘0’.

10.20.6. Energy-Efficient Ethernet (EEE)

For HW5 switches the Powersave function Energy-Efficient Ethernet (EEE) can be separately enabled for every port.

This feature enables EEE for the respective port. In the case of ports with Gigabit Link, the data rate is reduced to 100 MegaBits / s if this is sufficient for the operation of the connected end device (see chapter *10.20.4 Speed/Duplex*).

NOTE:
For HW3 switches EEE is enabled by default and cannot explicitely be set up.

10.20.7. Extended Powersave

For certain HW5 switches the Powersave function Extended Powersave can be separately enabled for every port.

If this feature is activated, in addition to the standard EEE, the Extended Powersave mode for the port is turned on. The power consumption of the port is reduced if there is no link for a longer time. It is then checked at regular intervals whether the power must be booted up again and the link needs to be recovered.

10.20.8. Autocrossover/Autopolarity

This setting defines whether an automatic crossover of the TX and RX pairs is to be performed (Autocrossover) for the respective port.

If a 10 Mbps terminal is connected to the port, additionally an automatic crossover of the RX+/RX- pair is performed (Autopolarity).

IMPORTANT NOTE:
The Autocrossover function should only be enabled, if at the same time Speed/Duplex is set to 'Autoneg.' or 'ECO 10/100'. According to IEEE802, no correct link detection is guaranteed with fixed Speed/Duplex settings.

10.20.9. Client Remove Alarm

This function detects, if a terminal unit has been permanently removed from the port. If the link of the monitored port is ‘Down’ for a configurable period of time (0…60000 seconds), a ‘Client Remover Alarm’ will be triggered which can be sent via the Alarm Destination Table and will be shown in the “Global+Link State” for the NEXMAN. This also applies for ports that never had a link.

If the Link Down time is set to ‘0’, an alarm will be sent immediately after a Link Down.

10.21. Link / EEE State

The Link State shows the current data rate, the current duplex mode and the Energy-Efficient Ethernet (EEE) state of the respective port.

The following table indicates the supported values:

Link State	
Designation	**Function**
No Link	No valid link signal was detected on the port.
Admin-Disabled	The port has been disabled by administrator
Security-Disabled	The port has been disabled automatically due to a portsecurity failure (see chapter *10.36.1. Portsecurity Failure Action)*
Loop-Disabled	The port has been disabled automatically by the 'Active Loop Protection'
CLIENT-REMOVE-ALARM	The port was automatically disabled by the Client Remove Alarm.
1000 FDX	1 Gbps - full duplex
1000 FDX / EEE	1 GigaBit/s - Full-Duplex and "Energy-Efficient Ethernet (EEE)" aktiveted mode This mode will only be activated if the switch and the end device that is connected to the switch support EEE. Note: In the Device Editor of the Manager the EEE state is shown in a separate column at the tab "Global+Link State".
100 FDX	100 Mbps - full duplex
100 HDX	100 Mbps - half duplex
10 FDX	10 Mbps - full duplex
10 HDX	10 Mbps - half duplex

NOTE:
If Speed/Duplex is set to 'Autoneg' and 'ECO 10/100' the data rate and the duplex mode, which the switch and the connected device have agreed on, are displayed.
In case of a fixed Link Setup (e.g. 100 FDX), on principle, the data rate and the duplex mode as specified in Speed/Duplex are indicated (if a valid link signal is available).

10.22. Send Link Alarms

This option is enabled by default and ensures that the ‘Link Up’, ‘Link Down’ and ‘Link Change’ alarm types will be sent for the port concerned, provided they have also been enabled in the Alarm Destination Table.

If this option is disabled, no link alarms will be sent for the port concerned, not even, if these have been enabled in the Alarm Destination Table.

10.23. Cable Diagnostic for Twisted-Pair Ports

The cable diagnostic function allows you to perform an active verification of Twisted-Pair ports for the connected Twisted-Pair cable. Even if no link signal is detected on the port, you can find out whether a cable is connected at all and whether the end of the cable is open or short-circuited. The diagnosis can be initiated optionally for all ports or for one single port.

After starting the diagnosis each wire pair is individually measured (with 100Mbit/s: two wire pairs), and the result is indicated with the status 'open' (open end) or 'short' (short-circuited end) and the respective distance displayed. If the remote side is correctly connected, including correct impedance matching, the status of 'Good termination' will be displayed. However, in this case it will not be possible to determine the line length. For that reason 'n/a' (Not available) is indicated here.

CAUTION! Starting the cable diagnostic procedure for a port with an active link signal will result in an interruption of the link for about five seconds.

NOTE: This feature is supported by selected switch types and firmware versions only.

10.24. Remote Fault

This function is supported for fiber-optical ports only.
With the Remote Fault function enabled the optical transmitter of the respective port will only be switched on, if an optical input signal is received.
This makes sense especially for central switches and media converters with management functions. If there is an error on a link at a particular location, this failure is passed on to the central switch or FiberCon and can then be displayed there in the management as a link failure.
For detailed information please read the manual of the respective switch.

NOTE:
In order to ensure correct function any vendor-specific link monitoring feature of the central switch (e.g. UDLP) must be disabled.

10.25. SFP Info, Diagnostic and Alarms

SFP (Small Form Factor Pluggable) is a specification of a generation of optical or electrical modular transceivers. SFP modules fit into a special SFP slot and are thus simply and quickly swappable ("hot-swap"). Switches equipped with SFP slots can thus easily be converted to other media and ensure a quick repair in case of defect.

SFP modules always contain a manufacturer-programmed memory which contains information on the manufacturer, type, etc. Special SFPs additionally offer a diagnostic function via which temperature, voltage, optical power levels and laser currents can be verified. Nexans’ current switch types support the display of this information and diagnostic data. Moreover, it is possible to configure alarm limits for the optical power levels and the laser current. If a limit is violated, an "SFP Event" is sent via SNMP trap or SYSLOG.

The following SFP information is displayed:
- Vendor Name
- Revision Number

- Serial Number
- Date Code
- Bit Rate
- Wavelengt (nm)
- Length 9µm (km)
- Length 50µm (m)
- Length 62.5µm (m)
- Connector Description

The following SFP diagnostic is displayed:

- Temperature (°C)
- Power Supply Voltage (V)
- Transmitter Laser Bias Current (mA)
- Transmitter Output Power (uW)
- Transmitter Output Power (dBm)
- Received Input Power (uW)
- Received Input Power (dBm)

The following alarms can be configured:

- Transmitter Laser Bias Current, Upper Limit
- Transmitter Output Power, Lower Limit
- Received Input Power, Lower Limit

The metrics of the most popular SFPs are listed in the below table. The alarm values indicated in brackets are the recommended lower limits for the “SFP Alarms” configuration. Typically, for RX Power a 3dB margin and for TX Power a 0dB margin should be observed.
IMPORTANT:
Depending on manufacturer and SFP type, the actual minimum and maximum values for RX/TX Power can deviate from the values indicated below and thus should be taken from the respective SFP datasheets. Mostly the datasheets don’t indicate any specific values for Bias Current. Consequently the Alarm Limit for the Bias Current will have to be individually configured for each SFP depending on the actual value shown under “Show SFP Info”.

Nexans Part-Nr.	Fiber type	Wave length TX/RX	Coverage	Rx Power Min…Max [SFP Alarm Limit]	Tx Power Min…Max [SFP Alarm Limit]
Fast Ethernet SFPs Dual Fiber					
88646010	MM(GI)	TX: 1310 nm RX: 1310 nm	2 km	-31 dBm…-14 dBm [-28 dBm / 2 uW]	-19 dBm…-14 dBm [-19 dBm / 13 uW]
88646011	SM	TX: 1310 nm RX: 1310 nm	10 km	-31 dBm…-5 dBm [-28 dBm / 2 uW]	-15 dBm…-8 dBm [-15 dBm / 32 uW]
88646012	SM	TX: 1310 nm RX: 1310 nm	40 km	-35 dBm…-3 dBm [-32 dBm / 1 uW]	-5 dBm…0 dBm [-5 dBm / 316 uW]
88646013	SM	TX: 1550 nm RX: 1550 nm	80 km	-35 dBm…-3 dBm [-32 dBm / 1 uW]	-5 dBm…0 dBm [-5 dBm / 316 uW]
Gigabit Ethernet SFPs Dual Fiber					
88646015	MM(GI)	TX: 850 nm RX: 850 nm	550 m	-18 dBm…0 dBm [-15 dBm / 32 uW]	-9 dBm…-4 dBm [-9 dBm / 126 uW]
88646016	SM	TX: 1310 nm RX: 1310 nm	10 km	-21 dBm…-3 dBm [-18 dBm / 16 uW]	-9 dBm…-3 dBm [-9 dBm / 126 uW]
88646017	SM	TX: 1310 nm RX: 1310 nm	40 km	-23 dBm…-3 dBm [-20 dBm / 10 uW]	-4 dBm…0 dBm [-4 dBm / 398 uW]
88646018	SM	TX: 1550 nm RX: 1550 nm	80 km	-24 dBm…-3 dBm [-21 dBm / 8 uW]	0 dBm…4 dBm [0 dBm / 1000 uW]

Nexans Artikel-Nr.	Stecker-typ	Wellelänge TX/RX	Reichweite	Rx Power Min…Max [SFP Alarm Limit]	Tx Power Min…Max [SFP Alarm Limit]
Fast Ethernet SFPs, Singlemode, Single Fiber					
88645914	LC-SX	Tx: 1310 nm Rx: 1550 nm	10 km	-31 dBm…-8 dBm [-28 dBm / 2 uW]	-17 dBm…-5 dBm [-17 dBm / 20 uW]
88646113	LC-SX	Tx: 1310 nm Rx: 1550 nm	40 km	-35 dBm…-3 dBm [-32 dBm / 1 uW]	-5 dBm…0 dBm [-5 dBm / 316 uW]
88646115	LC-SX	Tx: 1550 nm Rx: 1310 nm	40 km	-35 dBm…-3 dBm [-32 dBm / 1 uW]	-5 dBm…0 dBm [-5 dBm / 316 uW]
88645915	SC-SX	Tx: 1310 nm Rx: 1550 nm	40 km	-35 dBm…-3 dBm [-32 dBm / 1 uW]	-5 dBm…0 dBm [-5 dBm / 316 uW]
88645916	SC-SX	Tx: 1550 nm Rx: 1310 nm	40 km	-35 dBm…-3 dBm [-32 dBm / 1 uW]	-5 dBm…0 dBm [-5 dBm / 316 uW]
Gigabit Ethernet SFPs, Singlemode, Single Fiber					
88646073	LC-SX	Tx: 1310 nm Rx: 1550 nm	10 km	-21 dBm…-3 dBm [-18 dBm / 16 uW]	-9 dBm…-3 dBm [-9 dBm / 126 uW]
88646075	LC-SX	Tx: 1550 nm Rx: 1310 nm	10 km	-21 dBm…-3 dBm [-18 dBm / 16 uW]	-9 dBm…-3 dBm [-9 dBm / 126 uW]
88646022	LC-SX	Tx: 1310 nm Rx: 1550 nm	40 km	-23 dBm…-3 dBm [-20 dBm / 10 uW]	-4 dBm…0 dBm [-4 dBm / 398 uW]
88646023	LC-SX	Tx: 1550 nm Rx: 1310 nm	40 km	-23 dBm…-3 dBm [-20 dBm / 10 uW]	-4 dBm…0 dBm [-4 dBm / 398 uW]

10.26. Error Counter

For each port an error counter is displayed indicating the sum of the following individual counters:
- Rx FCS/CRC Error Packets
- Rx Alignment Error Packets
- Tx Late Collisions

The main purpose of the Error Counter is to detect incorrect FDX/HDX settings between switch and terminal unit. In case of an incorrect setting at least one of the individual counters will increment and thus increment also the Error Counter.

The most frequent causes for incorrect settings are:
- The switch port is set to {Autoneg} and the terminal is set to {100FDX}.
- The switch port is set to {100FDX} and the terminal is set to {Autoneg}.

IMPORTANT:
Please observe the basic principle that both the switch port and the remote side (terminal or core switch) should have identical settings, e.g. both set to {Autoneg} or both set to {100FDX}.

IMPORTANT: Error packets, mostly caused by switching on/off terminal units, will be suppressed. Additionally, the Error Counter is incremented by 1 only if FCS Errors or Late Collisions have occurred within a 2-second-intervall. This prevents the actual number of FCS or Late-Collisions from displaying, which could reach very high values, even if the error state was present for a short time only. With the time-interval procedure it is now possible to exactly see in how many (2-second) time intervals errors have been counted. Thus, it is easier to detect the duration of the failure.

10.27. Reset all Port Counters

The {Reset all Counters} command resets the following counters back to 0:
- Error Counter (see *10.26. Error Counter)*
- Statistic Counter (see *10.52. Statistic / RMON Counters)*

10.28. Switch Times

10.28.1. System Uptime

The 'System Uptime' shows the operating period of the switch since the last reboot. This can be both a software reboot (e. g. by firmware update) and hardware reboot (e. g. by switching on the operating voltage).

10.28.2. Time Since Last Link Change

Here the time per port is indicated which is elapsed since the last link change (Link-Up or Link-Down) of the respective port.

10.28.3. Network Time Protocol - SNTP

The Simple Network Time Protocol (SNTP) is a simplified version of the NTP. It is described in RFC 4330. If an appropriate time server can be reached in the local network, the current time of day can be taken over into the switch by activating the SNTP clients in the switch.

This time of day is used e.g. to provide Syslog events with a current time stamp.

The following table shows a summary of all SNTP client settings:

Designation in NEXMAN	Default Value	Function
Client enable	disabled	If selected, the SNTP client will be activated in the switch.
Time Server IP 1	<none>	The IP address of the first time server.
Time Server IP 2	<none>	The IP address of the second time server. If both server IPs are configured, then both servers are requested synchronously and the first valid response is used to update the system time.
Server Request Interval (seconds)	3600	The time interval for the periodic retrieval of the current time.
SNTP Protocol Version	3	The SNTP protocol version with which the requests to the server are executed.
Accept SNTP Broadcasts	disabled	If selected, also SNTP broadcasts, which do not come from the time server configured above, are accepted.
UTC Local Offset (minutes)	60	The time difference between local time and Coordinated Universal Time (UTC). The switch will not switch automatically between summer and winter time.
Summer time correction	Disabled	Defines whether an automatic summer time correction shall be made. • Disabled No correction is made. • European summer time A correction is made, which is applicable to most European states. Here the summer time counts from the last Sunday in the month of March to the last Sunday of the month of October, each from 2 o'clock a.m. Central European Time (CET).

10.29. Switch Temperature

The temperature of the switch is indicated in degrees Celsius.

10.29.1. Temperature Alarm Limits

The limits for allowed temperature can be configured via switch management:

- Low Alarm Limit (-20…+20 °C) [Default = 0 °C]
This is the lower limit. If the temperature falls below this value an alarm will be triggered.

- High Alarm Limit (-30…+100 °C) [Default = 70 °C]
This is the upper limit. If the temperature exceeds this value an alarm will be triggered.

For firmware versions with SNMP support a Temperature Failure event is sent periodically, if the limits are exceeded.

10.29.2. Temperature Powersave Function

The 'Overtemperature Powersave Action' feature allows you to configure an action which is to be triggered when the 'High Alarm Limit' temperature is exceeded.

The following function is available:

- Set Speed/Duplex of ports with 'Autoneg.' or '1000FDX' to 'ECO 10/100'

Ports supporting the 'ECO 10/100' Speed/Duplex Mode will automatically be switched into this ECO mode, in order to reduce power consumption. Each port not operated at 1 Gbps reduces power consumption by about 0.5 Watt in the switch and the terminal unit. As a precondition the port at the switch must be set to 'Autoneg' or '1000 FDX'.

IMPORTANT: For ports switched into the ECO mode due to over-temperature, the 'ECO 10/100 (Overtemp.)' setting is displayed during Speed/Duplex Setup. After checking the cause of the excess temperature, the Speed/Duplex Setup must be reset manually to the desired setting.

10.30. Switch Operating Voltages

The following internal operating voltages are displayed with a resolution of 0.05V:
- 2.5V operating voltage
- 3.3V operating voltage

If the two internal supply voltages are below or above the accepted threshold values (< 2,35 / > 2,65 V or < 3,15 / > 3,45 V), a "Internal Voltage Alarm” and an IEC61850 "Power Supply Alarm” will be triggered.

For industrial switches the following external operating voltages with 1V resolution are also displayed:
- Power Input S1
- Power Input S2

If one of the two voltages is below or above the accepted threshold values (< 18 / > 60 V), an IEC61850 "Power Supply Alarm” will be triggered, too. Moreover, if one of the two external voltages fails, an alarm can also be triggered via the alarm outputs M1 or M2.

All internal and external supply voltages can be read via the SNMP Private MIB.

10.31. VLAN Support

The Nexans switch offers full VLAN support, including trunking according to IEEE802.1Q, and is compatible to all commercially available switches from other vendors.

The following global configuration settings are possible for the switch:
- VLAN Table
- VLAN Mode
- Tagging Ethertype

The following settings are available for each port:
- Default-VLAN-ID
- Voice-VLAN-ID
- Trunking Mode

The following state information are displayed for each port:
- Active Default-VLAN-ID
- Active Voice-VLAN-ID
- Active Trunking Mode

The above parameters are fully explained in the following chapters**.**

10.31.1. VLAN Table

All VLAN IDs to be forwarded by the switch must be entered into the VLAN table. Up to 256 different VLAN IDs in the range from 1 … 4095 can be configured. IDs not entered into the table will be discarded by the switch.
The following VLAN IDs are automatically entered into the table and cannot be deleted:
- Default-VLAN-ID of the individual ports
- Voice-VLAN-ID of the individual ports
- RADIUS-Unsecure-VLAN-ID
- RADIUS-Guest-VLAN-ID
- RADIUS-Inaccessible-VLAN-ID
- IEEE802.1X-Authentication-Failure-VLAN-ID

The manual entry of additional VLAN IDs is required only, if two or more ports have been switched to trunking. In this case the switch must be informed via the VLAN table which VLAN IDs are allowed to be forwarded between the trunked ports.

IMPORTANT:
Switches from other vendors often have a predefined Default-VLAN which cannot be deleted. Although in the Nexans switch the VLAN-ID 1 is entered as factory default value, this Factory Default-VLAN is no fixed VLAN. You could, for example, after switching all ports to a different Default-VLAN ID delete VLAN ID 1 from the VLAN Table.

10.31.2. VLAN Mode

Chapter *10.31.1.VLAN Table* explains how to enter the VLAN IDs into the table.

However, the procedure of how to delete existing entries is determined by the VLAN Mode.
The following configuration settings are possible:
- Static - 802.1Q based (16 VLANs)
- Static - 802.1Q based (64 VLANs)
- Static - 802.1Q based (256 VLANs) (Supports Hybrid Trunking Mode)
- Dynamic - 802.1Q based (16 VLANs)
- Static - Port based (16 VLANs)

IMPORTANT:
When changing the VLAN Table Mode the complete VLAN Table will be deleted. Only those VLANs, which are automatically entered, will be preserved.

Static - 802.1Q based (16 VLANs):
The static setting principally requires that IDs in the VLAN table are deleted manually or overwritten via NEXMAN. This setting makes sense, when the configuration of the VLAN IDs is predefined and usually not changed while in operation.
If the table is full and you try e.g. to set the Default-VLAN ID of a port to an unknown VLAN ID, this new VLAN ID will be rejected. In order to be able to set the new ID nevertheless, an unused ID needs to be manually deleted from the VLAN table first.

Static - 802.1Q based (64 VLANs):
This mode is identical with the above ‘Static - 802.1Q based (16 VLANs)’ mode, but here up to 64 VLANs are supported.
Static - 802.1Q based (256 VLANs) (Supports Hybrid Trunking Mode):
This mode is identical with the above ‘Static - 802.1Q based (64 VLANs)’ mode, but here up to 256 VLANs are supported.
In addition, the so-called "hybrid" port trunking mode is supported, which can be configured separately for each port (see chapter *10.31.7. Port Trunking Mode*).

Dynamic - 802.1Q based (16 VLANs):
All VLAN IDs, which are not used as Port Default-VLAN-ID, Port Voice-VLAN-ID, RADIUS-Unsecure-VLAN-

ID, RADIUS-Guest-VLAN-ID, RADIUS-Inaccessible-VLAN-ID or IEEE802.1X-Authentication-Failure-VLAN-ID are automatically removed from the VLAN table. This makes sense, e.g. when the VLAN IDs of the ports are to be set dynamically via RADIUS and you want to prevent an overflow of the VLAN table.
IMPORTANT: The Dynamic Mode automatically detects new VLANs, independent of whether these have been configured per RADIUS or manually per CLI, SNMP, WEB or Manager. Also general VLANs, such as the Management VLAN or the Unsecure VLAN, are automatically added to or deleted from the VLAN table. This function should only be used, if just one port (e.g. the uplink) is set to trunking.
Furthermore, if Spanning Tree is activated globally, VLAN 1 is never deleted from the VLAN table. This is necessary because VLAN 1 is required for eventually connected PVST (Per-VLAN Spanning Tree) devices.

Static - Port based (16 VLANs):
This mode has been primarily designed for provider applications. All ports set to the same Default VLAN-ID are transparently connected with one another. All packets (including a possibly present 802.1Q VLAN tag) will be transmitted without any change between these connected ports. Received packets without VLAN tag will be output to the other connected ports also without VLAN tag.
However, if received untagged packets shall be output with an 802.1Q tag, the Trunking Mode needs to be set to ‘802.1Q Tagging (Tag Default VLAN)’ for this port. In this case the Default VLAN-ID set on this trunk port is inserted in the untagged packet as an 802.1Q VLAN tag. This function is quite useful, e. g. if the management port, which is untagged by default, shall be transmitted on a trunk port with VLAN tag. In the opposite direction for all packets received on the trunk port and then forwarded on the management port a possibly included VLAN tag is removed again.

10.31.3. Fabric Attach

Fabric Attach is a technology extension of Shortest Path Bridging (SPB) that allows the integration of non-SPB enabled devices and switches into SPB networks. To do this, an SPBM I-SID must be configured for each VLAN ID defined in the VLAN table. If a core switch supporting Fabric Attach is connected to the uplink port, the configured I-SIDs will be sent to it via LLDP. To authenticate against the core switch, an optional "Fabric Attach Authentication Key" can be configured. If this key is left blank, the key 'nexans' is used by factory default.

10.31.4. Global VLAN Port Isolation

When VLAN Port Isolation is enabled, all or selected User ports and the Management port are principally isolated from each other and cannot transfer data. This applies in particular, if the ports are assigned to the same VLAN. In this case, the ports can exchange data via the Uplink/Downlink port only.

The ‘Link type' configuration setting allows you to define which ports are User ports or Uplink/Downlink ports. By factory default the fiber ports and SFP ports are configured as Uplink/Downlink ports and all other ports as User ports.

This function makes sense if VLAN assignment of the connected device is done by a core switch by MAC or IP Address. It is often used with the Multi-User-Authentication according to IEEE802.1X and/or MAC-based by the Core-Switch.

The following settings are possible:

- Disabled
- Isolate all User ports and Management port
- Isolate selected User ports and Management port

Disabled:
VLAN Port Isolation is globally disabled.

Isolate all User ports and Management port:
All User ports and the Management port are globally isolated from each other.

Isolate selected User ports and Management port:
Only selected User ports and the Management port are isolated from each other. To configure which User port and if the Management port shall be isolated, the Per-Port VLAN Port Isolation must be enabled for the respective port, see chapter *10.31.5 Per-Port VLAN Port Isolation*.

10.31.5. Per-Port VLAN Port Isolation

If Global VLAN Port Isolation is set to ‘Isolate selected User ports and Management port’, VLAN Port Isolation can be enabled separately for each User port and the Management port.

NOTE:
If Global VLAN Port Isolation is disabled, then this feature is disabled for all individual ports.

10.31.6. Tagging Ethertype (Q-in-Q)

The Tagging Ethertype defines which value shall be inserted as Ethertype in tagged packets. According to the IEEE802.1Q standard this value is '8100'. However, some manufacturers of core switches also support other values, in order to tunnel IEEE801.Q VLANs, etc. This is of particular interest for service providers.

The following settings are possible:
- 8100 (IEEE802.1Q)
- 9100(Q-in-Q)
- 9200(Q-in-Q)

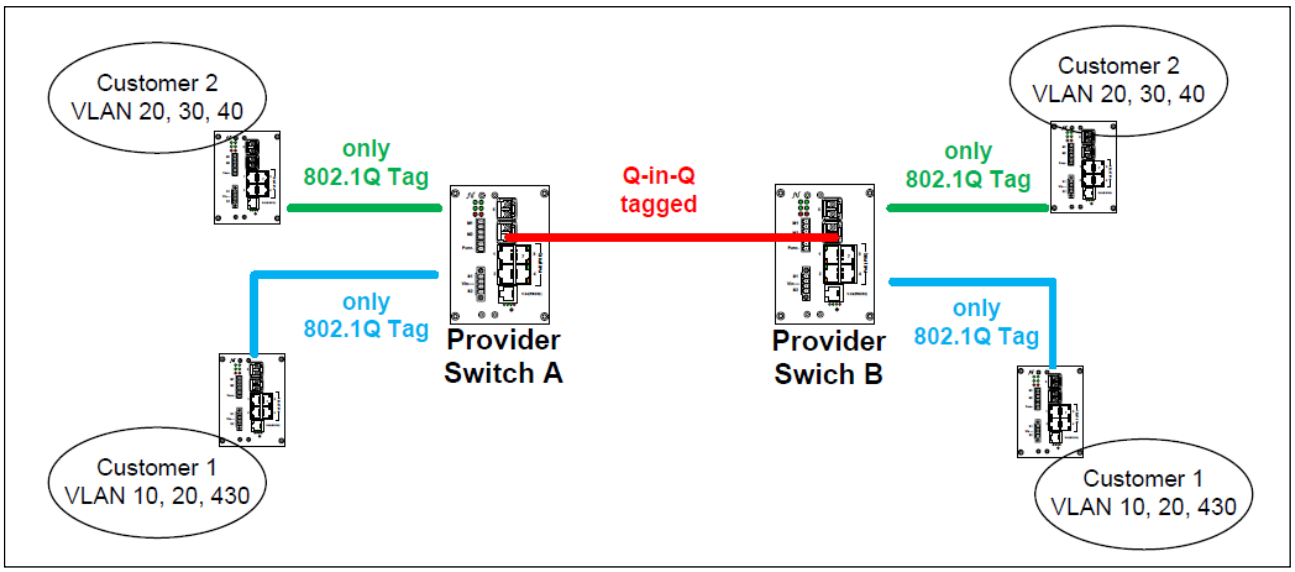
IMPORTANT:
The (Q-in-Q) configuration '9100 (Q-in-Q)' and '9200 (Q-in-Q)' should only be set, if the core switch is configured accordingly. Moreover, with these settings no Default-VLAN ID is supported for tagged ports, i.e., with tagged ports principally all VLANs will be tagged. In this case, a preset Default-VLAN ID, if any, will be ignored.

NOTE:
The Tagging Ethertype parameter can only be configured with some Nexans switch types. For all other switche types this value is fixed to 8100.

10.31.6.1. Q-in-Q with two Nexans Switches

Example A shows the setup with two Nexans switches used as provider switches. For this topology it is important that different default VLANs have been assigned to Customer 1 and Customer 2 at the provider switch. The respective assigned VLAN must be identical on both provider switches. For Q-in-Q to work properly, the tagging Ethertype must be changed, Trunking be enabled and the default VLAN between the two Nexans switches be set to “0”.

Example A



10.31.6.2. Q-in-Q with three Nexans Switches

Example B shows the setup with three Nexans switches used as provider switches. *10.31.6.1Q-in-Q with two Nexans Switches*

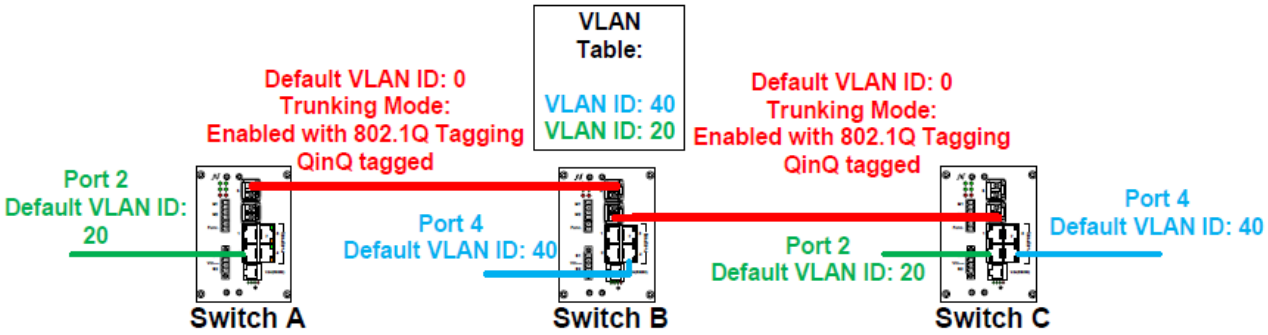
.The configuration of the customer ports and of the links between the Nexans switches is identical with the configuration used above in section *10.31.6.1 Q-in-Q with two Nexans Switches*

. Each customer must have its own default VLAN assigned. The links between the Nexans switches must have Trunking enabled and have the default VLAN “0”. For this constellation it is important that VLAN 20 is added to the VLAN Table of Switch B, allowing it to forward the data in VLAN 20. *10.31.1VLAN Table*

See also chapter *10.31.1. VLAN Table*

.

Example B)



Wichtiger Hinweis:
The forwarding of Q in Q Frames as described in chapter *10.31.6.2 Q-in-Q with three Nexans Switches* is only supported by the following switch types
- iGigaSwitch 542
- iSwitch G 1043E+
- iGigaSwitch 1604
- iGigaSwitch 1608
- iGigaSwitch 160C

On all other switch types, only one uplink port can be configured as an trunking port. The forwarding of Q in Q Frames is not supported by these switch types. See also chapter *10.31.6.1 Q-in-Q with two Nexans Switches.*

10.31.7. Port Trunking Mode

The Trunking Mode defines whether the respective port shall transport all VLAN Ids defined in the VLAN Table.

The Trunking Mode offers the following settings:
- Disable
- Enabled with 802.1Q Tagging
- Hybrid
- Enabled without Tagging

The mode of function of the different settings depends on whether the VLAN Table Mode is set to an ‘802.1Q based’ or ‘Port-based’ mode.

Disable:
- 802.1Q based: With this setting only those packets are sent on the respective port which are part of the Default- or Voice-VLAN of the respective port.

- Port-based: Packets are sent on this port exactly as they have been received on another connected port. Included 802.1Q VLAN tags, if any, are passed through 1:1.

Enable with 802.1Q Tagging:
- 802.1Q based: On the respective port the packets of all VLANs, which are indicated in the VLAN table, are sent and provided with a VLAN tag according to IEEE802.1Q (with the exception of the Default-VLAN).
Any received packets, which also contain an IEEE802.1Q tag, are assigned to the VLAN indicated in the tag. However, if this VLAN ID is not listed in the VLAN table, the packet will be discarded.
Any received packets, which do not contain a tag, are principally assigned to the Default-VLAN of the respective port (see also chapter *10.31.8. Port Default VLAN-ID*).
Please note that also the remote side (central switch) must be able to read these tags and has been configured accordingly.

• Port-based: Untagged packets, which have been received on another connected port, are sent with an 802.1Q tag. The Default VLAN-ID set on this port is inserted as an 802.1Q VLAN tag. Tagged packets received on another connected port are sent unchanged.

Hybrid:

• 802.1Q based: For the respective port, it can be set individually for each VLAN in the VLAN table whether this VLAN is allowed or not.
Received packets containing an IEEE802.1Q tag will be assigned to the VLAN specified in the tag if the VLAN is allowed for that port. Otherwise, the package is discarded.
Any received packets, which do not contain a tag, are principally assigned to the Default-VLAN of the respective port (see also chapter *10.31.8. Port Default VLAN-ID*).
Please note that also the remote side (central switch) must be able to read these tags and has been configured accordingly.

• Port-based: The Hybrid mode is not supported here.

Enable without Tagging:

• 802.1Q based: On the respective port the packets of all VLANs, which are indicated in the VLAN table, are sent - however always without tag. Due to the missing tag the connected switch does not receive any VLAN information on the individual packets. Thus, it will be the task of the central switch to determine the VLAN assignment from other sources (e.g. from the MAC source address). IMPORTANT: In any case, a tag is needed in the received packets to enable the Nexans switch to determine which VLAN they belong to. Any received packets, which do not contain a tag, are principally assigned to the Default-VLAN ID of the respective port.

• Port-based: Packets received on another connected port are principally sent without VLAN tag.

10.31.8. Port Default VLAN-ID

The Port Default-VLAN ID defines which packets are sent and received without tag on the respective port. Even if IEEE802.1Q tagging has been enabled for the respective port, the packets of the Default-VLAN ID will be sent without tag on this port. In receive direction this means that all receive packets which have no tag are assigned to this Default-VLAN ID.

If for a trunked port principally all packets shall be sent and received in tagged format, the Default-VLAN ID of the respective port needs to be set to 0. In this case all received packets, which contain no tag, will be discarded.

IMPORTANT:
If a Default-VLAN-ID is used for a tagged port, the same VLAN ID on the remote side (central switch) should be set as Default-VLAN-ID, too. Otherwise the packet may find no receiver and will be discarded.

NOTE:
The Default-VLAN-ID is sometimes also called Native-VLAN-ID.

10.31.9. Port Voice VLAN-ID

A single tagged VLAN can be configured on the respective port using the Voice-VLAN-ID of the port. As the name indicates, this function is especially designed for the combination of IP phone and downstream PC. In most Voice-over-IP installations the PC sends and receives untagged packets, whereas the IP phone sends and receives tagged packets with the appropriate 802.1Q prioritisation information. In this case the Default-VLAN-ID should be configured to the PC's VLAN and the Voice-VLAN-ID to the VLAN of the IP phone.

If only the default VLAN shall be accepted for the port, the Voice-VLAN-ID of the respective port should be set to 0 (factory default).

NOTE: If IEEE802.1Q Tagging is enabled for the respective port, a configured Voice-VLAN-ID, if any, will be ignored.

10.31.10. Port VLAN Tagging

The VLAN Tagging determines for each port and each VLAN whether packets of the respective VLAN are allowed through and whether the VLAN of the sent packets is provided with an IEEE802.1Q tag or not. It depends on the set Trunking Mode and the set default VLAN-ID or Voice-VLAN-ID of the respective port.

VLAN Tagging of all VLANs, except the Default VLAN-ID and Voice VLAN-ID, can only be set individually in Trunking Mode "Hybrid". Tagging is fixed for all other Trunking Modes. The corresponding configuration parameters are read-only for the respective port (see chapter *10.31.7 Port Trunking Mode*).

With VLAN Tagging, the following settings are displayed for each port and each VLAN:

- D
- V
- T
- U
- -

D:
The respective VLAN is set as the Default VLAN-ID for the port. Packets of the Default VLAN are always sent untagged via the port. Received packets from the Default VLAN can be tagged or untagged.

V:
The respective VLAN is set as the Voice VLAN-ID for the port. Packets of the Voice VLAN are always sent tagged via the port. Received packets of the voice VLAN must also be tagged.

T:
Packets of the respective VLAN are sent tagged via the port. Received packets from the VLAN must also be tagged.

U:
Packets of the respective VLAN are sent untagged via the port. Received packets from the VLAN must be tagged.

-:
Packets from the respective VLAN are not permitted for the port and are discarded on receipt.

In Trunking Mode "Hybrid" the following settings can be changed for the respective port and each VLAN, except for the Default VLAN-ID and Voice VLAN-ID:

- T
- U (depending on the switch type)
- -

10.31.11. Active Default VLAN-ID

The 'Active Default VLAN-ID' shows the currently valid Default VLAN-ID for the respective port. Normally this is the Default VLAN-ID which was configured for the port.

If a Portsecurity function with authentication via Radius server is enabled for the port, the Active Default VLAN-ID can also be the RADIUS-Unsecure-VLAN-ID, RADIUS-Guest-VLAN-ID, RADIUS-Inaccessible-VLAN-ID or IEEE802.1X-Authentication-Failure-VLAN-ID. This depends on whether the MAC address or the user has not yet been authenticated or the authentication has failed. Furthermore, the Active Default VLAN can also be assigned via Radius server and is thus completely independent from the VLAN-IDs configured in the switch.

For further information see chapter *10.59. Portsecurity with authentication via RADIUS server*

Moreover, if the portmonitor function is enabled, the Monitor-Destination-Port is set to the Default VLAN-ID of the source port (see chapter *10.34. Portmonitor*).

10.31.12. Active Voice VLAN-ID

The 'Active Voice VLAN-ID' shows the currently valid Voice VLAN-ID for the respective port. Normally this is the Voice VLAN-ID which was configured for the port.

If a Portsecurity function with authentication via Radius server is enabled for the port, the Active Voice VLAN can also be assigned via Radius server and is thus completely independent from the Voice VLAN-ID configured in the switch.

Moreover, if the portmonitor function is enabled, the Monitor-Destination-Port is set to the Voice VLAN-ID of the source port (see chapter *10.34. Portmonitor*).

10.31.13. Active Trunking Mode

The 'Active Trunking Mode' shows the currently valid Trunking Mode for the corresponding port. Normally this is the Trunking Mode which was configured for the port.

If a Portsecurity function with authentication via Radius server is enabled for the port, the active Trunking Mode can also be 'Disabled', although the configuration shows that the Trunking Mode is enabled. This depends on whether the MAC address or the user has not yet been authenticated or the authentication has failed. For further information see chapter *10.59. Portsecurity with authentication via RADIUS server*

Moreover, the Destination Port will be set to the Trunking Mode of the Source Port, if the Port Monitor function is activated (see chapter *10.34. Portmonitor*).

10.31.14. Port Active VLAN Tagging

The 'Active VLAN Tagging' shows the currently valid VLAN Tagging for the respective port and VLAN. This is usually the VLAN Tagging configured for the port.

If a Portsecurity function with authentication via Radius server is enabled for the port, VLAN Tagging depends on the resulting active VLAN parameters 'Active Trunking Mode', 'Active Default VLAN-ID' and 'Active Voice VLAN-ID'. The settings for Active VLAN Tagging are made in according to chapter *10.31.10 Port VLAN Tagging*. However, the active VLAN parameters are used instead of the configured ones.

10.31.15. RADIUS Unsecure VLAN-ID

All ports, for which a RADIUS-MAC-based or IEEE802.1X Portsecurity mode is enabled, will be switched to this RADIUS-Unsecure-VLAN if unauthenticated. Here the Default-VLAN-ID of the respective port is ignored, and the RADIUS-Unsecure-VLAN-ID used instead. Thus, if the central switch is configured accordingly, an 'unauthenticated' port can be switched to a special VLAN, which offers limited functionality only. If, however, an 'unauthenticated' port shall not have any access to the network, the RADIUS-Unsecure-VLAN ID should have a value which is not used on the central switch. In this case no packets from this VLAN will be received.

For further information about VLAN assignment see flowchart in chapters *10.59.1. Portsecurity Modes {RADIUS allow ...}* and *10.59.2 Portsecurity Mode {IEEE802.1X allow one MAC address}*.

10.31.16. RADIUS Guest VLAN-ID

The 'RADIUS Guest VLAN-ID' is a global VLAN setting and applies only to ports for which a RADIUS-MAC-based or IEEE802.1X Portsecurity mode is enabled. A port will be moved into this VLAN if authentication fails.

Set this VLAN-ID to 0 if you don’t want to apply this VLAN.

For further information about VLAN assignment see flowchart in chapters *10.59.1. Portsecurity Modes {RADIUS allow ...}* and *10.59.2Portsecurity Mode {IEEE802.1X allow one MAC address}*.

10.31.17. RADIUS Inaccessible VLAN-ID

The 'RADIUS Inaccessible VLAN-ID' is a global VLAN setting and applies only to ports for which a RADIUS-MAC-based or IEEE802.1X Portsecurity mode is enabled. A port will be moved into this VLAN if all RADIUS servers are down.

Set this VLAN-ID to 0 if you don’t want to apply this VLAN.

For further information about VLAN assignment see flowchart in chapters *10.59.1. Portsecurity Modes {RADIUS allow ...}* and *10.59.2Portsecurity Mode {IEEE802.1X allow one MAC address}*.

10.31.18. IEEE802.1X Authentication Failure VLAN-ID

The 'IEEE802.1X Authentication Failure VLAN-ID' is a global VLAN setting and applies only to ports for which an IEEE802.1X Portsecurity mode is enabled. A port will be shifted into this VLAN, when the connected 802.1X client has exceeded the maximum number of authentication retries.

Set this VLAN-ID to 0 if you don’t want to apply this VLAN.

For further information about VLAN assignment see flowchart in chapters *10.59.1. Portsecurity Modes {RADIUS allow ...}* and *10.59.2Portsecurity Mode {IEEE802.1X allow one MAC address}*.

10.32. VLAN Portmirror

By selecting VLAN Portmirror the address learning feature in the switch is disabled and the switch behaves like a hub within any VLAN. This means that on all ports of a VLAN all packets of the respective VLAN are forwarded.

Thus, function is quite useful, if e.g. the data traffic of a selected TP port shall be recorded on a different TP port. To do so, both ports must be in the same VLAN.

IMPORTANT NOTE:
When this function is enabled, the MAC address list can no longer be displayed in Telnet/SSH/V.24 console and SNMP. Moreover, the Portsecurity function and the bandwidth limiter of all ports are disabled.

10.33. Global LED Mode

The LED Setup function allows you to modify the display mode of the switch LEDs. The following display modes can be set:

- Standard
- All LEDs Off
- All LEDs Off, except Mgmt LED
- All LEDs On
- All LEDs green blinking
- Right LEDs red/blue blinking

Standard:
This is the factory default. The User LEDs light up, as soon as a link is established.

All LEDs Off:
All User LEDs ae always switched off, independent of whether the port has an active link or not.

All LEDs Off, execpt Mgmt LED:
The management LED shows its normal functionality. All other LEDs are permanently off.

All LEDs On:
All User LEDs are always switched on, independent of whether the port has an active link or not.

All LEDs green blinking:
All LEDs blinking green.

Right LEDs red/blue blinking:
All LEDs are blinking red and blue.

10.34. Portmonitor

The Port Monitor function (also called port mirroring) allows the duplication of the data traffic of one single switch port to a second port. The Source Port, whose traffic shall be monitored, and the Destination Port, to which these data shall be duplicated, can be freely selected.
The following modes can be selected:

- Disabled
- Rx and Tx
- Rx only
- Tx only

Disabled:
This Port Monitor function is disabled.

Rx and Tx:
All packets which are received or sent on the Source Port will be duplicated onto the Destination Port.

Rx only:
Only packets which are received on the Source Port will be duplicated onto the Destination Port.

Tx only:
Only packets which are sent on the Source Port will be duplicated onto the Destination Port.

IMPORTANT:
If the Port Monitor function is enabled, the selected destination port is blocked for normal data traffic and can only be used for monitoring the data of the source port. Moreover the Active VLAN-ID, Voice VLAN-ID and the Active Trunking Mode of the destination port will automatically be set to the corresponding values of the source port. This means, that packets will leave the destination port just as they were received or sent on the source port. If the source port is set to Trunking, any tagged packets on the source port will also be sent with tag on the destination port.

NOTE:
Does only apply to switches whose tagging Ethertype is set to 9100(Q-in-Q) or 9200(Q-in-Q):
If on the monitor source port packets with Q-in-Q Tag 9100 or 9200 are sent or received, this Q-in-Q Tag might be removed prior to forwarding the packet to the monitor destination port.

10.35. IEEE802.1X Transparency

This feature ensures that all multicast packets '01:80:C2:00:00:03' used for IEEE802.1x authentication will transparently pass through the switch. Even if the individual ports have been configured in different VLANs, these special multicasts will be distributed to all ports. However, all other multicasts and broadcasts will remain within the defined VLAN limits.

This function is used in connection with central switches which support Multi-User Authentication per Port with IEEE802.1x. In this way the central switch can perform IEEE802.1x authentication, although the users on the Nexans switch have been configured for different VLANs.

NOTE:
This function is automatically disabled, if IEEE802.1X authentication is enabled for at least one port. In this case, IEEE802.1X authentication is exclusively executed by the Nexans switch.

10.36. Portsecurity

The following modes are supported:
- Auto allow one, two or three MAC address(es)
- Manual setting of three MAC addresses
- Manual setting of three vendor MAC addresses
- Learn and fix one or two MAC address(es)

The following modes, **with** authentication via Radius server, are additionally supported by firmware versions with IEEE802.1X functionality (description see chapter *10.59. Portsecurity with authentication via RADIUS server*):
- RADIUS allow one, two or three MAC-Address(es)
- IEEE802.1X allow one MAC-Address
- IEEE802.1X PC+Voice allow two MAC-Addresses
- IEEE802.1X Multi-User allow three MAC-Addresses
- IEEE802.1X allow all MAC-Addresses
- IEEE802.1X Supplicant with MD5 Challenge
- IEEE802.1X Radius MAC Bypass enable

10.36.1. Portsecurity Failure Action

This setting defines whether a Portsecurity failure will disable the respective port or whether only periodic events will be sent.

Disabled ports can automatically reactivated by an configurable “Re-Enable Time for Security-Disabled Ports”. This time can be from 1 to 60000 seconds.

The following settings are possible for Portsecurity Failure Action:
- Don't disable Port. Send periodic Events only

- Disable Port immediately after first wrong MAC
- Disable Port after second wrong MAC
- Disable Port immediately after wrong MAC or Authentication

Disable Port immediately after first wrong MAC:
Immediately after the detection of a Portsecurity-MAC failure the corresponding port will be disabled. As a consequence the value 'SECURITY DISABLED' will be displayed as state under 'Link State' and 'Security State'.

Disable Port after second wrong MAC:
In case of a Portsecurity-MAC failure the first faulty MAC address will be blocked first and displayed in NEXMAN in the 'Allowed MACs Overflow Address' column. Then the value 'SECURITY WARNING' will be displayed as state under 'Security State'.
Only after the detection of a second faulty MAC address the corresponding port will be disabled. As a consequence the value 'SECURITY DISABLED' will be displayed as state under 'Link State' and 'Security State'.

Don't disable Port. Send periodic Events only:
This setting is only possible for firmware versions with SNMP support. In case of a Portsecurity failure the respective port will remain active and SECURITY WARNING will be displayed in Security State. However, a Portsecurity Failure event will be sent periodically (5-minute interval) containing the initiating MAC address and the respective switch port. Moreover, this MAC address is entered into the SNMP variable bmSwitchInfoSecurityFailMacAddr and can be queried via SNMP request.

Disable Port immediately after wrong MAC or Authentication:
This mode is identical to the “Disable Port immediately after first wrong MAC” security mode. Additionally, the respective port will be disabled, if authentication was refused by the RADIUS Server in the “RADIUS …” and “IEEE802.1X …” security modes. Consequently, the value SECURITY DISABLED is displayed as a state under “Link State” and “Security State”.

For firmware versions with SNMP support additionally a single Portsecurity Failure event will be sent containing the initiating MAC address and the respective switch port. Moreover, this MAC address is entered into the SNMP variable bmSwitchInfoSecurityFailMacAddr and can be queried via SNMP request.

The following events result in a Portsecurity-MAC failure:

Security Mode	Event
Manual setting of three MAC addresses	Detection of a MAC address which was not manually configured using NEXMAN.
Manual setting of three vendor MAC addresses	Detection of a vendor MAC address which was not configured using NEXMAN.
Auto allow one MAC address	Detection of more than one MAC address during Link Up.
Auto allow two MAC addresses	Detection of more than two MAC addresses during Link Up.
Auto allow three MAC addresses	Detection of more than three MAC addresses during Link Up.
Learn and fix one MAC address	Detection of a MAC address, which was not automatically learned before. A maximum of one MAC address can be learned.
Learn and fix two MAC addresses	Detection of a MAC address, which was not automatically learned before. A maximum of two MAC addresses can be learned.
RADIUS allow one MAC address	Detection of more than one MAC address during Link Up.
RADIUS allow two MAC addresses	Detection of more than two MAC addresses during Link Up.
RADIUS allow three MAC addresses	Detection of more than three MAC addresses during Link Up.
IEEE802.1X allow one MAC address	Detection of more than one MAC address during Link Up.
IEEE802.1X PC+Voice allow two MAC-Addresses	Detection of more than two MAC addresses during Link Up.
IEEE802.1X Multi-User allow three MAC-Addresses	Detection of more than three MAC addresses during Link Up.
IEEE802.1X allow all MAC-Addresses	not applicable

10.36.2. Portsecurity - Voice VLAN Authentication Mode

For MAC addresses which are discovered in the Voice VLAN the 'Voice VLAN Authentication Mode ‘determines, if a RADIUS-MAC-based or IEEE802.1X authentication will be achieved.

Two modes are available:
- Enable Authentication
- Bypass Authentication

Enable Authentication (Default):
MAC addresses discovered in the Voice VLAN must be authenticated in accordance with the configured portsecurity mode. Without a valid authentication the access to the Voice VLAN is blocked.

Bypass Authentication:
MAC addresses discovered in the Voice VLAN have direct access to the configured Voice VLAN.

NOTE:
The 'Voice VLAN Authentication Mode‘ is only relevant for ports which have
a) a Voice VLAN configured
and
b) a RADIUS-MAC-based or IEEE802.1X Portsecurity mode enabled

10.36.3. Portsecurity - Allowed MACs Overflow Address

In case of a Portsecurity failure the faulty MAC address will be displayed among others in NEXMAN in the 'Allowed MACs Overflow Address' column. The values 'SECURITY WARNING' and 'SECURITY DISABLED' respectively will be displayed as state in the 'Security State' column, depending on the setting of the 'Port Security Failure Action' parameter (see chapter *10.36.1. Portsecurity Failure Action*).

10.36.4. Portsecurity – Security State

The Security State is only displayed if one of the above mentioned Portsecurity modes is enabled for the respective port. Otherwise 'not supported' or '-' will be displayed.

The following table indicates the possible state values:

Security State	
Designation	**Description**
-	Portsecurity is disabled
Waiting for Link	No valid link signal was detected on the port.
Waiting for MAC’s	A valid link signal was detected on the port. However, no data packet from a connected device has been received yet, in order to learn its MAC address.
Authenticating	An authentication according to IEEE802.1X or RADIUS MAC-based is currently being performed for at least one MAC address of the port.
Port Authenticated	No Portsecurity failure and no Portsecurity warning have occurred for any of the learned MAC addresses. Moreover, all authentications according to IEEE802.1X or RADIUS MAC-based have been completed.
SECURITY DISABLED	The port was automatically disabled because a Portsecurity failure was detected (see chapter *10.36.1. Portsecurity Failure Action*)
Security Warning	A Portsecurity failure was detected on the port, but the port was not disabled (see chapter (see chapter *10.36.1. Portsecurity Failure Action*)
LOOP-DISABLED	The port was automatically disabled, because the activated 'Active Loop Protection' has detected a loop.
Port Admin Disabled	The port was manually disabled by the administrator.
RADIUS Server(s) down	All configured Radius Server are not reachable. An alarm will be shown in the Manager’s Device List.
Unsecure VLAN	The Unsecure VLAN has been assigned to this port
Auth.-Failure-VLAN	The Auth.-Failure-VLAN has been assigned to this port
BPDU-DISABLED	The port was automatically disabled, because a Spanning-Tree BPDU packet was received

RING-LOOP-DISABLED	The port was automatically disabled, because a Loop-Protection packet was received
DHCP-SNOOP-DISABLED	The port was automatically disabled, because a DHCP-Server packet was received

10.36.5. Portsecurity - Renew Command

If you want to re-initialize a port with enabled Portsecurity or re-activate an automatically disabled port, this can be done via the 'Portsecurity - Renew' command.

NOTE:
This renew command can be used via CLI and WEB in the user mode (Read/Only Access) as well as in the admin mode (Read/Write Access).

Upon entry of this command the following actions will be executed for the respective port:

- **Portsecurity Modi {Disabled}:**
- If the port is disabled it will be enabled again.

- **Portsecurity Modes {Manual setting ...}:**
- If the port is disabled, it will be enabled again.

- **Portsecurity Modes {Auto allow ...}:**
- If the port is disabled, it will be enabled again.
- All learned MAC addresses will be deleted.

- **Portsecurity Modes {Learn and fix ...}:**
- If the port is disabled, it will be enabled again.
- All learned MAC addresses, which are stored in flash, will be deleted.

- **Portsecurity Modes {RADIUS allow ...}:**
- If the port is disabled, it will be enabled again.
- All learned MAC addresses will be deleted and have to be re-authenticated via Radius.
- The port is set to the Startup VLAN (Default-VLAN or RADIUS-Unsecure-VLAN).

- **Portsecurity Mode {IEEE802.1X allow one MAC address}:**
- If the port is disabled, it will be enabled again.
- The learned MAC address will be deleted.
- The port is set to the Startup-VLAN (Default-VLAN e.g. Radius-Unsecure-VLAN)

- Authentication of the terminal unit according to IEEE802.1X is re-started.

- **Portsecurity Modus {PC+Voice allow two MAC-Addresses}:**
- If the port is disabled, it will be enabled again.
- The learned MAC address will be deleted.
- The port is set to the Startup-VLAN (Default-VLAN e.g. Radius-Unsecure-VLAN)
- Authentication of the terminal unit according to IEEE802.1X is re-started.

- **Portsecurity Modus {Multi-User allow three MAC-Addresses}:**
- If the port is disabled, it will be enabled again.
- The learned MAC address will be deleted.
- The port is set to the RADIUS-Unsecure-VLAN, new MAC addresses will be blocked until authentication
- Authentication of the terminal unit according to IEEE802.1X is re-started.

- **Portsecurity Mode {IEEE802.1X allow all MAC addresses}:**
- If the port is disabled, it will be enabled again.
- The port is set to the Startup-VLAN (Default-VLAN e.g. Radius-Unsecure-VLAN)
- Authentication of the connected terminal unit according to IEEE802.1X is re-started.

- **Portsecurity Modus {Supplicant with MD5 Challenge}:**
- No applicable. Authentication must be done by core switch.

10.36.6. Portsecurity Mode {Auto allow one, two or three MAC address(es)}

The Security modes {Auto allow one MAC address}, {Auto allow two MAC addresses} and {Auto allow three MAC addresses} allow the switch to dynamically limit access via the respective ports to one, two or three MAC

addresses and to report any other address as Portsecurity Failure and that the port is disabled, if necessary (see chapter *10.36.1. Portsecurity Failure Action*). This prevents e.g. that the user connects another switch behind a TP port. The learned MAC addresses are automatically deleted, when the link of the respective port fails (e.g. when a different PC is inserted) or when the port is disabled manually.

If you want to reinitialise the Portsecurity function of a selected port or re-activate an automatically disabled port, this can be enforced via the Renew command (see chapter *10.36.5. Portsecurity - Renew Command*).

10.36.7. Portsecurity Mode {Manual setting three MAC addresses}

In this mode up to three MAC addresses can be permanently configured per port. If the respective port then receives an unknown MAC address, this port will be disabled, if necessary (see chapter*10.36.1. Portsecurity Failure Action)*.

If you want to reinitialise the Portsecurity function of a selected port or re-activate an automatically disabled port, this can be enforced via the Renew command (see chapter *10.36.5. Portsecurity - Renew Command*).

10.36.8. Portsecurity Mode {Manual setting three vendor MAC addresses}

In this mode up to three vendor MAC addresses can be permanently configured per port. This function is identical with the setting {Manual setting three MAC addresses}. However, only the vendor part (i.e. the first three bytes) of the configured MAC addresses will be checked.

10.36.9. Portsecurity Mode {Learn and fix one or two MAC address(es)}

With the Security functions {Learn and fix one MAC address} and {Learn and fix two MAC addresses} the switch automatically learns one or two MAC addresses and writes them permanently into flash. Any other addresses are reported as Portsecurity Failure and the port is disabled, if necessary (see chapter *10.36.1. Portsecurity Failure Action*). Since the learned MAC addresses are stored in flash, these will be active also after rebooting the switch.

If you want to reinitialise the Portsecurity function of a selected port or re-activate an automatically disabled port, this can be enforced via the Renew command (see chapter *10.36.5. Portsecurity - Renew Command*).

10.36.10. Portsecurity - MAC Addresses

In NEXMAN, WEB, Telnet and SNMP for each port up to three MAC addresses are indicated which are relevant to Portsecurity. These are either the fixed or the automatically learned MAC addresses. If Portsecurity is disabled, the learned MAC addresses are also shown; however, these will not be used for any security functions. If in this case more than three MAC addresses per port are detected, the message 'More than three MACs' will be shown instead of the MAC addresses. In order to show all addresses you can use, e.g. in NEXMAN the 'Show MAC Table' function is used.

10.36.11. Portsecurity - MAC State

The Security MAC status indicates the current authentication status for each Security MAC address.

The following table shows the possible status values:

Security MAC State	
Designation	**Description**
Fixed	The MAC address is preset and cannot be changed. For this port either a Security mode with manually preset or with automatically fixed MAC address is set.
Learned	The MAC address was learned, but no authentication performed.
MAC:Authen. via RADIUS	The port is set to a mode with MAC-based authentication {RADIUS allow ...} and the request to the RADIUS server for authentication of this MAC address is currently being executed.

MAC:REJECTED BY RADIUS	The request to the RADIUS server for authentication of this MAC address was rejected by the server sending an Access Reject message. An alarm will be shown in the Manager's Device List.
MAC:OK	The request to the RADIUS server for authentication of this MAC address was accepted by the server sending an Access Accept message. The MAC address was assigned to the default VLAN of the respective port.
MAC:OK:Voice-VLAN	The request to the RADIUS server for authentication of this MAC address was accepted by the server sending an Access Accept message. The MAC address was assigned to the voice VLAN of the respective port.
BYPASS:OK:Voice-VLAN	This MAC address is discovered in the Voice VLAN has direct access to the configured Voice VLAN without authentication.
DOT1X:Requesting Identity	The port is set to a mode with IEEE802.1X-based authentication and the switch is trying to establish a contact to the IEEE802.1X supplicant of the connected terminal via EAP-Request-Identity packets.
DOT1X:Authen. via RADIUS	The port is set to a mode with IEEE802.1X-based authentication and the request to the RADIUS server for authentication of this IEEE802.1X device is currently being executed.
DOT1X:REJECTED BY RADIUS	The request to the RADIUS server for authentication of this IEEE802.1X device was rejected by the server sending an Access Reject message. An alarm will be shown in the Manager's Device List.
DOT1X:OK	The request to the RADIUS server for authentication of this IEEE802.1X device was accepted by the server sending an Access Accept message. The MAC address was assigned to the default VLAN of the respective port.
DOT1X:OK:Voice-VLAN	The request to the RADIUS server for authentication of this IEEE802.1X device was accepted by the server sending an Access Accept message. The MAC address was assigned to the voice VLAN of the respective port.

10.36.12. Portsecurity - MAC Address Ageing

The MAC addresses learned via Portsecurity are listed in a separate table independent of the Switch Forwarding Table (see Chapter *10.37. MAC Address Table*). The MAC addresses learned via Portsecurity are displayed e. g. in the Manager on the 'MAC+Security State' tab and normally deleted only after a link-down or (with fixed MAC's) after a Renew command.

Via the Portsecurity Address Ageing Setup alternative an ageing time of between 1 and 255 minutes can be set for the learned Portsecurity MAC addresses. The pot security aging time cannot be less than the aging time that is configured for the forwarding table (see Chapter *10.39 Address Ageing Time of the Forwarding Table*).

There are two configureable times:

- Portsecurity ageing time
- Portsecurity ageing time for PC behind IP-Phone

Portsecurity ageing time:
This time setting applies to the following Portsecurity modes:
- Disabled
- Auto allow one/two/three MAC address(es)
- IEEE802.1X PC+Voice allow two MAC addresses
- IEEE802.1X Multi-User allow three MAC addresses

The set time applies to all learned MAC addresses in the above mentioned modes, with the exception of MAC addresses from terminal devices, which have been learned in connection with a voice VLAN, i. e. from PCs connected behind an IP phone. For these terminal devices a separate ageing time can be configured (see below). If the ageing time is set to "0", ageing is disabled (factory default) and the Portsecurity MAC addresses can only be deleted using the Link Down or Renew commands.

Portsecurity ageing time for PC behind IP-Phone:
This ageing time does only apply to devices connected behind an IP-phone. The precondition is that the Portsecurity mode is set to “IEEE802.1X PC+Voice allow two MAC addresses” and that a MAC address was detected on the port in the voice VLAN.

This is particularly interesting for installations which have an IP phone and a cascaded notebook connected to one port of the switch (e. g. flexible work places). If the connected notebook is removed, the notebook’s MAC address will be deleted after expiration of the ageing time and a notebook with a different MAC address can be connected. If the ageing time is set to ‘0’, ageing is disabled (factory default), that means that the MAC address can only be deleted by a link down of the switch port or by the portsecurity renew command.

Portsecurity ageing time for Allowed MACs Overflow Address:
This time setting applies to the following Portsecurity modes:
- Auto allow one/two/three MAC address(es)
- IEEE802.1X PC+Voice allow two MAC addresses
- IEEE802.1X Multi-User allow three MAC addresses

In case of a Portsecurity-MAC failure the first faulty MAC address will be blocked and reported as 'Allowed MACs Overflow Address'. If an ageing time is configured and the MAC address shown in 'Allowed MACs Overflow Address' is not seen for the configured ageing period, the MAC address will be deleted.
If the ageing time is set to ‘0’, ageing is disabled (factory default), that means that the 'Allowed MACs Overflow Address' can only be delete by a link down of the switch port or by the portsecurity renew command.

10.37. MAC Address Table

Via NEXMAN, Telnet/SSH/V.24-Console and SNMP a list of all learned MAC addresses and of the related VLANs and Ports can be retrieved.

In NEXMAN this is done via the 'Show MAC Table' function.

The respective console command is: '`sh:ow ma:c-address-table d:ynamic [<if-no>|a:ll]`'

Via SNMP the MAC addresses can be requested via the following standard MIBs:
- BRIDGE-MIB: dot1dTpFdbTable

Chapter *0*

List of SNMP MIBs contains a detailed summary of all SNMP-MIBs.

10.38. Quality of Service (QoS) / Prioritization

There are two QoS procedures which are based on current industry standards and are fully supported by the switch:
- IEEE802.1p (Layer-2)
- IPv4 / IPv6 (Layer-3)

Moreover a port-based default prioritisation is supported:
- Default 802.1p Priorityvalue / Default Queue

Each switch port has four output queues. The packets of Queue 0 have the lowest priority and those of Queue 3 the highest priority.

10.38.1. Prioritization Scheme

One of the following prioritization schemes can be chosen to process the queues:
- Strict Priority Queuing
- Weighted

The following schemes are only available with newer switch versions:
- Strict for Queue 3 / Weighted for Queues 2,1,0
- Strict for Queues 3,2 / Weighted for Queues 1,0

Strict:
In this case all packets of one queue are always send, before packets from the next lower queue will be processed.

Weighted:
With Weighted Queuing after sending 2 packets of one queue, one packet of the next lower queue is sent. If you compare e.g. Queue 3 with Queue 0, this means that after sending eight packets of Queue 3 one packet of Queue 0 is sent.

Strict for Queue 3 / Weighted for Queues 2,1,0:
In this case all packets from Queue are send, before packets from Queue 0, 1 and 2 are send with the Weighted Fair Queuing.

Strict for Queues 3,2 / Weighted for Queues 1,0:
In this case all packets from Queue 3 and 2 are send, before packets from Queue 0 and 1 are send with the Weighted Fair Queuing.

10.38.2. Prioritization according to IEEE802.1p

Prioritization according to IEEE802.1p can be separately enabled for each port and reads the IEEE802.1p priority value in tagged receive packets to assign it to one of the four internal queues.

There are two exceptional cases:
- For untagged packets the configured 'Default 802.1p Priorityvalue' priorityvalue of the respective port is used to the assign of queue.
- If the priorityvalue is overwritten or assigned by the function “IEEE802.1p VLAN based priority override“ this new priorityvalue will be used to assign the queue.

The IEEE802.1p standard defines a total of 8 priority values for the tag:
0 = Best effort
1 = Background
2 = Reserved
3 = Excellent effort
4 = Controlled load
5 = Video
6 = Voice
7 = Network control

Now, in the global IEEE802.1p Priority Setup within the switches the desired queue can be assigned to the respective priority value. Example: If all receive packets with priority value 6:voice shall receive priority treatment (e.g. because IP phones with IEEE802.1Q/p support are to be connected), the queue for Voice must be set to a value greater than 0 in the Priority Setup: 802.1p.

The factory default assignment of the queues for the above listed priority values are defined within the IEEE standard 802.1D chapter 7.7.3 table 7-2:

Table 7-2—Recommended user priority to traffic class mappings

User Priority	Number of available traffic classes							
	1	2	3	4	5	6	7	8
0 (Default)	0	0	0	1	1	1	1	2
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	1
3	0	0	0	1	1	2	2	3
4	0	1	1	2	2	3	3	4
5	0	1	1	2	3	4	4	5
6	0	1	2	3	4	5	5	6
7	0	1	2	3	4	5	6	7

NOTE—The rationale for these mappings is discussed in Annex G (informative). Frames with default user priority are given preferential treatment over user priority 1 and 2 in Bridges that implement four or more Traffic Classes.

IMPORTANT:
If prioritisation according to IEEE802.1p is enabled for the respective port, prioritisation will be performed in line with the set Default 802.1p Priority value. (see *10.38.5 Port Default 802.1p Priorityvalue / Port Default Queue*)

NOTE:
The Priority Setup: 802.1p is a global switch setting and applied to all ports with enabled IEEE802.1p prioritization.

10.38.3. IEEE802.1p VLAN based Priority Override

Using the “IEEE802.1p VLAN based Priority Override” function, the IEEE802.1p priority value can be overwritten depending on the VLAN-ID of the received packet.

This function can be enabled separately for each port and VLAN-ID.

The basic procedures are as follows:

• A Priority Override is only performed if the port where the packet was received has the “IEEE802.1p VLAN based Override” function enabled.

• If an untagged packet is received, this packet will be assigned to the default VLAN of the respective port. If this Default VLAN “IEEE802.1p VLAN based override value” is set in the VLAN table, the priority value will be taken from the VLAN table. If, however, the „IEEE802.1p VLAN based override value“ is disabled in the VLAN table, the “Default 802.1p priority value” of the corresponding port will be used instead.

• If a tagged packet is received, this packet will be assigned to the VLAN according to the tag and checked whether this VLAN is permitted for the respective port. If so, the packet will be forwarded. If this VLAN “IEEE802.1p VLAN based Override value” is set in the VLAN table, the received priority value will be overwritten by the priority value from the VLAN table. If, however, the “IEEE802.1p VLAN based override value” is disabled in the VLAN table, we have to differentiate between two cases:
a) If prioritization according to IEEE802.1p is enabled for the respective port, the priority value will be used as indicated in the received tag.

b) If prioritization according to IEEE802.1p is disabled for the respective port, the “Default 802.1p priority value” of the respective port will be used.

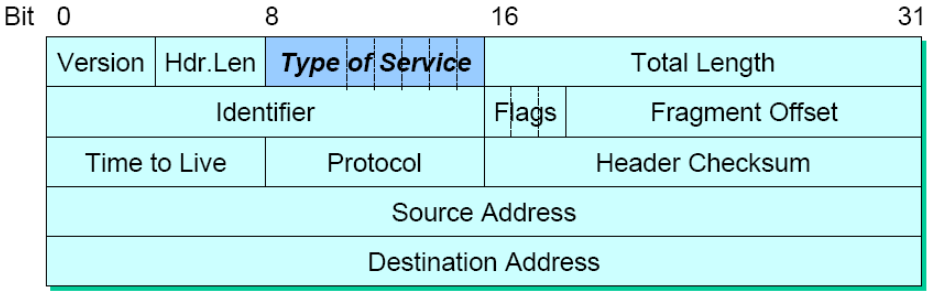
10.38.4. Prioritization according to IPv4/IPv6

Prioritization according to IPv4/IPv6 can be separately enabled for each port and reads the Type-of-Service field (IPv4) or the Traffic Class field (IPv6) of the receive packets.

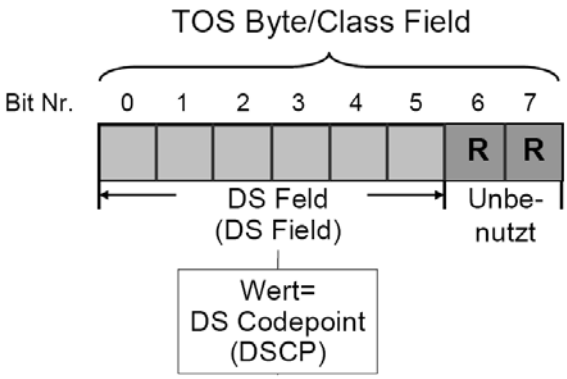
64 different priority values are possible for both fields. In the Priority Setup: IPv4/IPv6 the desired queue can then be assigned to each of these values.

If, on the respective port an IP packet is received and this packet is sent with a tag on another port (e. g. an uplink with enabled IEEE802.1Q Tagging), the queue set in “Priority Setup:IPv4/IPv6” is multiplied by 2 and inserted in the tag as an IEEE802.1p value.

Please find below the structure of an IPv4 packet header:



NOTE: From the Type-of-Service field only the first six bits are relevant, which have different meaning depending upon RFC standard. According to the current standards RFC2474 and RFC3168 this bits are called DSCP (Differentiated Services Code Point). The following figure shows the assignment between Type-of-Service and DSCP:



NOTE:
The management interface transmits all IPv4 packets using the DSCP value of 60. Thus it is possible to configure a unique IPv4 prioritisation of the management packets in the core switch.

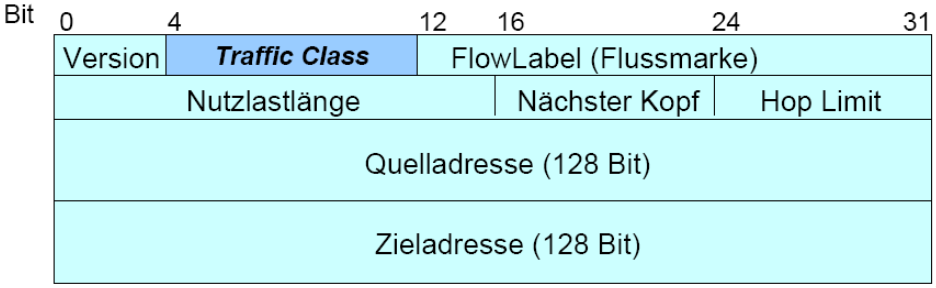
Conversion between the old designations in the RFC791 shows the following table:

RFC2474 / RFC3168	**RFC791**			
DSCP Differentiated Services Code Point	**Precedence (Priority)**	**D Delay**	**T Throughput**	**R Reliability**
0	0 : Normal	0	0	0
1	0 : Normal	0	0	1
2	0 : Normal	0	1	0
3	0 : Normal	0	1	1
4	0 : Normal	1	0	0
5	0 : Normal	1	0	1
6	0 : Normal	1	1	0
7	0 : Normal	1	1	1
8	1 : Priority	0	0	0
9	1 : Priority	0	0	1
10	1 : Priority	0	1	0

11	1 : Priority	0	1	1
12	1 : Priority	1	0	0
13	1 : Priority	1	0	1
14	1 : Priority	1	1	0
15	1 : Priority	1	1	1
16	2 : Immediate	0	0	0
17	2 : Immediate	0	0	1
18	2 : Immediate	0	1	0
19	2 : Immediate	0	1	1
20	2 : Immediate	1	0	0
21	2 : Immediate	1	0	1
22	2 : Immediate	1	1	0
23	3 : Flash	1	1	1
24	3 : Flash	0	0	0
25	3 : Flash	0	0	1
26	3 : Flash	0	1	0
27	3 : Flash	0	1	1
28	3 : Flash	1	0	0
29	3 : Flash	1	0	1
30	3 : Flash	1	1	0
31	3 : Flash	1	1	1
32	4 : Flash Override	0	0	0
33	4 : Flash Override	0	0	1
34	4 : Flash Override	0	1	0
35	4 : Flash Override	0	1	1
36	4 : Flash Override	1	0	0
37	4 : Flash Override	1	0	1
38	4 : Flash Override	1	1	0
39	4 : Flash Override	1	1	1
40	5 : Critical	0	0	0
41	5 : Critical	0	0	1
42	5 : Critical	0	1	0
43	5 : Critical	0	1	1
44	5 : Critical	1	0	0
45	5 : Critical	1	0	1
46	5 : Critical	1	1	0
47	5 : Critical	1	1	1
48	6 : Internet Control	0	0	0
49	6 : Internet Control	0	0	1
50	6 : Internet Control	0	1	0
51	6 : Internet Control	0	1	1
52	6 : Internet Control	1	0	0
53	6 : Internet Control	1	0	1
54	6 : Internet Control	1	1	0
55	6 : Internet Control	1	1	1
56	7 : Network Control	0	0	0
57	7 : Network Control	0	0	1
58	7 : Network Control	0	1	0
59	7 : Network Control	0	1	1

60	7 : Network Control	1	0	0
61	7 : Network Control	1	0	1
62	7 : Network Control	1	1	0
63	7 : Network Control	1	1	1

Please find below the structure of an IPv6 packet header:



NOTE:
The Priority Setup: IPv4/IPv6 is a global switch setting and applied to all ports with enabled IPv4/IPv6 prioritization.

10.38.5. Port Default 802.1p Priorityvalue / Port Default Queue

Default prioritization, also called port-based prioritization, is independent from the contents of the received packet and is used whenever none of the above mentioned prioritization methods apply to the respective received packet.

The following settings are possible:

Default 802.1p Priorityvalue	Default Queue
0 = Best effort	0
1 = Background	0
2 = Reserved	1
3 = Excellent effort	1
4 = Controlled load	2
5 = Video	2
6 = Voice	3
7 = Network control	3

Default 802.1p Priorityvalue:
If prioritization according to IEEE802.1p and IPv4/IPv6 are disabled on the respective, prioritization will exclusively be made according to the set Default Queue. 0 is the default value for all ports, i.e. no packet will be prioritized (the packets are forwarded in the order of their reception).

If a untagged packet is received on the respective port and if this packet is subsequently sent on another port with tag, (e. g. on an uplink with activated IEEE802.1Q tagging) the set Default 802.1p Priorityvalue will be inserted into the tag.

Important note:
If a packet **with** a tag is received on the respective port and if for the respective port prioritisation according to IEEE802.1p is disabled, the IEEE802.1p Priorityvalue contained in the tag will be overwritten by the set Default 802.1p Priorityvalue.

IMPORTANT:
If prioritization according to IEEE802.1p or IPv4/IPv6 is enabled for a port, the selected 'Default 802.1p Priorityvalue' will be ignored. If, however, a packet is received, to which none of the enabled prioritization methods applies (e.g. IPX packet without IEEE802.1p-Tag), the 'Default 802.1p Priorityvalue' is used again as a fallback value.

If prioritisation according to IEEE802.1p **and** IPv4/IPv6 is enabled, and a packet with IEEE802.1p tag **and** IP header is received, prioritisation according to IEEE802.1p will be given priority.

10.39. Address Ageing Time of the Forwarding Table

This feature allows you to set the time period after which the switch engine will automatically delete any learned MAC address of the forwading table..

NOTE:
Address ageing of the forwarding table has no influence on the learned MAC addresses of the Portsecurity aging time..(*10.36.12. Portsecurity - MAC Address Ageing*).

10.40. Port Name

For each port any Port Name containing a maximum of 64 characters can be entered. This name will then be displayed additionally in the respective tables and can be used e.g. to indicate the connected terminal.

10.41. Port Type

The Port Type shows the physical interface type of the respective port.

The following types are possible:
- Internal Management Port
- 10/100 Mbps Twisted Pair
- 10/100/1000 Mbps Twisted Pair
- 100 Mbps Fiber Optic
- 1000 Mbps Fiber Optic

10.42. Programming of Port Status-LEDs

The function of the port LED of the user ports is programmable. The setting of the LED has no influence on the port's function.

For the green Port Status-LED the following settings are possible:

- Show Link/Activity
  - Permanently off, if no link signal is received
  - Permanently on, if a valid link signal is received
  - Blinking, if data is received or send
- Blink (1) - Permanently blinking
- Off - Permanently off
- On - Permanently on
- Show Link/Speed-Duplex (1)
  - Permanently off, if no link signal is received
  - 1x short flash + pause, if a 1000-FDX link signal is received
  - 2x short flashes + pause, if a 100-FDX link signal is received
  - 3x short flashes + pause, if another link signal is received

For the yellow Port Status-LED the following settings are possible (only for desk systems):

- Show Full-Duplex - Permanently on, if a full-duplex link signal is received
- Show Speed (1)
  - Permanently off, if no link signal is received
  - 1x short flash + pause, if a 10 Mbit/s link signal is received
  - 2x short flash + pause, if a 100 Mbit/s link signal is received
  - 3x short flash + pause, if a 1000 Mbit/s link signal is received
- Blink (1) - Permanently blinking
- Off - Permanently off
- On - Permanently on
- Show PoE-Setup (1) - Permanently on, if PoE-Setup is set to 'Auto 802.3af' or 'On (Forced)'

(1) This function is not available for all switch types and firmware versions.

(2) The yellow Port Status-LED is available for desk and industrial switches only.

10.43. Bandwidth Limiter

For each port a bandwidth limiter can be enabled.

The following configuration settings of the bandwidth limiter are available:
1) RX Bitrate
2) TX Bitrate
3) Packet Type

IMPORTANT:
Switching the VLAN port mirror on will disable the bandwidth limiter for all ports.

10.43.1. In/Out Speed Limit

The bit rate limit value can be selected separately for RX and TX and can be set in the following increments:
- disable (factory default), no limiting
- 128kbps
- 256kbps
- 512kbps
- 1Mbps
- 2Mbps
- 4Mbps
- 8Mbps

Additionally the following levels can be selected for switches with gigabit ports:
- 16Mbps
- 32Mbps
- 64Mbps
- 128Mbps
- 256Mbps

The RX and TX Speed Limiters are working differently and this should be taken into consideration when configuring the limiters.

- **RX-Limiter**

The procedure depends on the 'Limiter Packet Type' setting:
a) If set to ' **Limit all Packet Types (TCP/IP burst compatible)**' the Leaky Bucket procedure will be used. The packets are written into a buffer and continuously forwarded according to the RX bit rate. The overall size of the RX buffer is 112 kB and is dynamically distributed among all active ports.

b) The **'Limit all Packet Types**' setting uses a procedure, which contrary to a) above uses a fixed-size buffer of 1.5 to 12 kB per port. The received packets are written into this FIFO buffer and forwarded according to the RX bit rate. Due to the smaller buffer size than for the procedure under a), there is a bigger probability that packets are discarded. This primarily depends on the transmission protocol used and the related burst traffic. Consequently this procedure is primarily suited for continuous data streams such as video and audio streams.

- **TX-Limiter**

This procedure is independent of the 'Limiter Packet Type' setting.
For the TX-Limiter principally the Leaky Bucket procedure is used. That means, the packets are written into a buffer and forwarded according to the TX bit rate. The overall size of the buffer is 112 kB and is dynamically distributed among all active ports.

10.43.2. Limiter Packet Type

The Packet Type defines which type of packets the limiter shall be applied to.

The following configuration settings are possible:
- Limit all Packets
- Limit Loop and Broadcast Packets

Limit all Packet Types:
This setting includes all packets in the calculation of the data rate. Different limit values for sent and received packets can be selected.

Limit all Packet Types (TCP/IP burst compatible):
This setting is identical with the above 'Limit all Packet Types' configuration. Additionally, for the RX-Limiter the traffic shaping of bursty TCP/IP data streams is supported. IMPORTANT: For optimum function this procedure requires the 'Flow Control State' to be enabled on the corresponding port. Moreover this mode is supported by certain newer switch types (e. g. GigaSwitch V3, GigaSwitch 54x and iGigaSwitch 54x) only.

Limit RX Flood-/Broadcast/Multicast Packets Only:
This limit value is exclusively applied to flooded receive packets. These are either broadcasts/multicasts or Unicast packets whose destination MAC address is unknown and which consequently are flooded to all ports. IMPORTANT: With this setting only the RX limiter can be enabled. The TX limiter will be automatically disabled.

10.44. Flow Control

The task of the Flow Control function is to prevent an overflow of the packet buffers in the switch by signalling the connected devices to stop sending. This is done in half-duplex mode by simulating a collision or in full-duplex mode by sending special 'pause' packets.

The flow control function is deactivated by default because the switch has enough packet buffer to store load peaks without loss. The flow control function can be enabled if necessary (but is not recommended as otherwise network blockages can occur due to faulty end devices).

Furthermore the current Flow Control state can be indicated in WEB, Telnet and NEXMAN:

Flow Control State	
Designation	**Function**
NOT ACTIVE	Flow Control is not active
ACTIVE	Flow Control is active

NOTE:
For ports in full-duplex operation the Flow Control feature is activated only if the switch and the connected terminal unit are set to {Autoneg}. This also applies to Gigabit fiber-optic ports, since here Autonegotiation is used, too.

10.45. Layer-2 Discovery Functios

10.45.1. Periodic Transmission of Life and Autodiscover Packets

The Life Packet function sends IP broadcast packets to the management VLAN in periodic intervals. Sending of packets is activated as soon as the switch has obtained a valid IP address via DHCP or when a fixed IP address has been specified.

This function is useful, e.g. when the central switch has selected an automatic IP-based VLAN configuration. The periodic transmission of Life Packets prevents the central switch from forgetting the management VLAN, because it has not seen the IP address of the Nexans switch for too long.

The interval between the Life Packets can be set as follows:
- 1 minute (factory default)
- 10 minutes
- 1 hour
- 10 hours
- Disable Life Packets
- Disable Life and Autodiscover Packets

If “Disable Life Packets” is selected, no Life Packets are sent. If the „Disable Life and Autodiscover Packets” setting is used, neither Life nor Autodiscover packets are sent. The result is that the switch cannot be found via Layer 2, but only via Layer 3 Autodiscover.

10.45.2. Disable Basic Configurator

By disabling the basic configurator function on the switch the reading as well as the writing via basic configurator will be disabled.

10.46. Function Inputs for Industrial and Office Switches

Industrial switches may have one or more function inputs. Depending on the version, Office switches may have a single function input next to the power supply input.

Depending on the type of switch, the function inputs have an internal or external auxiliary voltage.
Internal auxiliary voltage:
Here it is sufficient to short-circuit the two terminals of the functional input via an external switch (eg door contact). The shorted state is then considered "active", and the open state is considered "inactive".
External auxiliary voltage:
In this case, the input must be supplied with a voltage so that it is regarded as "active". For this either the auxiliary voltage provided by the switch can be used or a customer's source of voltage.

The function inputs can be used to trigger the following actions:
• Switching the local alarm outputs (Config via Alarm Output Mode)
• Switching the alarm outputs of another switch (Cnfig via Function Input Alarm Mode / Alarm Output Mode)
• Delete all local inactive alarms of the alarm outputs (Config via Function Input Alarm Mode)
• Sending an alarm via SNMP trap, remote syslog or local logging (Config via Alarm Destination Table)

10.46.1. Function Input Alarm Mode

The switching of the alarm outputs of another switch can be configured via the "Function Input Alarm Mode" and requires on the opposite side a Nexans Industrial Switch with corresponding alarm outputs. The prerequisite is that the desired alarm output for the Remote Switch is configured to the "Function Input from Remote Switch" mode. Furthermore, the same "Alarm Group" must be entered on both sides and both switches must be in the same VLAN or LAN segment as the data exchange takes place at Layer-2 level.

NOTE: A function input can trigger multiple alarm outputs from different remote switches simultaneously, provided that all alarm outputs are assigned to the same "Remote Alarm Group".

Furthermore, active alarms of the local alarm outputs can be cleared via the function inputs.

The following modes can be selected for the Alarm mode:
- Disabled
- Send Alarm when Function Input shorted
- Send Alarm when Function Input shorted / Clear Alarm when re-opened
- Send Alarm when Function Input open
- Send Alarm when Function Input open / Clear Alarm when re-shorted
- Clear all active Output Alarm when Function Input opened
- Clear all active Output Alarm when Function Input shorted

Disabled:
The function is switched off.

Send Alarm when Function Input shorted:
The alarm contact of the remote switch is triggered when the local input becomes active. After the input becomes inactive again, the alarm contact on the remote switch remains in the alarm state but is marked as inactive in the managemet. This must then be cleared manually on the remote switch via the management command "Clear Alarm" or a function input of the remote switch (see below).

Send Alarm when Function Input shorted / Clear Alarm when re-opened:
The alarm contact of the remote switch is triggered as soon as the local input is active. If the input becomes inactive again, the alarm is also cleared on the remote switch.

Send Alarm when Function Input shorted:
Here it is assumed that the function input is active in the normal state. The alarm contact of the remote switch is triggered here as soon as the input becomes inactive. After the input becomes active again, the alarm contact on the remote switch remains in the alarm state, but is marked as inactive in the managemet. This must then be cleared manually on the remote switch via the management command "Clear Alarm" or a function input of the remote switch (see below).

Send Alarm when Function Input open / Clear Alarm when re-shorted:
Here it is assumed that the function input is active in the normal state. The alarm contact of the remote switch is triggered here as soon as the input becomes inactive. If the input becomes active again, the alarm is also cleared on the remote switch.

Clear all active Output Alarm when Function Input opened:
When the function input becomes inactive, all inactive alarms of the local alarm contacts are cleared.

Clear all active Output Alarm when Function Input shorted:
When the function input becomes active, all inactive alarms of the local alarm contacts are cleared.

10.47. Alarm Outputs for Industrial Switches

The Nexans industrial switches provide two potential-free alarm outputs designated as M1 and M2.

The following modes can be set for each of the outputs:
- Link Down
- Forced On
- Forced Off
- Function Input from Remote Switch
- Alarm Destination from Remote Switch
- Alarm Destination from Local Switch

The following modes are only supported for some types of industrial switches only:
- Power Input S1 failed
- Power Input S2 failed
- Power Input S1 or S2 failed
- Function Input shorted
- Function Input open

Link Down:
Here the alarm output is enabled, when the link of one or more ports fails. Via the parameters 'Link Down Alarm M1' and 'Link Down Alarm M2' it is possible to separately specify for each port, whether a link failure of the respective port shall initiate an alarm on output M1 or M2:

Forced On:
The alarm output is permanently enabled {On}.

Forced Off:
The alarm output is permanently disabled {Off}.

For example, the **Forced On** and **Forced Off** functions can be used for systematically driving actuators.

Function Input from Remote Switch:
With this setting the alarm output is controlled depending on the functional input of another Nexans industrial switch. The precondition is that the functional input has been configured accordingly and been assigned to the same remote group. Moreover, the two switches have to be in the same VLAN and/or segment, because the data is exchanged on layer 2.

Alarm Destination from Remote Switch:
With this setting the alarm output is controlled depending on the ‘Alarm Destination Table’ of another Nexans switch (may also be an Office switch). As a precondition the ‘Destination Type’ in the ‘Alarm Destination Table’ must be set to ‘Remote Alarm Output M1/M2’ and the correct IP address entered there. The two switches may be situated in different VLANs because the data is exchanged on layer 3.

Alarm Destination from Local Switch:
In this case the alarm output is controlled depending on its own ‘Alarm Destination Table’. As a precondition the ‘Destination Type’ in the ‘Alarm Destination Table’ must be set to ‘Local Alarm Output M1/M2’. The IP address entered there will be ignored.

Power Input S1 failed:
In the case of a voltage loss on power input S1 the alarm output will be enabled.

Power Input S2 failed:
In the case of a voltage loss on power input S2 the alarm output will be enabled.

Power Input S1 or S2 failed:
In the case of a voltage loss on power input S1 or S2 the alarm output will be enabled.

Function Input shorted:
In the case of a aktiv function input the alarm output will be enabled.

Function Input open:
In the case of an inactive function input the alarm output will be enabled.

10.48. Telnet Console Authentication Mode

Six different authentication modes can be selected for Telnet:

- Local: Local authentication
- Telnet disabled: Telnet interface disabled
- Radius only: Authentication through the RADIUS server only
- Radius first, then local: Authentication through RADIUS. If no server response, local authentication.
- TACACS+ only: Authentication through the TACACS+ server only
- TACACS+ first, then local: Authentication through TACACS+. If no server response, local authentication.

Local (factory default):
A name and password each for Admin and User access is stored in the switch (see chapter *10.5. Admin/User Accounts for Management*). They are the factory default data for authentication during Telnet login and will be compared with the entered login name and login password.

Telnet disabled:
The Telnet interface is disabled. The switch will reject any connection setup on the Telnet TCP port.

Radius Only:
Radius first, then local:
These modes are only supported by firmware versions with RADIUS functionality. See chapter *10.56. RADIUS Console Authentication Mode*.

TACACS+ Only:
TACACS+ first, then local:
These modes are only supported by firmware versions with TACACS+ functionality. See chapter *10.64 TACACS+ Console Authentication Modes*.

NOTE:

When the user enters the wrong name or password three times, all Console interfaces (SSH, TELNET and V.24) will be locked for 60 seconds.

10.49. SSHv2 Console Authentication Mode

Six different authentication modes can be selected for SSHv2:

- Local: Local authentication
- SSHv2 disabled: SSHv2 interface disabled
- Radius only: Authentication through the RADIUS server only
- Radius first, then local: Authentication through RADIUS. If no server response, local authentication.
- TACACS+ only: Authentication through the TACACS+ server only
- TACACS+ first, then local: Authentication through TACACS+. If no server response, local authentication.

Local (factory default):
A name and password each for Admin and User access is stored in the switch (see chapter *10.5. Admin/User Accounts for Management*). They are the factory default data for authentication during SSHv2 login and will be compared with the entered login name and login password.

SSHv2 disabled:
The SSHv2 interface is disabled. The switch will reject any connection setup on the SSHv2 TCP port.

Radius Only:
Radius first, then local:
These modes are only supported by firmware versions with RADIUS functionality. See chapter *10.56. RADIUS Console Authentication Mode*.

TACACS+ Only:
TACACS+ first, then local:

These modes are only supported by firmware versions with TACACS+ functionality. See chapter *10.64 TACACS+ Console Authentication Modes*.

NOTE:

When the user enters the wrong name or password three times, all Console interfaces (SSH, TELNET and V.24) will be locked for 60 seconds.

10.50. SCP Authentication Mode

Seven different authentication modes can be selected for SCP:

- Local — Local authentication
- Radius only — Authentication through the RADIUS server only
- Radius first, then local — Authentication through RADIUS. If no server response, local authentication.
- TACACS+ only — Authentication through the TACACS+ server only
- TACACS+ first, then local — Authentication through TACACS+. If no server response, local authentication.
- Use SSHv2 mode — The SSHv2 authentication mode will be used
- Disabled — SCP Interface disabled

Local:
A name and password each for Admin and User access is stored in the switch (see chapter *10.5. Admin/User Accounts for Management*). They are the factory default data for authentication during SCP login and will be compared with the entered login name and login password.

Disabled:
The SCP interface is disabled. The switch will reject any connection setup on the SCP TCP port.

Radius only:
Radius first, then local:
These modes are only supported by firmware versions with RADIUS functionality. See chapter *10.58 RADIUS SCP Authentication Modes*.

TACACS+ only:
TACACS+ first, then local:
These modes are only supported by firmware versions with TACACS+ functionality. See chapter *10.66 TACACS+ SCP Authentication Modes*.

Use SSHv2 mode (Factory-Default):
The configured SSHv2 Console Authentication Mode will be used.

10.51. Console Password Mode

The Console Password Mode can be used to specify whether the console password shall be displayed or not upon entry. This is quite useful, e.g. when one-time passwords are used with RADIUS servers and the entered password can only be used once.

The following settings are possible:
- Invisible (Default)
- Visible

10.52. Statistic / RMON Counters

Via NEXMAN, Telnet/SSH/V.24 console and SNMP comprehensive Statistic Counters per port can be displayed.

The following counters are supported:
- Rx Unicast Pkts (*)
- Rx Broadcast Pkts (*)
- Rx Multicast Pkts (*)
- Rx FCS Error Pkts (*)
- Rx Align Error Pkts
- Rx Good Octets (*)

- Rx Fragment Pkts
- Rx Discards Pkts
- Rx Bad Octets
- Rx Undersized Pkts
- Rx Jabber
- Rx Oversize Pkts
- Rx Bad Octets
- Tx Unicast Pkts
- Tx Broadcast Pkts
- Tx Multicast Pkts
- Tx Octets (*)
- Tx Collisions
- Tx Late Collisions (*)
- Tx Single Collisions
- Tx Multiple Collisions
- Tx Excessive Collisions
- Rx 0-64 Oct. Pkts
- Rx 65-127 Oct. Pkts
- Rx 128-255 Oct. Pkts
- Rx 256-511 Oct. Pkts
- Rx 512-1023 Oct. Pkts
- Rx 1024-1536 Oct. Pkts
- Tx 0-64 Oct. Pkts
- Tx 65-127 Oct. Pkts
- Tx 128-255 Oct. Pkts
- Tx 256-511 Oct. Pkts
- Tx 512-1023 Oct. Pkts
- Tx 1024-1536 Oct. Pkts

The counters marked with an (*) are implemented in 64 bit. An overflow of these counters can virtually be excluded. The 64-bit value is returned on all management interfaces, incl. the SNMP High-Capacity-Counter.

Via SNMP the counters can be requested via the following standard MIBs:

- MIB-II: interfaces
- IF-MIB: ifXTable
- BRIDGE-MIB: dot1dTpPortTable
- EtherLike-MIB: dot3StatsTable
- RMON-MIB: statistics

Chapter *0*

List of SNMP MIBs contains a detailed summary of all SNMP-MIBs.

10.53. SNMP Support

10.53.1. SNMP Protocol Version

This allows you to define the SNMP protocols used to access the SNMP-MIB of the switches.

For the SNMP Protocol Version the following settings are available:

- SNMPv1
- SNMPv2c
- SNMPv1 and SNMPv2c
- SNMPv3[Auth.-MD5][No Priv.]
- SNMPv3[Auth.-MD5][Priv.-DES.]
- SNMPv3[Auth.-MD5][Priv.-AES-128.]
- SNMPv3[Auth.-SHA][No Priv.]
- SNMPv3[Auth.-SHA][No Priv.] with SNMPv1/SNMPv2c read/only access
- SNMPv3[Auth.-SHA][Priv.-DES.]

- SNMPv3[Auth.-SHA][Priv.-AES-128.]
- SNMPv3[Auth.-SHA][Priv.-AES-128.] with SNMPv1/SNMPv2c read/only access

SNMPv1:
Access to the SNMP-MIB is allowed via SNMP Version 1 only. For authentication the community of the packet will be analysed and checked.

SNMPv2c:
Access to the SNMP-MIB is allowed via SNMP Version 2c only. For authentication the community of the packet will be analysed and checked.

SNMPv1 and SNMPv2c:
Access to the SNMP-MIB is allowed via SNMP Version 1 and Version 2c. For authentication the community of the packet will be analysed and checked.

SNMPv3[Auth.-MD5][No Priv.]:
Access to the SNMP-MIB is allowed via SNMP Version 3 only. For authentication the Username and MD5 Password Hash of the packet are analysed and checked. No encryption of the data is performed.

SNMPv3[Auth.-MD5][Priv.-DES]:
SNMPv3[Auth.-MD5][Priv.-AES-128]:
Access to the SNMP-MIB is allowed via SNMP Version 3 only. For authentication the Username and MD5 Password Hash of the packet are analysed and checked. The encryption of the data is performed by DES ord AES

SNMPv3[Auth.-SHA][No Priv.]:
Access to the SNMP-MIB is allowed via SNMP Version 3 only. For authentication the Username and SHA Password Hash of the packet are analysed and checked. No encryption of the data is performed.

SNMPv3[Auth.-SHA][Priv.-DES]:
SNMPv3[Auth.-SHA][Priv.-AES-128]:

Access to the SNMP-MIB is allowed via SNMP Version 3 only. For authentication the Username and SHA Password Hash of the packet are analysed and checked. The encryption of the data is performed by DES or AES.

SNMPv3[Auth.-SHA][No Priv.] with SNMPv1/SNMPv2c read/only access:
SNMPv3[Auth.-SHA][Priv.-AES-128] with SNMPv1/SNMPv2c read/only access:
This setting allows read and write access for SNMPv3 and simultaneously read-only access for SNMPv1 and SNMPv2c. This allows you, for example, to change parameters via the secure SNMPv3 protocol while the query of parameters can be performed via the less complex SNMPv1 or SNMPv2c protocols.

10.53.2. SNMP Access Mode

The following modes can be selected for SNMP access:
- Read/Write: Read/Write access allowed
- Read/Only Read/Only access allowed
- SNMP disabled: SNMP Interface disabled

Read/Write (factory default):
This setting provides read and write access via SNMP.

Read/Only:
Here only read access via SNMP is allowed.

SNMP disabled:
The SNMP interface is disabled.

10.53.3. SNMPv1/v2c Communities

Access via SNMPv1 and SNMPv2c is possible with any standard SNMP manager. The read/write and read/only communities will be read accordingly and have to be set correctly at the SNMP manager station. If a wrong parameter is entered for the community, the switch will report the error No Such Name or Read/Only.

The default values for the communities are:

- Read/Only Community: public
- Read/Write Community: nexans
- Trap Community: public (if empty, the Read/Only community will be used instead)

The following ASCII characters are allowed for the community names and are checked in WEB, CLI and Manager input masks:

a-z A-Z 0-9 . , ; ! " ' % # $ & ^ ~ @ * : + - = _ / \ | ( ) [ ] { } < >

The only exceptions are the following not supported ASCII characters:

? (ASCII 63) Can't be used because in CLI console “?” is always interpreted as help command

` (ASCII 96) User must press keys <shift + `> + <space> to enter this character, which is not practical

10.53.4. SNMPv1 MAC Table Mode

The following modes can be selected for the SNMP MAC Table mode:

- List MAC's of all ports: The MACs of all ports are listed.
- List only MAC's of user ports Only the MACs of the user ports are listed.

By factory default this parameter is set to 'List MAC's of all ports'. If this setting is configured to 'List only MAC's of user ports', the SNMP MAC table will list only MAC addresses located on the user ports. Via the 'Link type' setting you can define which ports are 'User Ports' or 'Uplink Ports'. By factory default the fiber ports are configured as uplink ports and the other ports as user ports.

NOTE: This setting is relevant to SNMPv1 access only. For SNMPv2c and SNMPv3 the ‘List MAC's of all port’ mode is principally used.

10.53.5. SNMPv3 Engine ID

The SNMPv3 Engine ID is part of the SNMPv3 network protocol and is used to indentify the switch agent against the SNMP manager. This ID can be configured manually via the “Engine ID” configuration parameter in HEX notation.

If the Engine ID parameter is empty the switch uses an automatically generated and unique MAC based ID with the following syntax (in HEX notation):
8000010A03xxxxxxxxxx
With the following parts:
8000 (SNMPv3 protocol indentification)
010A (Nexans Enterprise ID)
03 (Use MAC address scheme)
xxxxxxxxxx (Switch MAC address, six HEX bytes)

10.53.6. SNMPv3 User Setup

Via SNMPv3 User Setup the user names and passwords for SNMP authentication can be configured.

Here three user accounts are available:

- Read/Write User Account: Full read/write access to the MIB
- Read/Only User Account: Read/only access to the MIB
- Flexible User Account: You can choose between Read/Write or Read/Only Access to the MIB
- Trap User Account: Will be used zp send SNMPv3 Traps.

For each account one username and password can each be defined. By default these accounts are empty, i. e. no access via SNMPv3 is possible using the factory default settings.

The following ASCII characters are allowed for Usernames and Passwords and are checked in WEB, CLI and Manager input masks:

a-z A-Z 0-9 . , ; ! " ' % # $ & ^ ~ @ * : + - = _ / \ | ( ) [ ] { } < >

The only exceptions are the following not supported ASCII characters:

? (ASCII 63) Can't be used because in CLI console "?" is always interpreted as help command

` (ASCII 96) User must press keys <shift + `> + <space> to enter this character, which is not practical

10.53.7. List of SNMP MIBs

The below list indicates all implemented MIBs and the supported groups. The individual variables of the MIBs have not been listed, can, however, be found in the respective MIB files.

NOTE:
The below MIBs are partly contained in the zip archive of the update file (see column 1).

Two MIB files are relevant to Nexans switches:
- ***NEXANS-MIB.mib*** - Global MIB for all Nexans products
- ***NEXANS-BM-MIB.mib*** - product-specific MIB for Nexans office and industrial switches

a) Designation b) Filename	RFC	MIB OID
a) NEXANS-MIB **NEXANS-BM-MIB** b) NEXANS-MIN.mib NEXANS-BM-MIB.mib		iso(1).org(3).dod(6).internet(1).. ..private(4) enterprises(1) nexansActiveNetworkingSystems(266) bmSwitchMIB (20) bmTraps(0) switchOverTemperature(1) portLinkChange(2) portNewMacAddress(3) portSecurityFailure(4) portErrorCountFailure(5) switchMgmtAuth(6) radiusMgmtAuthReject(7) radiusPortSecurityReject(8) switchPoeVoltageFailure(10) switchPoeOverloadFailure(11) portPoeOverloadFailure(12) portActiveLoopDetectionFailure(13) switchIndustrialAlarmM1(14) switchIndustrialAlarmM2(15) switchInternalVoltageFailure(16) tftpMessage(17) sfpEvent(18) clientRemoved(19) internalMgmtWarning(20) switchFunctionInputAlarm(21) switchConfigurationChanged(22) portErrorDisabled(23) bmSwitchInfo(1) infoDescr(1) infoType(2) infoProductNo(3)

		infoSerie(4) infoSeriesNo(5) infoManufactureDate(6) infoSwitchHardwareVersion(7) infoMgmtHardwareVersion(8) infoMgmtFirmwareVersion(9) infoNoOfPorts(10) infoNoOfReboots(11) infoTemperature(12) infoTemperatureMaxAllowed(13) infoPowerVoltage2500(14) infoPowerVoltage3300(15) infoMgmtAuth(16) infoSecurityFailMacAddr(17) infoNewMacAddr(18) infoPoeInputVoltage(19) infoPoeInputPower(20) infoAlarmStateM1(21) infoAlarmStateM2(22) infoLastTftpMessage(23) infoLastSfpEventMessage(24) infoLastInternalMgmtWarning(25) infoFunctionInputStateF1(26) infoTotalConfigChanges(27) infoLastSourceInterface(28) infoLastPortStateChangeSource(29) infoFunctionInputStateF2(30) infoFunctionInputStateF3(31) infoFunctionInputStateF4(32) infoLastFuncInputAlarmNumber(33) infoLastFuncInputAlarmState(34) infoLastFuncInputAlarmName(35) infoConfigChanged(36) infoS1InputVoltage(37) infoS2InputVoltage(38) infoLastSntpTime(39) infoCfgDefaultSize(40) infoCfgDefaultChecksum(41) infoCfgRebootSize(42) infoCfgRebootChecksum(43) infoMCFirmware(44) bmSwitchAdmin(2) adminReset(1) adminAgentDhcp(2) adminAgentIpAddress(3) adminAgentPhysAddress 4) adminAgentDefRouterIpAddress(5) adminAgentNetmask(6) adminAgentDhcpServerIpAddress(7) adminAgentVlanId(8) adminAgentPrioValue(9) adminAddrAgingTimeMinutes(10) adminSwitchPortMirror(11) adminMgmtAccessList(12)

		adminSwitchPoEPowerLimit(13) adminSwitchVlanTableMode(14) adminUnsecureVlanId(15) adminDot1xAuthFailureVlanId(16) adminTftpAccess(17) adminSnmpMacTableMode(18) adminAlarmM1(19) adminAlarmM2(20) adminMemoryCardMode(21) adminAlarmNameM1(22) adminAlarmNameM2(23) adminFunctionInputNameF1(24) adminLedGlobalMode(25) adminFunctionInputNameF2(26) adminFunctionInputNameF3(27) adminFunctionInputNameF4(28) bmSwitchPort(3) bmSwitchPortTable(1) bmSwitchPortEntry(1) portIndex(1) portDescr(2) portName(3) portAdminState(4) portSpeedDuplexSetup(5) portLinkState(6) portErrorCounter(7) portRemoteFault(8) portDefaultVlanId(9) portTrunkingMode(10) portDot1qDefaultPrioValue(11) portDefaultPrioQueue(12) portLEDGreen(13) portLEDYellow(14) portBandwidthLimitRxd(15) portBandwidthLimitTxd(16) portSecurityAdminState(17) portSecurityMacAddr1(18) portSecurityMacAddr2(19) portSecurityMacAddr3(20) portPoeAdminState(21) portPoeVoltage(22) portPoeCurrent(23) portPoePower(24) portSecurityForwardingState(25) portPoePowerLimit(26) portLimiterPacketType(27) portAcApSetup(28) portLinkType(29) portVoiceVlanId(30) portPrioDot1p(31) portPrioIp(32) portActiveDefaultVlanId(33) portActiveVoiceVlanId(34) portPrioOverride(35) bmSwitchVlan(4)

		bmSwitchVlanTable(1) bmSwitchVlanEntry(1) vlanIndex(1) vlanId(2) vlanDescr(3) vlanPrioOverride(4) bmSwitchSfp(5) bmSwitchSfpTable(1) bmSwitchSfpEntry(1) sfpPortIndex(1) sfpState(2) sfpInfoVendorName(3) sfpInfoPartNumber(4) sfpInfoRevisionNumber(5) sfpInfoSerialNumber(6) sfpInfoDateCode(7) sfpInfoBitRate(8) sfpInfoWavelenght(9) sfpInfoLenght9um(10) sfpInfoLenght50um(11) sfpInfoLenght62um(12) sfpInfoConnectorDescr(13) sfpDiagTemperature(14) sfpDiagSupplyVoltage(15) sfpDiagTxBiasCurrent(16) sfpDiagTxOutputPower(17) sfpDiagTxOutputPowerDbm(18) sfpDiagRxIntputPower(19) sfpDiagRxInputPowerDbm(20) sfpAlarmTxBiasCurrentUpperLimit(21) sfpAlarmTxOutputPowerLowerLimit(22) sfpAlarmRxInputPowerLowerLimit(23) bmSwitchAlarmDest(6) bmSwitchAlarmDestSyslogSeverities(1) alarmSyslogSeverityColdStart(1) alarmSyslogSeverityMgmtAuth(2) alarmSyslogSeverityTemperatureFailure(3) alarmSyslogSeverityPortLinkChange(4) alarmSyslogSeverityPortNewMacAddress(5) alarmSyslogSeverityPortSecurityFailure(6) alarmSyslogSeverityPortErrorCounter(7) alarmSyslogSeverityPoeFailureSwitchVoltage(9) alarmSyslogSeverityPoeFailureSwitchOverload(10) alarmSyslogSeverityPoeFailurePortOverload(11) alarmSyslogSeverityRadiusMgmtAuth(12) alarmSyslogSeverityRadiusPortSecurityFailure(13) alarmSyslogSeverityPortLinkUp(14) alarmSyslogSeverityPortLinkDown(15) alarmSyslogSeverityPortBcastFailure(16) alarmSyslogSeverityPortLoopDetected(17) alarmSyslogSeverityIndustrialAlarmM1(18) alarmSyslogSeverityIndustrialAlarmM2(19) alarmSyslogSeverityRstpNewRoot(20) alarmSyslogSeverityRstpTopologyChanged(21)

		alarmSyslogSeverityIntVoltageFailure(22) alarmSyslogSeverityTftpMessage(23) alarmSyslogSeveritySfpEvent(24) alarmSyslogSeverityClientRemoved(25) alarmSyslogSeverityIntMgmtWarning(26) alarmSyslogSeverityFunctionInput(27) alarmSyslogSeverityConfigChanged(28) alarmSyslogSeverityPortErrorDisabled(29) alarmSyslogSeverityPortStateChanged(30) bmSwitchAlarmDestTable(2) bmSwitchAlarmDestEntry(1) alarmDestIndex(1) alarmDestType(2) alarmDestIpAddress(3) alarmModeColdStart(4) alarmModeMgmtAuth(5) alarmModeTemperatureFailure(6) alarmModePortLinkChange(7) alarmModePortNewMacAddress(8) alarmModePortSecurityFailure(9) alarmModePortErrorCounter(10) alarmModePoeFailureSwitchVoltage(12) alarmModePoeFailureSwitchOverload(13) alarmModePoeFailurePortOverload(14) alarmModeRadiusMgmtAuth(15) alarmModeRadiusPortSecurityFailure(16) alarmModePortLinkUp(17) alarmModePortLinkDown(18) alarmModePortBcastFailure(19) alarmModePortLoopDetected(20) alarmModeIndustrialAlarmM1(21) alarmModeIndustrialAlarmM2(22) alarmModeRstpNewRoot(23) alarmModeRstpTopologyChanged(24) alarmModeIntVoltageFailure(25) alarmModeTftpMessage(26) alarmModeSfpEvent(27) alarmModeClientRemoved(28) alarmModeIntMgmtWarning(29) alarmModeFunctionInput(30) alarmModeConfigChanged(31) alarmModePortErrorDisabled(32) alarmModePortStateChanged(33)
a) MIB-II b) nicht enthalten	1213	iso(1).org(3).dod(6).internet(1).. ..mgmt(2) mib-2(1) system(1) sysDescr(1) sysObjectID(2) sysUpTime(3) sysContact(4) sysName(5) sysLocation(6)

		sysServices(7) interfaces(2) ifNumber (1) ifTable(2) ifEntry(1) ifIndex(1) ifDescr(2) ifType(3) ifMtu(4) ifSpeed(5) ifPhysAddress(6) ifAdminStatus(7) ifOperStatus(8) ifLastChange(9) ifInOctets(10) ifInUcastPkts(11) ifInNUcastPkts(12) ifInDiscards(13) ifInErrors(14) ifInUnknownProtos(15) ifOutOctets(16) ifOutUcastPkts(17) ifOutNUcastPkts(18) ifOutDiscards(19) ifOutErrors(20) ifOutQLen(21) ifSpecific(22) at(3) atTable(1) atEntry(1) atIfIndex(1) atPhysAddress(2) atNetAddress(3) ip(4) ipForwarding(1) ipDefaultTTL(2) ipAddrTable(20) ipAddrEntry(1) ipAdEntAddr(1) ipAdEntIfIndex(2) ipAdEntNetMask(3) ipAdEntBcastAddr(4) ipAdEntReasmMaxSize(5) ipRouteTable(21) ipRouteEntry(1) ipRouteDest(1) ipRouteIfIndex(2) ipRouteMetric1(3) ipRouteMetric2(4) ipRouteMetric3(5) ipRouteMetric4(6) ipRouteNextHop(7) ipRouteType(8) ipRouteProto(9)

		ipRouteAge(10) ipRouteMask(11) ipRouteMetric5(12) ipRouteInfo(13) ipNetToMediaTable(22) ipNetToMediaEntry(1) ipNetToMediaIfIndex(1) ipNetToMediaPhysAddress(2) ipNetToMediaNetAddress(3) ipNetToMediaType(4)
a) IF-MIB b) IFMIB.mib	2863	iso(1).org(3).dod(6).internet(1).. ..mgmt(2) mib-2(1) ifMIB(31) ifMIBObjects(1) ifXTable(1) ifXEntry(1) ifName(1) ifInMulticastPkts(2) ifInBroadcastPkts(3) ifOutMulticastPkts(4) ifOutBroadcastPkts(5) ifHCInOctets(6) ifHCInUcastPkts(7) ifHCInMulticastPkts(8) ifHCInBroadcastPkts(9) ifHCOutOctets(10) ifHCOutUcastPkts(11) ifHCOutMulticastPkts(12) ifHCOutBroadcastPkts(13) ifLinkUpDownTrapEnable(14) ifHighSpeed(15) ifPromiscuousMode(16) ifConnectorPresent(17) ifAlias(18) ifCounterDiscontinuityTime(19)
a) BRIDGE-MIB b) BRIDGE.mib	4188	iso(1).org(3).dod(6).internet(1).. ..mgmt(2) mib-2(1) dot1dBridge(17) dot1dBase(1) dot1dBaseBridgeAddress(1) dot1dBaseNumPorts(2) dot1dBaseType(3) dot1dBasePortTable(4) dot1dBasePortEntry(1) dot1dBasePort(1) dot1dBasePortIfIndex(2) dot1dBasePortCircuit(3) dot1dBasePortDelayExceededDiscards(4) dot1dBasePortMtuExceededDiscards(5) dot1dStp(2)

		dot1dStpProtocolSpecification(1) dot1dStpPriority(2) dot1dStpTimeSinceTopologyChange(3) dot1dStpTopChanges(4) dot1dStpDesignatedRoot(5) dot1dStpRootCost(6) dot1dStpRootPort(7) dot1dStpMaxAge(8) dot1dStpHelloTime(9) dot1dStpHoldTime(10) dot1dStpForwardDelay(11) dot1dStpBridgeMaxAge(12) dot1dStpBridgeHelloTime(13) dot1dStpBridgeForwardDelay(14) dot1dStpPortTable(15) dot1dStpPortEntry(1) dot1dStpPort(1) dot1dStpPortPriority(2) dot1dStpPortState(3) dot1dStpPortEnable(4) dot1dStpPortPathCost(5) dot1dStpPortDesignatedRoot(6) dot1dStpPortDesignatedCost(7) dot1dStpPortDesignatedBridge(8) dot1dStpPortDesignatedPort(9) dot1dStpPortForwardTransitions(10) dot1dStpPortPathCost32(11) dot1dTp(4) dot1dTpLearnedEntryDiscards(1) dot1dTpAgingTime(2) dot1dTpFdbTable(3) dot1dTpFdbEntry(1) dot1dTpFdbAddress(1) dot1dTpFdbPort(2) dot1dTpFdbStatus(3) dot1dTpPortTable(4) dot1dTpPortEntry(1) dot1dTpPort(1) dot1dTpPortMaxInfo(2) dot1dTpPortInFrames(3) dot1dTpPortOutFrames(4) dot1dTpPortInDiscards(5)
a) Q-BRIDGE-MIB b) Q-BRIDGE.mib	4188	iso(1).org(3).dod(6).internet(1).. ..mgmt(2) mib-2(1) dot1dBridge(17) qBridgeMIB(7) qBridgeMIBObjects(1) dot1qBase(1) dot1qVlanVersionNumber(1) dot1qMaxVlanId(2) dot1qMaxSupportedVlans(3) dot1qNumVlans(4)

		dot1qGvrpStatus(5) dot1qTp(2) dot1qFdbTable(1) dot1qFdbEntry(1) dot1qFdbId(1) dot1qFdbDynamicCount(2) dot1qTpFdbTable(2) dot1qTpFdbEntry(1) dot1qTpFdbAddress(1) dot1qTpFdbPort(2) dot1qTpFdbStatus(3) dot1qVlan(4) dot1qVlanNumDeletes(1) dot1qVlanCurrentTable(2) dot1qVlanCurrentEntry(1) dot1qVlanTimeMark(1) dot1qVlanIndex(2) dot1qVlanFdbId(3) dot1qVlanCurrentEgressPorts(4) dot1qVlanCurrentUntaggedPorts(5) dot1qVlanStatus(6) dot1qVlanCreationTime(7) dot1qVlanStaticTable(3) dot1qVlanStaticEntry(1) dot1qVlanStaticName(1) dot1qVlanStaticEgressPorts(2) dot1qVlanForbiddenEgressPorts(3) dot1qVlanStaticUntaggedPorts(4) dot1qVlanStaticRowStatus(5) dot1qNextFreeLocalVlanIndex(4) dot1qPortVlanTable(5) dot1qPortVlanEntry(1) dot1qPvid(1) dot1qPortAcceptableFrameTypes(2) dot1qPortIngressFiltering(3) dot1qPortGvrpStatus(4) dot1qPortGvrpFailedRegistrations(5) dot1qPortGvrpLastPduOrigin(6)
a) RSTP-MIB b) RSTP.mib	4318	iso(1).org(3).dod(6).internet(1).. ..mgmt(2) mib-2(1) dot1dBridge(17) dot1dStp(1) dot1dStpVersion(16) dot1dStpTxHoldCount(18) dot1dStpExtPortTable(19) dot1dStpExtPortEntry(1) dot1dStpPortProtocolMigration(1) dot1dStpPortAdminEdgePort(2) dot1dStpPortOperEdgePort(3) dot1dStpPortAdminPointToPoint(4) dot1dStpPortOperPointToPoint(5) dot1dStpPortAdminPathCost(6)

a) EtherLike-MIB b) ETHERLIKE.mib	2665	iso(1).org(3).dod(6).internet(1).. ..mgmt(2) mib-2(1) transmission(10) dot3(7) dot3StatsTable(2) dot3StatsEntry(1) dot3StatsIndex(1) dot3StatsAlignmentErrors(2) dot3StatsFCSErrors(3) dot3StatsSingleCollisionFrames(4) dot3StatsMultipleCollisionFrames(5) dot3StatsSQETestErrors(6) dot3StatsDeferredTransmissions(7) dot3StatsLateCollisions(8) dot3StatsExcessiveCollisions(9) dot3StatsInternalMacTransmitErrors(10) dot3StatsCarrierSenseErrors(11) dot3StatsFrameTooLongs(13) dot3StatsInternalMacReceiveErrors(16) dot3StatsEtherChipSet(17) dot3StatsSymbolErrors(18) dot3StatsDuplexStatus(19)
a) RMON-MIB b) RMON.mib	2819	iso(1).org(3).dod(6).internet(1).. ..mgmt(2) mib-2(1) rmon(16) statistics(1) etherStatsTable(1) etherStatsEntry(1) etherStatsIndex(1) etherStatsDataSource(2) etherStatsDropEvents(3) etherStatsOctets(4) etherStatsPkts(5) etherStatsBroadcastPkts(6) etherStatsMulticastPkts(7) etherStatsCRCAlignErrors(8) etherStatsUndersizePkts(9) etherStatsOversizePkts(10) etherStatsFragments(11) etherStatsJabbers(12) etherStatsCollisions(13) etherStatsPkts64Octets(14) etherStatsPkts65to127Octets(15) etherStatsPkts128to255Octets(16) etherStatsPkts256to511Octets(17) etherStatsPkts512to1023Octets(18) etherStatsPkts1024to1518Octets(19) etherStatsOwner(20) etherStatsStatus(21) etherStatsBadOctets(22)

a) ENTITY-MIB b) ENTITY-MIB.mib	6933	iso(1).org(3).dod(6).internet(1).. ..mgmt(2) mib-2(1) entityMIB(47) entityMIBObjects(1) entityMIBObjects(1) entPhysicalTable(1) EntPhysicalEntry(1) entPhysicalIndex(1) entPhysicalDescr(2) entPhysicalVendorType(3) entPhysicalContainedIn(4) entPhysicalClass(5) entPhysicalParentRelPos(6) entPhysicalName(7) entPhysicalHardwareRev(8) entPhysicalFirmwareRev(9) entPhysicalSoftwareRev(10) entPhysicalSerialNum(11) entPhysicalMfgName(12) entPhysicalModelName(13) entPhysicalAlias(14) entPhysicalAssetID(15) entPhysicalIsFRU(16) entPhysicalMfgDate(17) entPhysicalUris(18) entPhysicalUUID(19)
a) SNMP-FRAMEWORK-MIB b) SNMP-FRAMEWORK.mib	3411	iso(1).org(3).dod(6).internet(1).. ..snmpV2(6) snmpModules(3) snmpFrameworkMIB(10) snmpFrameworkMIBObjects(2) snmpEngine(1) snmpEngineID(1) snmpEngineBoots(2) snmpEngineTime(3) snmpEngineMaxMessageSize(4)
a) LLDP-MIB b) LLDP.mib		iso(1).std(0).iso8802(8802).ieee802dot1(1).ieee802dot1mibs(1).. ..lldpMIB(2) lldpObjects(1) lldpConfiguration(1) lldpMessageTxInterval(1) lldpMessageTxHoldMultiplier(2) lldpReinitDelay(3) lldpTxDelay(4) lldpNotificationInterval(5) lldpPortConfigTable(6) lldpPortConfigEntry(1) lldpPortConfigPortNum(1) lldpPortConfigAdminStatus(2) lldpPortConfigNotificationEnable(3) lldpPortConfigTLVsTxEnable(4) lldpConfigManAddrTable(7) lldpConfigManAddrEntry(1) lldpConfigManAddrPortsTxEnable(1) lldpLocalSystemData(3) lldpLocChassisIdSubtype(1) lldpLocChassisId(2) lldpLocSysName(3) lldpLocSysDesc(4)

		lldpLocSysCapSupported(5) lldpLocSysCapEnabled(6) lldpLocPortTable(7) lldpLocPortEntry(1) lldpLocPortNum(1) lldpLocPortIdSubtype(2) lldpLocPortId(3) lldpLocPortDesc(4) lldpLocManAddrTable(7) lldpLocManAddrEntry(1) lldpLocManAddrSubtype(1) lldpLocManAddr(2) lldpLocManAddrLen(3) lldpLocManAddrIfSubtype(4) lldpLocManAddrIfId(5) lldpLocManAddrOID(6) lldpRemoteSystemsData(4) lldpRemTable(1) lldpRemEntry(1) lldpRemTimeMark(1) lldpRemLocalPortNum(2) lldpRemIndex(3) lldpRemChassisIdSubtype(4) lldpRemChassisId(5) lldpRemPortIdSubtype(6) lldpRemPortId(7) lldpRemPortDesc(8) lldpRemSysName(9) lldpRemSysDesc(10) lldpRemSysCapSupported(11) lldpRemSysCapEnabled(12) lldpRemManAddrTable(1) lldpRemManAddrEntry(1) lldpRemManAddrSubtype(1) lldpRemManAddr(2) lldpRemManAddrIfSubtype(3) lldpRemManAddrIfId(4) lldpRemManAddrOID(5)
a) LLDP-EXT-MED-MIB b) LLDP-MED.mib		iso(1).std(0).iso8802(8802).ieee802dot1(1).ieee802dot1mibs(1).. ..lldpMIB(2) lldpObjects(1) lldpExtensions(4) lldpXMedMIB(4795) lldpXMedObjects(1) lldpXMedRemoteData(3) lldpXMedRemInventoryTable(3) lldpXMedRemInventoryEntry(1) lldpXMedRemHardwareRev(1) lldpXMedRemFirmwareRev(2) lldpXMedRemSoftwareRev(3) lldpXMedRemSerialNum(4) lldpXMedRemMfgName(5) lldpXMedRemModelName(6)

		`lldpXMedRemAssetID(7)`

10.54. Alarm Destination Table

In the Alarm Destination Table up to eight alarm receivers can be entered. For each receiver it is possible to separately select the relevant alarm types.

You can individually set for each receiver which of the following destination types shall be used:

- SNMPv1 Trap
- SNMPv2 Trap
- SNMPv3 Trap
- SYSLOG Server
- Local Logging
- Remote Alarm Output M1
- Remote Alarm Output M2

The following destination types are available for industrial switches only:

- Local Alarm Output M1
- Local Alarm Output M2

SNMPv1 Trap:
SNMPv2 Trap:
Transmits an SNMPv1 and SNMPv2 Trap respectively to the configured IP address.

SNMPv3 Trap:
Transmits an SNMPv3 trap to the configured IP address. The precondition is that the SNMP Protocol Version is set to SNMPv3 and a matching Trap Account (Username and Password) is set.
Important note: With pure SNMPv3 trap receivers it might be necessary to enter the so-called SNMPv3 Engine ID of the switch in the trap receiver, in order to allow the received traps to be decrypted. If the SNMP Protocol Version is set to SNMPv3, the SNMPv3 Engine ID can be displayed using the "`show configuration access`" or "`show run`" CLI command (see chapter "ACCESS SNMP" in the CLI issue).

SYSLOG Server:
Transmits a SYSLOG message to the configured IP address. The SYSLOG Severity can be set separately for each alarm type. Furthermore, the syslog facility can be configured between 1 and 31. The following data is defined in RFC 3164:

0 kernel messages
1 user-level messages
2 mail system
3 system daemons
4 security/authorization messages
5 messages generated internally by syslogd
6 line printer subsystem
7 network news subsystem
8 UUCP subsystem
9 clock daemon
10 security/authorization messages
11 FTP daemon
12 NTP subsystem
13 log audit
14 log alert
15 clock daemon
16 local0
17 local1
18 local2
19 local3
20 local4
21 local5
22 local6
23 local7

Local Logging:
With this function alarms are stored in the local log. This log can store approximately 500 - 1000 alarms, depending on the length of the alarm texts. The **Local Logging Mode** can be used to define whether the oldest entries shall be overwritten in case of overflow or whether the logging shall be stopped. Moreover, local logging can be disabled globally.

The log can be displayed via WEB, Telnet/SSH/V.24-Console and Manager. The Log can also be read vie SCP with the following syntax:

Windows: `pscp -scp -P 50271 <username>@<ip-address>:/log <filename>`

Linux: `scp -P 50271 <username>@<ip-address>:/log <filename>`

Remote Alarm Output M1:
Remote Alarm Output M2:
With this setting the alarm output M1 or M2 of a Nexans industrial remote switch is controlled. As a precondition the correct IP address of the remote switch needs to be set and the alarm output of the corresponding switch must be set to ‘Alarm Destination from Remote Switch‘.

Local Alarm Output M1:
Local Alarm Output M2:
This mode controls its own alarm output M1 or M2. As a precondition the alarm output needs to be set to ‘Alarm Destination from Local Switch‘. An IP address entered, if any, will be ignored.

NOTE:
The NEXMAN function "Test Traps/Syslog" on tab "SNMP+SYSLOG" or the console command '`te:st-traps-syslog`' can be used for testing the SNMP traps of the Syslog messages and of the local logging. The switch will then send a Trap or Syslog message of each event type to all valid entries in the destination Table or to the internal logbook. This allows you to verify the representation in the SNMP manager or Syslog server.

NOTE:
Only those event types are sent, which are supported by the respective switch type and by the installed firmware.

The following table contains a complete list of all event types:

Event Type	Trap Class	Trap is sent...
Cold Start	Standard Trap	Upon switch power-up or reboot. With each "Cold Start" message a "Source" is given in local log file and remote syslog messages (not for SNMP traps). Example message: Cold Start: Source= Software reboot via config buttons Cold Start: Source= Power up or Power interruption If the "Source" is marked with "Unknown", than the reset was caused by a software or hardware malfunction. In this case the "Reset Reason" shows a number which is only useful for manufacturer support. Example message: Cold Start: Source=Unknown [Reset reason=0x02000] If such a reset occurs often, please update the switch firmware to the latest firmware version first. If this doesn't solve the problem the management module must be checked in the factory.
Link Up	Standard Trap	Upon change of link from down to up on a port.
Link Down	Standard Trap	Upon change of link from up to down on a port.
RSTP New Root	Standard Trap	Upon this switch selected itself as the new root of the Spanning Tree. This happens directly after boot and if the switch didn’t receive any BPDU from a neighbour switch with a higher bridge priority for a certain time.
RSTP Topology Change	Standard Trap	Upon topology change if Rapid Spanning Tree is enabled

Temperature Failure	Enterprise Trap 1	when the switch temperature is outside the configured limits. NOTE: As long as a violation exists for any limit, this event will be sent in five-minute intervals.
Link Change	Enterprise Trap 2	Upon change of link on a port with indication of data rate and duplex mode.
New MAC Address	Enterprise Trap 3	when a new MAC address is learned on a port with enabled port security. Does not apply to the {Manual setting ...} and {IEEE802.1X allow multiple MAC addresses} modes.
Portsecurity Failure	Enterprise Trap 4	when an unauthorized MAC address is detected on a port with enabled port security (see also chapter *10.36.1. Portsecurity Failure Action)*.
Port Error Counter Failure	Enterprise Trap 5	Upon incrementing the port error counter by 2 or more within a time window of 2 seconds. NOTE: Only sent in five-minute intervals, in order to avoid an SNMP trap storm in case of massive faults.
Management Authentication Info	Enterprise Trap 6	when a station has tried to access the switch management with authentication. This info includes the IP-address, the authenticated user name, the authentication status (OK, FAILURE) and the interface over which the access was made (SSH, TELNET, V.24, WEB, SNMP, SCP or Manager). In case of an authentication failure the reason (wrong user/password for telnet/ssh/v.24, wrong community for SNMP read/write and wrong accessrights in the accesslist) is also included.
Radius Management Authentication Reject	Enterprise Trap 7	when a Telnet/SSH/V.24 console or NEXMAN login is rejected by the Radius server.
Radius Portsecurity Reject	Enterprise Trap 8	when a Portsecurity Access Request is rejected by the Radius server.
Port Broadcast Failure	Enterprise Trap 9	in case of an inadmissibly high broadcast/multicast reception on a TP user port. (> 25 packets/second for more than 10 seconds).
Switch PoE Voltage Failure	Enterprise Trap 10	when the PoE input voltage is outside the configurted limits. NOTE: This trap is exclusively supported for switches with installed PoE option.
Switch PoE Overload Failure	Enterprise Trap 11	when the PoE power limit for overall power consumption is exceeded. NOTE: This trap is exclusively supported for switches with installed PoE option.
Port PoE Overload Failure	Enterprise Trap 12	when the PoE power limit for an individual port is exceeded. NOTE: This trap is exclusively supported for switches with installed PoE option.
Port Loop Detected	Enterprise Trap 13	Upon detection of a loop between two ports by the Active Loop Protection function. This error will immediately disable the respective port.

Industrial Alarm M1	Enterprise Trap 14	Upon change of the M1 alarm state with indication of the current state (On or Off).
Industrial Alarm M2	Enterprise Trap 15	Upon change of the M2 alarm state with indication of the current state (On or Off).
Internal Voltage Failure	Enterprise Trap 16	If the two internal supply voltages of 2.5V and 3.3V are below or above the accepted threshold values. NOTE: As long as a violation exists for any voltage, this event will be sent in five-minute intervals.
TFTP Message	Enterprise Trap 17	In case of a successful or failed TFTP transfer of a configuration file. This does not apply to TFTP transfers which are directly performed by Nexans Device Manager , since these will be documented in the Manager's log book.
SFP Event	Enterprise Trap 18	Upon removal or insertion of an SFP module and upon violation of the SFP alarm limits for RX-Power, TX-Power or Laser-Bias-Current. NOTE: As long as a violation exists for at least one alarm limit, this event will be sent in five-minute intervals.
Client Remove Alarm	Enterprise Trap 19	If the terminal unit is permanently removed from the port (anti-theft protection).
Internal Management Warning	Enterprise Trap 20	In case of internal irregularities (e. g. available RAM memory too small, problems when accessing the switch engine, etc.). When receiving this warning the manufacturer’s support service should be contacted. NOTE: For certain critical conditions, this warning will be sent independent of whether it is enabled in the Destination Table or not. Some warning codes are explained below. If the reported warning code is not indicated, the manufacturer’s support service should be contacted. Code=101: The receive packet buffers of the management processor are permanently exhausted for a period of about 100 seconds. If this warning appears only occasionally, this indicates a temporarily high broadcast or multicast network load in the management VLAN. In this case the source of this high broadcast/multicast network load should be identified. Code=104: Detection of errors in the Ethernet coupling of the processor with the switching chip. If this coupling is faulty, severe errors in redundant network topologies might result. In particular, there is the risk of loops, because blocked ports are wrongly set to Forwarding. When receiving this warning the manufacturer’s support service should urgently be contacted. Code=105: A firmware update has failed. The shown value reports the reason for this: 1 or 2: The firmware file is corrupt or wrong

		3: The version of firmware is too old for that switch type.
Function Input Alarm	Enterprise Trap 21	Upon change of status of the functional input from Open to Shorted or from Shorted to Open.
Configuration Changed Info	Enterprise Trap 22	Upon change of switch configuration. This info includes the IP-address, the authenticated user name, the authentication status (OK, FAILURE) and the interface over which the access was made (SSH, TELNET, V.24, WEB, SNMP, SCP or Manager).
Port Error Disabled	Enterprise Trap 23	In case of port disabling because of an error. The reason of the disabling will be send in the alarm message.
Port State Changed	Enterprise Trap 24	By changing the Port Status from Blocking to Forwarding or reverse.

10.55. RADIUS Authentication

The switch supports the RADIUS authentication protocol according to RFC2865.

This protocol is used for the following authentication tasks in the switch:

- Telnet authentication of Name/Password
- SSHv2 authentication of Name/Password
- V.24 authentication of Name/Password
- Manager authentication of Name/Password
- MAC based portsecurity modes {RADIUS allow...}
- IEEE802.1X based portsecurity modes {IEEE802.1X …}

The following chapters provide a detailed description of the individual modes**.**

IMPORTANT:
For the authentication (Telnet, SSHv2, V24, Manager) separate RADIUS settings can be configured. However, if 'RADIUS Management Authentication Mode' is set to 'Use Global Authentication Server Setup' (factory default), the global settings are used for all RADIUS inquiries.

10.55.1. RADIUS Global Authentication Settings

The following tables contain a summary of all RADIUS Global Authentication settings:

Designation in NEXMAN	Default value	Function
Server 1 Address		Four Radius server IP addresses can be set, with the first address always indicating the primary Radius server. Depending on the Server request algorithm, the other IP addresses are reserved for the backup Radius servers or be requested alternating or in parallel (see field 'Server request algorithm' below). Via NEXMAN (Tabs 'Radius State' and 'MAC+Security State') and with the console command the '`show radius`' status of the Radius servers can be checked.
Server 2 Address		
Server 3 Address		
Server 4 Address		
Authentication UDP Port	1812	The UDP port number on which the Radius server receives authentication requests. The official number is 1812. An older specification also allows 1645.
Shared secret	<empty>	The Shared Secret is used as a password towards the Radius server. This password must be identical both in the switch and in the Radius server.
Request timeout	5	The maximum time period in seconds, the switch will wait for the answer of the Radius server after a Radius request.

Request retries	2	Indicates how often the switch will retry a Radius request before considering the request as a failure. The respective Radius server will then be designated as 'down ' .
Portsecurity password	<empty>	This password is exclusively used for MAC-based authentication and transmitted in the 'User-Password' Radius attribute. If this field is left empty, the MAC address of the terminal unit to be authenticated will be used instead. The format is identical with the 'User-Name' attribute. However, the 'User-Password' will be transmitted as an encrypted value. For further information see Chapter *10.59.1. Portsecurity Modes {RADIUS allow ...}*.
Portsecurity realm	<empty>	This realm string only applies for the MAC based portsecurity modes. The User-Name Radius attribute will be supplemented by this port security realm string. If an empty string is indicated in the configuration, no Portsecurity realm is added. For further information see chapter *10.59.1. Portsecurity Modes {RADIUS allow ...}* and *10.59.2. Portsecurity Mode {IEEE802.1X allow one MAC address}* respectively.
Management realm	<empty>	This realm string only applies to Telnet/SSH/V.24 console and NEXMAN Radius requests. The User Name Radius attribute will be supplemented by this management realm string. If an empty string is indicated in the configuration, no management realm is added. For further information see chapter *10.56. RADIUS Console Authentication Mode* and *10.57. RADIUS Manager Authentication Modes* respectively.
Realm location	Suffix	Indicates whether the realm string is added before (prefix) or after (suffix) the actual User Name.
Realm separator	<empty>	Defines the separator, which is inserted between the actual User Name and the realm string. If an empty string is indicated in the configuration, no realm separator is added.
MAC address separator	<empty>	For MAC based Portsecurity Radius requests the MAC address is entered in the 'User-Name' attribute and possibly in the 'User-Password' attribute. The individual bytes of this MAC address can be separated by this separator string. If an empty string is indicated in the configuration, no MAC separator is inserted.
Startup VLAN ID	Unsecure VLAN-ID (Allow RX traffic to VLAN for unauthorized MACs)	This setting applies only to ports for which RADIUS-based (IEEE802.1X or MAC based) authentication is activated. The following settings are possible:: • Unsecure VLAN-ID (Allow RX traffic to VLAN for unauthorized MACs) • Unsecure VLAN-ID (Block RX traffic to VLAN for unauthorized MACs) • Port Default VLAN-ID (Allow RX traffic to VLAN for unauthorized MACs) • Port Default VLAN-ID (Block RX traffic to VLAN for unauthorized MACs) Determines which VLAN ID is activated as a Port Default VLAN-ID after a link-up or port security renew command: **Unsecure VLAN-ID:** With this setting, the globally configured Unsecure VLAN-ID is activated. **Port Default VLAN-ID:** The Port Default VLAN-ID configured for each port is used here. If the Port - Default VLAN-ID is set to 0, the Unsecure VLAN-ID is used for this port instead. It can also be determined whether RX data is passed through or blocked from the end device to the activated VLAN: **Allow RX traffic to VLAN for unauthorized MACs:** With this setting, untagged RX packets are forwarded unfiltered to the relevant VLAN. In contrast, tagged RX packets in the configured Voice VLAN are blocked after a short delay, i.e. RX packets are passed through to the Voice VLAN for a few seconds. This blocking is removed again as soon as the relevant device has been authenticated via RADIUS. **Block RX traffic to VLAN for unauthorized MACs:** Here RX packets from the end device are immediately blocked. This RX blocking remains until the end device has been authenticated via RADIUS

		(via IEEE802.1X or via MAC-based authentication) or until the end device has been moved to the 'Guest VLAN', 'Inaccessible VLAN' or 'IEEE802.1x Authentication Failure VLAN'. In addition, tagged RX packets in the configured Voice VLAN are blocked immediately, i.e. no packets are forwarded to the Voice VLAN until the end device has been authenticated via RADIUS. Important note: With this setting, the "Portsecurity aging time for PC behind IP-Phone" has no function. **IMPORTANT:** Despite blocking the RX data, broadcast and multicast packets in the default and voice VLAN are forwarded to the end devices. This enables e.g. Wake-on-LAN while the end device is switched off or not yet authenticated..

VLAN Attribute	IETF Tunnel-Private-Group-ID with VLAN-ID	Defines which RADIUS attribute is evaluated in an Access-Accept for the configuration of the port Default-VLAN-ID and Voice-VLAN-ID. The following settings are possible:
		• Nexans Vendor Specific VLAN ID
		• IETF Tunnel-Private-Group-ID with VLAN-ID
		• IETF Tunnel-Private-Group-ID with VLAN-Description
		• IETF Tunnel-Private-Group-ID with VLAN-ID or VLAN-Description
		• Ignore VLAN attributes
		
		IMPORTANT:
		Only the preset attribute will be accepted. If this attribute is missing in the Access-Accept, the port will be set to the Default-VLAN ID of the respective port.
		If the correct attribute is received, but the VALN ID lies outside the admissible range of 1… 4095, the Access-Accept will be rejected and the port will stay in the RADIUS-Unsecure-VLAN.
		
		Nexans Vendor Specific VLAN-ID:
		Here the Nexans Enterprise attribute 'Nexans-Port-Default-VLAN-ID' und 'Nexans-Port-Voice-VLAN-ID' is read.
		
		This attribute must be declared in the Radius dictionary as follows:
		`VENDOR Nexans 266 ietf`
		`ATTRIBUTE Nexans-Port-Default-VLAN-ID 1 integer Nexans`
		`ATTRIBUTE Nexans-Port-Voice-VLAN-ID 2 integer Nexans`
		
		The attribute value must contain the VLAN-ID and be within the 1 ... 4095 range.
		The transmitted VLAN ID is automatically entered into the VLAN table. We recommend setting the VLAN mode to {dynamic}, in order to prevent an overflow of the table. If the VLAN mode is set to {static} and if the VLAN table is full, the transmitted VLAN ID will be ignored and the Default-VLAN-ID (stored in the switch) of the respective port will be used instead.
		
		IETF Tunnel-Private-Group-ID with VLAN ID:
		Here the IETF standard attribute Tunnel-Private-Group-ID is expected (see RFC2868). The attribute value must contain the VLAN ID and be within the 1 ... 4095 range.
		The transmitted VLAN ID is automatically entered into the VLAN table. We recommend setting the VLAN mode to {dynamic}, in order to prevent an overflow of the table. If the VLAN mode is set to {static} and if the VLAN table is full, the transmitted VLAN-ID will be ignored and the Default-VLAN-ID (stored in the switch) of the respective port will be used instead.
		
		If the RADIUS server only sends a numerical value, this value will be used as Default-VLAN-ID. If, however, the voice VLAN shall be assigned, the numerical value shall be preceded by the text 'v:' or 'V:'.
		Example:
		Tunnel-Private-Group-ID with VLAN-ID = '23' → Default-VLAN_ID = 23
		Tunnel-Private-Group-ID with VLAN-ID = 'v:50' → Voice-VLAN_ID = 50
		
		If additional to the Tunnel-Private-Group-ID, the *Cisco*-Attribute "device-traffic-class=voice" is received the VLAN-ID will basically interpreted as the Voice-VLAN.

		IETF Tunnel-Private-Group-ID with VLAN Description: Here also the IETF standard attribute Tunnel-Private-Group-ID is expected (see RFC2868). However, the attribute value must contain the VLAN description according to the VLAN table. If the transmitted VLAN description is not found in the VLAN table, the Access-Accept will be discarded and the port will stay in the RADIUS-Unsecure-VLAN. In this case the VLAN mode must be set to {static}, in order to prevent the deletion of unused VLAN-IDs. NOTE: If you want to assign the Voice-VLAN the text 'v:' or 'V:' must be set before the VLAN-Description. If additional to the Tunnel-Private-Group-ID, the *Cisco*-Attribute "device-traffic-class=voice" is received the VLAN-ID will basically interpreted as the Voice-VLAN. **Ignore VLAN attributes:** Here all VLAN attributes of the RADIUS Servers are ignored and the port is set to the Default-VLAN-ID of the respective port after an Access-Accept.
Cisco device-traffic-class mode		Determines how the propritary CISCO RADIUS attribute 'device-traffic-class=voice' included in thed RADIUS Access-Accept message is used. The following settings can be configured: • Use device-traffic-class=voice to set Voice-VLAN to received VLAN-ID • Use device-traffic-class=voice to allow access to Voice-VLAN **Use device-traffic-class=voice to set Voice-VLAN to received VLAN-ID:** This is the default and should be used if: • the attribute 'device-traffic-class = voice' is not used in the RADIUS Access-Accept messages. • No voice VLAN-IDs are configured on the switch ports and the Voice-VLAN-IDs are assigned by the RADIUS server via the attribute 'Tunnel Private Group ID' and 'device-traffic-class = voice'. Here, the RADIUS Access-Accept message is checked, if in addition to the received VLAN-ID (via attribute 'Tunnel-Private-Group-ID') the message also contains the attribute 'device-traffic-class = voice'. If this is the case, this VLAN-ID is used as Voice-VLAN-ID for the corresponding port. **Use device-traffic-class=voice to allow access to Voice-VLAN:** This setting should be used if the voice VLAN-IDs are configured fixed on the switch ports and the Access-Accept only activates them. Initially, the voice VLAN-IDs set per port are disabled and the Voice-VLAN is turned off. Then the RADIUS Access-Accept is checked whether the attribute 'device-traffic-class=voice' is included. If so, the configured Voice-VLAN-ID will be activated on the corresponding port. NOTE: If the RADIUS Access-Accept additionally contains a VLAN-ID in the "Tunnel-Private-Group-ID" attribute, this VLAN-ID is preferably used as the Voice-VLAN-ID for the port.
Server request algorithm	Strict-Priority	Defines the algorithm used to query the Radius servers: **Strict-Priority:** The Radius servers are strictly requested in order independent of their status. It always starts from the first registered Radius server. **Round-Robin:** With the Round-Robin algorithm the order of the registered Radius servers will always be continued. For example, if an authentication happens with the Server 1, the next request starts with Server 2. After finishing the last registered Radius, it starts again with the first one. With this algorithm the connection and usage of all registered Radius servers are guaranteed. **Parallel:** All registered Radius servers will be requested parallel. The first arriving response will be accepted from the switch.

10.55.2. RADIUS Management Authentication Settings

The following tables contain a summary of all RADIUS Management Authentication settings:

Designation in NEXMAN	Default value	Function
Management Authentication Mode	Use Global Server Setup	Defines if the global RADIUS Authentication settings or the following separate set of parameters shall be used for the authentication of name and password (Telnet, SSHv2, V24, Manager).
Server 1 Address		Function identical to the equivalent settings of the above Global RADIUS settings.
Server 2 Address		
Server 3 Address		
Server 4 Address		
Authentication UDP Port	1812	
Shared secret	<empty>	
Request timeout	5	
Request retries	2	

10.56. RADIUS Console Authentication Modes

Six different authentication modes can be selected for the SSHv2, Telnet and V.24 console:

- Disabled: Telnet or V.24 console disabled
- Local: Local authentication
- Radius Only: Authentication through the RADIUS server only
- Radius first, then local: Authentication through RADIUS. If no server response, local authentication.
- TACACS+ Only: Authentication through the TACACS+ server only
- TACACS+ first, then local: Authentication through TACACS+. If no server response, local authentication.

Local (factory default):
Disabled:
See chapters *10.14. V.24 Console Authentication Mode*, *10.48. Telnet Console Authentication Mode*

and *10.49. SSHv2 Console Authentication Mode*

TACACS+ Only:
TACACS+ first, then local:
See chapter *10.64 TACACS+ Console Authentication Modes*

Radius only:
Instead of using the locally stored authentication data, authentication is performed by a central RADIUS server.

Radius first, then local:
In this mode an authentication via RADIUS server is attempted first. Only if no RADIUS server responds depending on the set server request algorithm, the entered login name and the password are compared with the locally stored data.

RADIUS authentication is as follows:

- The user enters his name and password during console login.
- The switch sends name and password to the RADIUS server via Radius Access Request.
- The Radius server checks the request and answers with an Access-Accept or Access-Reject message.
- If an Access-Accept is received, the privileges specified in the included Service Type attribute will be granted. If an Access-Accept message is received without this attribute or with an invalid Service Type, the error message “Wrong Authentication” will be displayed at the console prompt on V.24 or Telnet consoles, and a Radius Mgmt Auth Reject event will be sent.

- If an Access-Reject message is received, the error message “Wrong Authentication” will be displayed at the console prompt on V.24 or Telnet consoles, and a Radius Mgmt Auth Reject event will be sent.
- If there is no Radius server response (timeout), the error message “No Response From RADIUS Server” will be displayed at the console prompt on V.24 or Telnet consoles. Moreover, an alarm will be shown in the Manager’s Device List.

10.56.1. RADIUS Attributes for Conole Authentication

The following attributes are sent from the switch to the Radius server:

Attribute	Attribute contains …
NAS-IP-Address	IP address of the Nexans switch
NAS-Identifier	Switch name
NAS Port	0
NAS-Port-Type	Virtual (5)
Calling-Station-ID	IP address of the station performing the Telnet access. NOTE: In the case of V.24 console access this value will be 0.0.0.0
Service-Type	Administrative-User (6)
User-Name	The login name entered by the user. As an option the User Name can be supplemented by a fixed realm string. This Management realm will be added before (prefix) or after (suffix) the actual login name and be separated by a realm separator. Example: Console login name: MeierF MAC separator: - Management realm: nexans-port Realm separator: @ Realm position: suffix → User Name: MeierF@nexans-port
User-Password	The login password entered by the user. NOTE: The password is encrypted before transmission according to PAP procedure according to RFC 2865 chapter 5.2 and thus can not be read in clear text via Wireshark.

The following Radius attributes are read by the switch:

Attribute	Attribute contains …
Service-Type	The Access-Accept message must contain this attribute. It tells the switch whether the user shall be logged in for the Admin-Account (R/W) or the User-Account (R/O). The following Service Type values are admissible: • Service Type = Login-User(1) → User Mode (R/O) • Service Type = Administrative-User(6) → Admin Mode (R/W)

10.57. RADIUS Manager Authentication Modes

Seven different authentication modes can be set in the switch for NEXMAN access:

- SCP – Use SCP authentication mode setting: Authentication via SCP
- UDP/TFTP – No authentication (Ignores Username and Password) No authentication
- UDP/TFTP – Local Accounts Local authentication

- UDP/TFTP – Radius Only — Authentication through the RADIUS server only
- UDP/TFTP – Radius first, then Local Accounts — Authentication through RADIUS. If no server response, local authentication
- SNMPv3 – Local Accounts — Local authentication via SNMPv3
- Disable Manager access — Manager access via UDP, TFTP and SNMPv3 is completely disabled

SCP – Use SCP authentication mode setting (Factory-Default)
UDP/TFTP – No authentication (Ignores Username and Password)
SNMPv3 – Local Accounts
Disable Manager access:
See chapter *10.10. Manager Authentication Mode.*

UDP/TFTP – Radius Only
UDP/TFTP – Radius first, then Local Accounts:
The authentication procedure is principally identical with the console authentication via Radius server (see chapter *10.56. RADIUS Console Authentication Mode*).

10.58. RADIUS SCP Authentication Modes

Seven different authentication modes can be selected for SCP:

- Local: Local authentication
- Radius Only: Authentication through the RADIUS server only
- Radius first, then local: Authentication through RADIUS. If no server response, local authentication.
- TACACS+ Only: Authentication through the TACACS+ server only
- TACACS+ first, then local: Authentication through TACACS+. If no server response, local authentication.
- Use SSHv2 mode SSHv2 authentication mode is used
- Disabled: SCP Interface disabled

Use SSHv2 mode (Factory-Default):
Local:
Disabled:
See chapters *10.50 SCP Authentication Mode.*

TACACS+ Only:
TACACS+ first, then local:
See chapter *10.66 TACACS+ SCP Authentication Modes*

Radius only:
Radius first, then local:
The authentication procedure is principally identical with console authentication via Radius server (see chapter *10.56. RADIUS Console Authentication Mode*).

10.59. Portsecurity with authentication via RADIUS server

The following Portsecurity modes with Authentication via Radius Server are supported:
- RADIUS allow one, two or three MAC-Address(es)
- IEEE802.1X allow one MAC-Address
- IEEE802.1X PC+Voice allow two MAC-Addresses
- IEEE802.1X Multi-User allow three MAC-Addresses
- IEEE802.1X allow all MAC-Addresses
- IEEE802.1X Supplicant with MD5 Challenge
- IEEE802.1X Radius MAC Bypass enable

The following modes, **without** authentication via a Radius server, are additionally supported (description see chapter *10.36. Portsecurity*):
- Auto allow one, two or three MAC-Address(es)

- Manual setting three MAC-Addresses
- Manual setting three Vendor MAC-Addresses
- Learn and fix one or two MAC-Address(es)

10.59.1. Portsecurity Modes {RADIUS allow ...}

The settings {RADIUS allow one MAC address}, {RADIUS allow two MAC addresses} and {RADIUS allow three MAC addresses} allow the switch to automatically learn one, two or three MAC addresses and to have them additionally authenticated by a Radius server. Here a maximum of two VLANs can be assigned, i. e. one untagged default VLAN (e. g. for a PC or printer) and additionally one tagged voice VLAN (e. g. for an IP phone).

As long as no positive response is received from the Radius server, the port stays in the RADIUS-Unsecure-VLAN (see RADIUS-Unsecure-VLAN-ID in chapter *10.55. RADIUS Authentication*). Only after reception of an Access-Accept message will the port be set to the VLAN-ID in accordance with the received VLAN attribute (see VLAN Attribute in chapter *10.55. RADIUS Authentication)*. If another Accept-Access also containing a default or voice VLAN ID is received for a second or third MAC address, the currently set default or voice VLAN ID might be overwritten. That means that the Access-Accept last received defines the default or voice VLAN ID of the port.

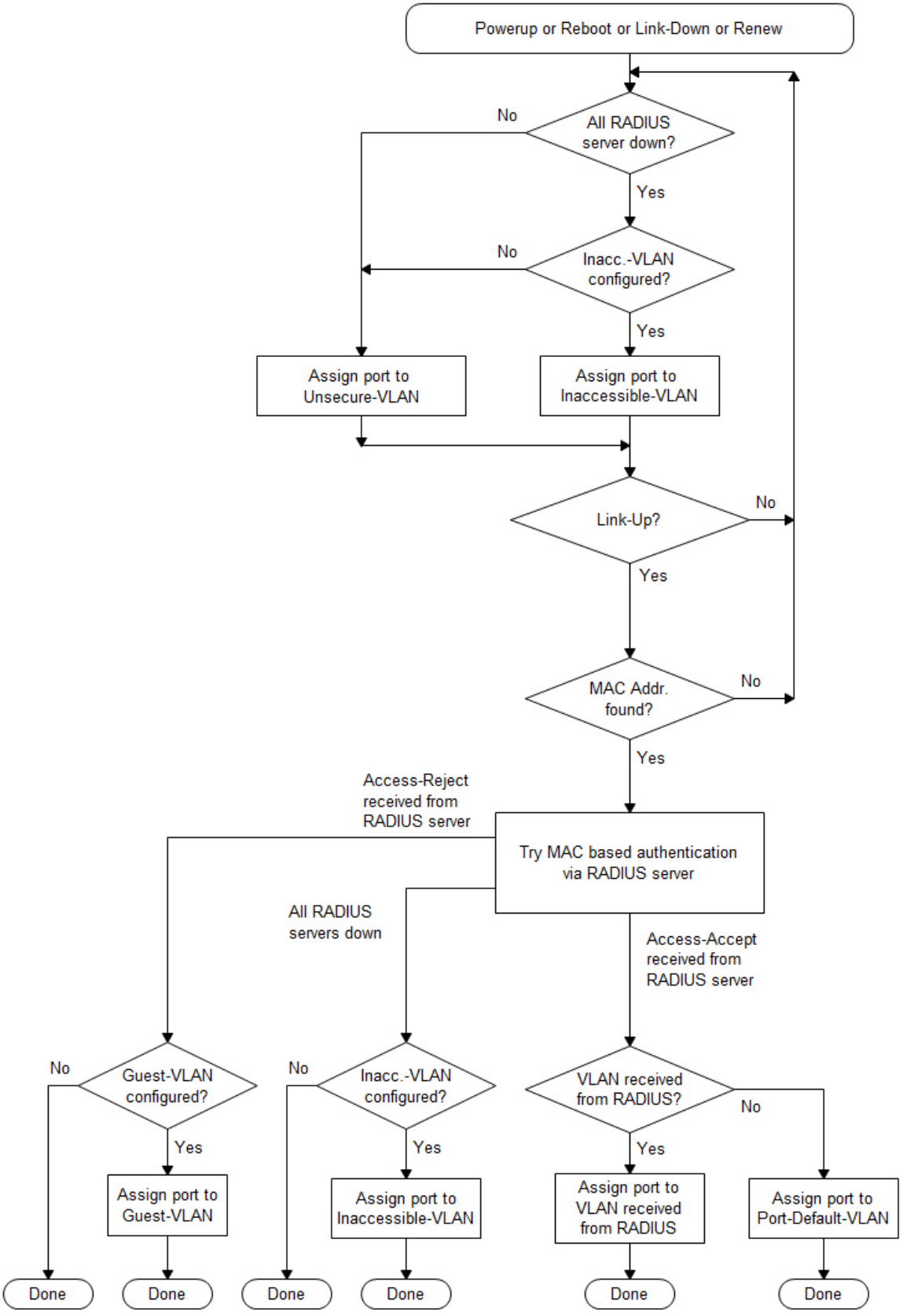
If a negative response is received from the Radius server, additionally a Radius Portsecurity Reject event will be sent, and an alarm will be shown in the Manager's Device List.

If there is no Radius server response (timeout), an alarm will be shown in the Manager's Device List, too.

If the switch detects more than the authorized one, two or three MAC addresses, the port will be disabled, if necessary (see chapter *10.36.1. Portsecurity Failure Action)*. This prevents e.g. that the user connects another switch behind a TP port. Moreover, a Port Security Failure event is sent, which contains the invalid MAC address. The learned MAC addresses are automatically deleted, when the link of the respective port is set to Down (e.g. when a different PC is plugged on) or when the port is switched off manually. Moreover, immediately after learning a new MAC address a New MAC Address event is sent.

If you want to reinitialise the Portsecurity function of a selected port or re-activate an automatically disabled port, this can be enforced via the Renew command (see chapter *10.36.5. Portsecurity - Renew Command*).

The following flow chart shows the basic procedure of the MAC based RADIUS authentication and the corresponding assignment of the VLANs:



The following Radius attributes are transmitted from the switch to the Radius server:

Attribute	Attribute contains …
NAS-IP-Address	IP address of the Nexans switch
NAS-Identifier	Switch name
NAS-Port	Number of the port on which the new MAC address has been received
NAS-Port-ID	Description of the port on which the new MAC address has been received
NAS-Port-Type	Ethernet(15)
Calling-Station-ID	The Calling-Station-ID consists of a text string containing the MAC address of the terminal (supplicant). The format is as follows (see RFC3580): **XX-XX-XX-XX-XX-XX** Example: MAC address: 00c02900000f → Calling-Station-ID: 00-C0-29-00-00-0F
Service-Type	Call-Check(10)
User-Name	The User-Name consists of a text string containing the MAC address of the terminal (supplicant). The format is as follows: **xx**<sep>**xx**<sep>**xx**<sep>**xx**<sep>**xx**<sep>**xx** As an option it can be supplemented by a fixed realm string. This Portsecurity realm will be added before (prefix) or after (suffix) the actual MAC address and be separated by a realm separator. Example: MAC address: 00c02900000f MAC separator: : Portsecurity realm: nexans-port Realm separator: @ Realm position: suffix → User Name: 00:c0:29:00:00:0f@nexans-port
User-Password	Default value = MAC address In principle, the Portsecurity request does not require a user password. However, not all Radius servers accept an empty password. For that reason, the switch uses the MAC address or specifies a fixed password which can be freely configured by the user (see setting 'Portsecurity Password' in chapter *10.55. RADIUS Authentication*). NOTE: The password is encrypted before transmission according to PAP procedure according to RFC 2865 chapter 5.2.

The following Radius attributes are read by the switch:

Attribute	Attribute contains …
Tunnel-Private-Group-ID Nexans-Port-Default-VLAN-ID Nexans-Port-Voice-VLAN-ID device-traffic-class	These attributes are only read in an Access-Accept message and defines which VLAN-ID the respective port shall be set to. For detailed information see VLAN Attribute Configuration Setting in chapter *10.55. RADIUS Authentication*.

10.59.2. Portsecurity Mode {IEEE802.1X allow one MAC address}

This setting enforces an authentication of the port according to IEEE802.1x and assumes that the connected terminal and the RADIUS server also support IEEE802.1x. Moreover, the switch checks, whether only one MAC address is received on the respective port. If the switch detects more than one MAC address, the port will be disabled, if necessary (see chapter *10.36.1. Portsecurity Failure Action)*. This prevents e.g. that the user connects another terminal behind an authenticated TP port. Furthermore, a Portsecurity Failure event is

sent, which contains the invalid MAC address. The learned MAC address is automatically deleted again, when the link of the respective port fails (e.g. when a different PC is plugged on) or when the port was switched off manually. Moreover, immediately after learning a new MAC address a New MAC Address event is sent.

As long as no positive response is received from the Radius server, the port stays in the RADIUS-Unsecure-VLAN (see RADIUS-Unsecure-VLAN-ID in chapter *10.55. RADIUS Authentication*). Only after reception of an Access-Accept message will the port be set to the VLAN-ID in accordance with the received VLAN attribute (see VLAN Attribute in chapter *10.55. RADIUS Authentication)*.

If a negative response (Access-Reject) is received from the Radius server, the port will be shifted into the Authentication Failure VLAN after a maximum number of Authentication Retries. This allows 802.1X Clients entering a wrong password once or several times to be shifted to a special VLAN. If you do not want to use this additional VLAN, the Authentication Failure VLAN-ID needs to be set to 0. In this case only the RADIUS-Unsecure-VLAN will be used. After the final negative respone an alarm will be shown in the Manager's Device List.

If there is no Radius server response (timeout), an alarm will be shown in the Manager's Device List, too.

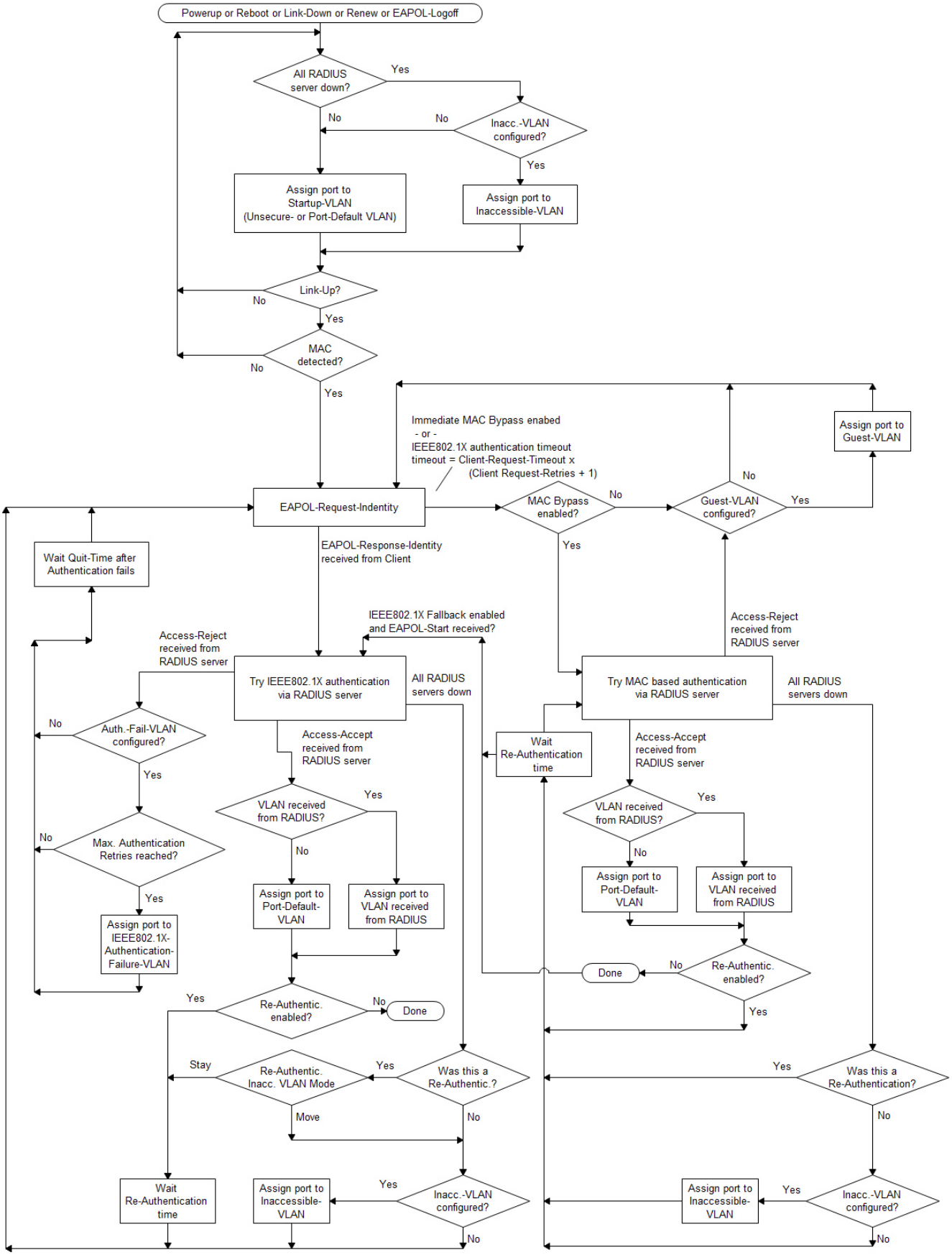
If you want to reinitialise the Portsecurity function of a selected port or re-activate an automatically disabled port, this can be enforced via the Renew command (see chapter *10.36.5. Portsecurity - Renew Command*).

The following tables contain a summary of all IEEE802.1X settings:

Designation in NEXMAN	Default Value	Function
IEEE 802.1X Global Setup		
IEEE 802.1X transparency enable	Disabled	See chapter *10.35. IEEE802.1X Transparency*
IEEE 802.1X Authenticator Setup		
Re-Authentication enable	No	If enabled, a periodical re-authentication of the terminal is enforced.
Re-Authentication initial delay	0	Only applies if the re-authentication is globally enabled: Defines the time delay until the first re-authentication is executed in seconds. After this first re-authentication, the 're-authentication interval' is used for all for further re-authentications. If the value is configured with 0, the 'Re-Authentication interval' is also used for the first re-authentication. This is especially useful if re-authentication should take place shortly after the initial authentication. This e.g. then the case, if, after the initial authentication, a check of the end device parameters takes place (current virus scanner installed? etc.) and then it is determined again whether the end device is allowed to remain in the initially assigned VLAN or should be moved to a special VLAN. This can be used as part of the CoA (Change of Authorization) strategy.
Re-Authentication interval	3600	Only applies if the re-authentication is globally enabled: Defines the time interval in seconds for re-authentication.

Re-Authentication Inaccessible VLAN Mode	Stay	Only applies if the re-authentication is globally enabled and an Inaccessible VLAN-ID is configured: Determines the behavior of the Port VLAN if all RADIUS servers can not be reached in case of an IEEE802.1X re-authentication. The following settings are available: Stay: The port remains in the currently activated VLAN • Move: The port is moved to the "Inaccessible VLAN" and the IEEE802.1X authentication of the port is restarted. The detailed procedure of the authentication can be seen from the flowchart below.
Quiet Time after Auth. fails	30	Quiet time in seconds after the RADIUS server has rejected an authentication. During this time no re-authentication is possible.
Client request timeout	30	Time period in seconds, the switch will wait for an answer from the terminal after an EAP request.
Client request retries	2	Number of retries of an EAP request before the authentication is aborted and restarted.
Max. Authentication Retries	0	The maximum number of failed authentication retries by the client. If this number is exceeded, the respective port will be set to the Authentication Failure VLAN. Example: The value of 0 means that after the first entry of a wrong password by the user the port will be shifted into the Authentication Failure VLAN. Example: The value of 2 means that the port will be shifted into the Authentication Failure VLAN after the user has entered a wrong password three times.
RADIUS MAC Bypass enable	Disabled	See chapter *10.59.6. Portsecurity Option {IEEE802.1X Radius MAC Bypass}*
MAC bypass Quiet Time	0	After receiving a Radius Reject, another authentication via MAC Bypass is attempted no sooner than after expiration of the MAC Bypass Quiet Time. The exact time depends on the configured Client Request Timeout and the Client Request Retries. If MAC Bypass Quiet Time is set to 0, after each 802.1x Timeout a MAC Bypass Authentication is triggered.
IEEE 802.1X Supplicant Setup		
MD5 Name	<none>	During IEEE802.1X authentication this name is send to the authenticator. See chapter *10.59.9. Portsecurity Modus {IEEE802.1X Supplicant}.*
M5 Password	<none>	During IEEE802.1X authentication this password is send to the authenticator. See chapter *10.59.9. Portsecurity Modus {IEEE802.1X Supplicant}.*

The following flow chart shows the basic procedure of the IEEE802.1X authentication and the corresponding assignment of the VLANs:



The following Radius attributes are transmitted from the switch to the Radius server:

Attribute	Attribute contains …
NAS-IP-Address	IP address of the Nexans switch
NAS-Identifier	Switch name
NAS-Port	Number of the switch port for which the authentication is performed.
NAS-Port-ID	Description of the switch port for which the authentication is performed.
NAS-Port-Type	Ethernet(15)
Calling-Station-ID	The Calling-Station-ID consists of a text string containing the MAC address of the terminal (supplicant). The format is as follows (see RFC3580): **XX-XX-XX-XX-XX-XX** Example: MAC address: 00c02900000f → Calling-Station-ID: 00-C0-29-00-00-0F
Service-Type	Framed(2)
Framed-MTU	Admissible frame length (1300)
User-Name	Here the identity string from the EAP response/identity packet of the terminal is entered. NOTE: The User Name is principally taken over without any change from the EAP packet. A configured Portsecurity realm string, as this is possible with the {RADIUS allow ...} modes, is ignored with 802.1X. Due to the limitation in the RADIUS protocol the maximum User Name length is limited to 253 characters. If the EAP packet contains a longer name, this one will be shortened to 253 characters before being included in the User Name RADIUS attribute. However, the EAP packet is included into the EAP-Message RADIUS attribute with its full-length User Name and fragmented, if necessary. Here the maximum User Name length in the EAP packet must not exceed 1400 characters.
Chargeable-User-Identity	This attribute is only inserted, when the parameter 'User-Name for 802.1X' is set to 'Chargeable-User-Identity' for Radius accounting. A detailed explanation of its function can be found in RFC4372.
EAP-Message	EAP message of the terminal.
State	This attribute is sent only, if it has been supplied by the Radius server in the previous Access Challenge or Access-Accept message. The attribute contents contained in the Access Challenge message will be used without any modification in the Access Request. In case of an Access-Accept message, in addition to the State attribute also the Termination Action attribute containing the RADIUS Request(1) value must be included, in order to ensure that the State attribute is contained in the next re-authentication.
Message-Authenticator	Signature, MD5-encoded

The following Radius attributes are read by the switch:

Attribute	Attribute contains …

Tunnel-Private-Group-ID Nexans-Port-Default-VLAN-ID Nexans-Port-Voice-VLAN-ID	This attribute is only read in an Access-Accept and defines which VLAN-ID the respective port shall be set to. Detailed information see VLAN Attribute Configuration Setting in chapter *10.55. RADIUS Authentication*.
State	If this attribute is supplied in an Access-Challenge, the indicated contents will be used without any modification in the next Access-Request. If this attribute is supplied in an Access-Accept, the Termination-Action attribute containing the RADIUS-Request(1) value must be additionally included in order to ensure that the State attribute is contained in the next re-authentication.
User-Name	This attribute is only read, when the parameter 'User-Name for 802.1X' is set to 'User-Name' for Radius accounting. A detailed explanation of its function can be found in RFC4372.
Chargeable-User-Identity	This attribute is only read, when the parameter 'User-Name for 802.1X' is set to 'Chargeable-User-Identity' for Radius accounting. A detailed explanation of its function can be found in RFC4372.
Termination-Action	This attribute is only read in an Access-Accept message. If present, it must have the value RADIUS-Request(1) (see State attribute).
Message-Authenticator	Signature, MD5-encoded

10.59.3. Portsecurity Mode {IEEE802.1X PC+Voice allow two MAC addresses}

In this mode two MAC addresses can be authenticated in two different VLANs according to IEEE802.1X. On the default VLAN the switch sends untagged EAP packets and on the voice VLAN it sends tagged EAP packets. As the name indicates, this function is especially designed for the combination of IP phone and downstream PC. In most Voice-over-IP installations the PC sends and receives untagged packets, whereas the IP phone sends and receives tagged packets with the appropriate 802.1Q prioritisation information.

In installations with *Cisco* IP phones the Voice VLAN can be additionally transmitted via CDP to the IP phone. Here the VLAN ID configured on the corresponding port of the Nexans switch is used. Thus, an automatic configuration of the *Cisco* IP phone is possible via CDP. Further information on configuring *Nexans* switches in a *Cisco* environment can be obtained from *Nexans* on request (keyword 'Cisco evaluation').

10.59.4. Portsecurity Mode {IEEE802.1X Multi-User allow three MAC addresses}

If a port is switched to this Security mode, on this port up to three MAC addresses can be simultaneously authenticated according to IEEE802.1X. First all detected MAC addresses will be blocked. The blocking will be cancelled only for those MAC addresses where it was possible to authenticate the supplicant via IEEE802.1X.

The port will be switched into the Unsecure VLAN as long as no client is authenticated.

If a default VLAN is configured (VLAN-ID = 1…4095), after successful authentication of at least one client, the port will always be switched to the configured default VLAN.

If no default VLAN is configured (VLAN-ID = 0), the switch expects the VLAN ID to be assigned by the RADIUS server. Here the first received VLAN-ID is used which was transmitted for a successfully authenticated (via IEEE802.1X or MAC-Bypass) client by the RADIUS server.

Via these functions PCs and other devices may be authenticated, on which in addition to their own MAC address, further MAC addresses of virtual machines are used.

Clients, which do not respond to EAP-Request-Identity during IEEE802.1X Re-Authentication (e. g. PC disconnected or shut down) or have been rejected by the RADIUS server during IEEE802.1X or MAC-Bypass Re-Authentication (user was blocked), will be blocked again.

Additionally, clients can be automatically removed from the port's MAC list after a selectable period of time via the Portsecurity Address Ageing function. This makes sense if another switch follows after the switch port so that a link-down of the client cannot be detected.

10.59.5. Portsecurity Modus {IEEE802.1X allow all MAC-Addresses}

This mode's functions is almost identical with {IEEE802.1X allow one MAC address} mode.

In contrast to the {IEEE802.1X allow one MAC address} mode, here any number of MAC addresses can be received on the port. At least one of the connected terminals (e.g. an access point which is an IEEE802.1X authenticator) has to support IEEE802.1X. The port will only be switched through, if the IEEE802.1X terminal was correctly authenticated.

If the 'IEEE802.1X Radius MAC Bypass' option is activated, only the first detected MAC address is authenticated after an IEEE802.1X timeout. If the RADIUS server confirms the MAC address, the port is switched through. Important: All subsequent detected MAC addresses are ignored for authentication, even in the event that the address detected first was rejected by the RADIUS server.

Also unlike the {IEEE802.1X allow one MAC address} mode, here no 'New-MAC-Address' events are transmitted.

10.59.6. Portsecurity Option {IEEE802.1X Radius MAC Bypass}

This option is only relevant to ports set to an IEEE802.1X-based Security mode.

Depending on the configuration of the MAC bypass, before or after an IEEE802.1X authentication attempt an authentication of the MAC address is attempted.

If this function is enabled, an authentication of the port according to IEEE802.1X is attempted first. If the connected terminal does not respond with its IEEE802.1X identity, alternatively an authentication of the MAC address at the Radius server is attempted after the EEE802.1X timeouts and retries have expired.

After successful authentication of the MAC address and enabled IEEE802.1X ‘Re-Authentication’ a periodic re-authentication of the MAC Address is performed. The re-authentication time interval corresponds to the IEEE802.1X ‘Re-Authentication interval’.

RADIUS MAC Bypass the following modes can be selected:

- Disable
- Send MAC-based RADIUS requests after each IEEE802.1X timeout
- Send single MAC-based RADIUS request after first IEEE802.1X timeout
- Send MAC bypass after each IEEE802.1X timeout, with IEEE802.1X fallback
- Send single MAC bypass after first IEEE802.1X timeout, with IEEE802.1X fallback
- Send MAC bypass immediately and after each IEEE802.1X timeout
- Send single MAC bypass immediately
- Send MAC bypass immediately and after each IEEE802.1X timeout, with IEEE802.1X fallback
- Send single MAC bypass immediately, with IEEE802.1X fallback

Disable:
MAC Bypass is disabled.

Send MAC bypass after each IEEE802.1X timeout:
This command first tries to authenticate the port according to IEEE802.1X. If the connected terminal does not respond with its IEEE802.1X identity, subsequently an authentication of the MAC address at the Radius server is attempted after the EEE802.1X timeouts and retries have expired.
- If the MAC address is rejected by the RADIUS server, the authentication attempts alternating between IEEE802.1X and MAC address are repeated until one of the two methods is successful.
- If MAC authentication is successful, no further IEEE802.1X authentication attempts are made. A return to IEEE802.1X can only be made after expiration of the IEEE802.1X re-authentication interval and the related rejection of the MAC address by the RADIUS server. Alternatively, an IEEE802.1X authentication can be initiated at any time by a Link-Down or by the Portsecurity “Renew” command on the corresponding port.

Send single MAC bypass after first IEEE802.1X timeout:
This command first tries to authenticate the port according to IEEE802.1X. If the connected terminal does not respond with its IEEE802.1X identity, subsequently one single authentication of the MAC address at the Radius server is attempted after the EEE802.1X timeouts and retries have expired.
- If the MAC address is rejected by the RADIUS server, only IEEE802.1X authentication attempts are made. However, if an authentication of the MAC address shall be initiated again, this must be done via a short Link-Down or the Portsecurity “Renew” command.

- If MAC authentication is successful, no further IEEE802.1X authentication attempts are made or accepted. A return to IEEE802.1X can only be made after expiration of the IEEE802.1X re-authentication interval and the related rejection of the MAC address by the RADIUS server. Alternatively, an IEEE802.1X authentication can be initiated at any time by a Link-Down or by the Portsecurity “Renew” command on the corresponding port.

Send MAC bypass after each IEEE802.1X timeout, with IEEE802.1X fallback:
Send single MAC bypass after first IEEE802.1X timeout, with IEEE802.1X fallback:
These modes are identical with the above **Send MAC bypass after each IEEE802.1X timeout** and **Send single MAC bypass after first IEEE802.1X timeout** modes respectively. But after a successful MAC authentication a renewed IEEE802.1X authentication can be initiated at any time by the connected terminal device. For this purpose, the terminal device can send any EAP packet to the switch (usually an EAP Start Request). This function is particularly interesting, if the connected terminal enables its IEEE802.1X function only after a successful MAC authentication (e. g. during the first filling of PCs).

Send MAC bypass immediately and after each IEEE802.1X timeout:
This command tries immediately after identifying the MAC address to authenticate it at the RADIUS server.
- If the MAC address is rejected by the RADIUS server, the authentication attempts alternating between IEEE802.1X and MAC address are repeated until one of the two methods is successful.
- If the MAC authentication is successful, no further IEEE802.1X authentication attempts are made. A return to IEEE802.1X can only be made after expiration of the IEEE802.1X re-authentication interval and the related rejection of the MAC address by the RADIUS server. Alternatively, an IEEE802.1X authentication can be initiated at any time by a Link-Down or by the Portsecurity “Renew” command on the corresponding port.

Send single MAC bypass immediately:
This command tries immediately after identifying the MAC address to authenticate it at the RADIUS server.
- If the MAC address is rejected by the RADIUS server, only IEEE802.1X authentication attempts are made. However, if an authentication of the MAC address shall be initiated again, this must be done via a short Link-Down or the Portsecurity “Renew” command.
- If MAC authentication is successful, no further IEEE802.1X authentication attempts are made or accepted. A return to IEEE802.1X can only be made after expiration of the IEEE802.1X re-authentication interval and the related rejection of the MAC address by the RADIUS server. Alternatively, an IEEE802.1X authentication can be initiated at any time by a Link-Down or by the Portsecurity “Renew” command on the corresponding port.

Send MAC bypass immediately and after each IEEE802.1X timeout, with IEEE802.1X fallback:
Send single MAC bypass immediately, with IEEE802.1X fallback:
These modes are identical with the above **Send MAC bypass immediately and after each IEEE802.1X timeout** and **Send single MAC bypass immediately** modes respectively. But after a successful MAC authentication a renewed IEEE802.1X authentication can be initiated at any time by the connected terminal device. For this purpose, the terminal device can send any EAP packet to the switch (usually an EAP Start Request). This function is particularly interesting, if the connected terminal enables its IEEE802.1X function only after a successful MAC authentication (e. g. during the first filling of PCs).

10.59.7. Portsecurity Option {Toggle Link}

If this function is enabled, after a successful RADIUS MAC authentication (e. g. via IEEE802.1X MAC Bypass) the link of the corresponding port is interrupted for one second. This forces the connected terminal unit to request a new IP address via DHCP. The already learned MAC addresses of the switch port are preserved.

This function is useful, if the terminal unit has first received an IP address in the Unsecure-VLAN and shall be moved to another VLAN with a different IP range after successful MAC authentication.

10.59.8. Portsecurity Option {EAP Packets within Voice-VLAN}

Here you can define, whether IEEE802.1X EAP packets, which receive the MAC address of a phone in the voice VLAN as a destination address, will be transmitted with or without VLAN tag. The correct setting depends on the specification made by the corresponding phone manufacturer.

10.59.9. Portsecurity Modus {IEEE802.1X Supplicant}

This function allows the switch to work as an IEEE802.1X supplicant to the uplink and authenticate itself towards the core switch by an EAP MD5-Challenge. This protects from the removal of the switch in order to gain access to the network via the uplink fiber.

NOTE: The core switch has to support an IEEE802.1X mode which will allow all other MAC addresses without authentication after authentication of the Nexans switch. With Nexans switches the respective mode is called {IEEE802.1X allow all MAC-Addresses}.

10.60. RADIUS Accounting

The switch supports the RADIUS accounting protocol according to RFC2866. This protocol can be separately activated for MAC- and IEEE802.1X-based authentication. In addition to Radius authentication, for Radius accounting there is a dedicated set of parameters available for configuring the Radius server.

Radius accounting can be used, among others, for the following tasks:

- Recording of the exact periods of time a MAC address and/or an IEEE802.1X user was active.
- Recording of the related IP addresses (only possible with GigaSwitch)
- Recording of the byte and packet counters for each port for accounting or data volume control purposes

NOTE:

All counters are transmitted with 64 bits. Here the extended Radius attributes 'Acct-Input-Gigawords' and 'Acct-Output-Gigawords' are used. Thus, an overflow of these counters can virtually be excluded. If a Portsecurity mode allowing more than one MAC address per port is set, no counters will be transmitted because the switch supports only counters per port and not per MAC address.

10.60.1. RADIUS Accounting Settings

The following table shows a summary of all RADIUS accounting settings:

Designation in NEXMAN	Default Value	Function
IEE802.1X Accounting enable	disabled	If selected, accounting is enabled for IEEE802.1X authentication. This applies to all ports on which an IEEE802.1X-based Security mode is activated.
MAC based Accounting enable	disabled	If selected, accounting is enabled for MAC-based authentication. This applies to all ports on which MAC-based authentication is performed. If an IEEE802.1X-based Security mode is enabled and simultaneously the 'IEEE802.1X Radius MAC Bypass' is enabled, accounting is also performed when the MAC bypass is executed.
Server 1 Address		Four Radius server IP addresses can be set, with the first address always indicating the primary Radius server. Depending on the Server request algorithm, the other IP addresses are reserved for the backup Radius servers or be requested alternating or in parallel (see field ‘Server request algorithm’ for Radius authentication). Via NEXMAN (Tabs 'Radius State' and 'MAC+Security State') and with the console command `'sh:ow ra:dius ac:counting'` the status of the Radius servers can be checked.
Server 2 Address		
Server 3 Address		
Server 4 Address		
Accounting UDP Port	1813	The UDP port number on which the Radius server receives accounting requests. The official number is 1813. An older specification also allows 1646.
Request timeout	5	The maximum time period in seconds, the switch will wait for the answer of the Radius server after a Radius request.

Request retries	2	Indicates how often the switch will retry a Radius request before considering the request as a failure. The respective Radius server will be designated as 'down' in the status display.
Shared secret	<empty>	The 'Shared Secret' is used as a password towards the Radius server. This password must be identical in the switch and in the Radius server.
Alive packets enable	disabled	If selected, so-called Alive or Interim packets are sent to the Radius server.
Alive packets interval	10 min	Defines the interval for sending the above mentioned alive packets.
User-Name for 802.1X	EAP only	Defines the name which will be used for the Radius accounting attribute 'User-Name'. The following settings are possible: • EAP-Identity only • User-Name from Access-Accept • Chargeable-User-Identity from Access-Accept **EAP-Identity only:** With this setting only the name transmitted by the terminal during the EAP-Response-Identity procedure is used. **User-Name from Access-Accept:** This setting makes sense above all when using EAP-TTLS, because in this case the EAP-Response-Identity packet contains an anonymous name only. If the Radius server supports the transmission of the actual name via the User-Name attribute, this setting should be used. However, if no User-Name attribute is delivered by the server, the name from the EAP-Response-Identity packet is used again. **Chargeable-User-Identity from Access-Accept:** This setting makes sense above all when using EAP-TTLS, because in this case the EAP-Response-Identity packet contains an anonymous name only. If the Radius server supports the transmission of the actual name via the Chargeable-User-Identity attribute according to RFC4372, this setting should be used. However, if no Chargeable-User-Identity attribute is delivered by the server, the name from the EAP-Response-Identity packet is used again.
Discover IP Address	disabled	If this parameter is set to 'Discover to Framed-IP-Address', the IP address of the terminal is determined after successful MAC- or IEEE802.1X-based authentication. Then the IP address will be sent in all alive packets and in the stop packet as Framed-IP-Address attribute.

10.60.2. RADIUS Attributes for Accounting

The following Radius attributes are transmitted from the switch to the Radius accounting server:

Attribute	Attribute contains …
Acct-Status-Type	The type of the accounting packet. This is either 'Start', 'Alive' or 'Stop'
Acct-Session-ID	Is used by the Radius server for the definite assignment of the individual accounting packets. The ID is incremented by the switch for each new successful authentication. Moreover, the number of switch reboots is integrated into the ID, so that the IDs cannot repeat even after a reboot.
Acct-Session-Time	Time in seconds elapsed since successful authentication. This attribute is not included in the Start packet, since at the start the time commences with 0.
NAS-IP-Address	IP address of the Nexans switch
NAS-Identifier	Switch name
NAS-Port	Number of the switch port
NAS-Port-ID	Description of the switch port
NAS-Port-Type	Ethernet (15)

Calling-Station-ID	MAC address of the terminal
Framed-IP-Address	IP address of the terminal. See above explanation on the 'Discover IP Address' parameter.
User-Name	With IEEE802.1X-based authentication usually the name transmitted by the terminal during the EAP-Response-Identity procedure is used. However, this depends on the ' User-Name for 802.1X' setting (see above). For MAC-based authentication the user name consists of a text string containing the MAC address. The format is as follows: **xx**<sep>**xx**<sep>**xx**<sep>**xx**<sep>**xx**<sep>**xx** Where xx are the individual bytes of the MAC address and <sep> is a freely selectable MAC separator. As an option this attribute can be supplemented by a fixed realm string. This Portsecurity realm will be added before (prefix) or after (suffix) the actual MAC address and be separated by a realm separator. Example: MAC address: 00c02900000f MAC separator: - Portsecurity realm: nexans-port Realm separator: @ Realm position: suffix → User Name: 00-c0-29-00-00-0f@nexans-port
Acct-Input-Octets Acct-Input-Gigawords	A 64-bit counter containing the number of bytes received by the switch. The following formula must be used for calculating the value: Input bytes = (Acct-Input-Gigawords * 2^{32}) + Acct-Input-Octets
Acct-Output-Octets Acct-Output-Gigawords	A 64-bit counter containing the number of bytes sent by the switch. The following formula must be used for calculating the value: Output bytes = (Acct-Output-Gigawords * 2^{32}) + Acct-Output-Octets
Acct-Input-Packets	A 32-bit counter containing the number of packets received by the switch.
Acct-Output-Packets	A 32-bit counter containing the number of packets sent by the switch.

NOTE:

The counters are not included in the Start packet, since at the start all counters commence with 0.

10.61. TACACS+ Authentication

HW5 switches support the TACACS+ authentication protocol according to Draft IETF-opsawg-tacacs-15.

This protocol is used for the following authentication tasks in the switch:

- Telnet authentication of Name/Password
- SSHv2 authentication of Name/Password
- V.24 authentication of Name/Password
- SCP authentication of Name/Password

The following chapters provide a detailed description of the individual modes**.**

10.61.1. TACACS+ Authentication Settings

The following table contains a summary of all TACACS+ Authentication settings:

Designation in NEXMAN	Default value	Function
Server 1 Address		Four TACACS+ Authentication server IP addresses can be set, with the first address always indicating the primary TACACS+ Authentication server.
Server 2 Address		

Server 3 Address		Depending on the Server request algorithm, the other IP addresses are reserved for the backup TACACS+ Authentication servers or be requested alternating or in parallel (see field 'Server request algorithm' below). Via NEXMAN (Tabs TACACS+State' and 'MAC+Security State') and with the console command '`sh:ow t:acacs+`' the status of the TACACS+ Authentication servers can be checked.
Server 4 Address		
Authentication TCP Port	49	The TCP port number on which the TACACS+ Authentication server receives authentication requests. The official number is 49.
Shared secret	<empty>	The Shared Secret is used as a password towards the TACACS+ Authentication server. This password must be identical both in the switch and in the TACACS+ Authentication server.
Request timeout	5	The maximum time period in seconds, the switch will wait for the answer of the TACACS+ Authentication server after a TACACS+ authentication request.
Server request algorithm	Strict-Priority	Defines the algorithm used to query the TACACS+ Authentication servers: **Strict-Priority:** The TACACS+ Authentication servers are strictly requested in order, independent of their status. It always starts from the first registered TACACS+ Authentication server. **Round-Robin:** With the Round-Robin algorithm the order of the registered TACACS+ Authentication servers will always be continued. For example, if an authentication happens with the Server 1, the next request starts with Server 2. After finishing the last registered TACACS+ Authentication server, it starts again with the first one. With this algorithm the connection and usage of all registered TACACS+ Authentication servers are guaranteed. **Parallel:** All registered TACACS+ Authentication servers will be requested in parallel. The first arriving response will be accepted by the switch.

10.62. TACACS+ Authorization

HW5 switches support the TACACS+ authorization protocol according to Draft IETF-opsawg-tacacs-15.

This protocol is used for the following authorization tasks in the switch:

- Telnet authorization of users for general access rights (read-write, read-only)
- Telnet authorization of CLI commands
- SSHv2 authorization of users for general access rights (read-write, read-only)
- SSHv2 authorization of CLI commands
- V.24 authorization of users for general access rights (read-write, read-only)
- V.24 authorization of CLI commands
- SCP authorization of users for general access rights (read-write, read-only)

The following chapters provide a detailed description of the individual modes**.**

IMPORTANT:

For the TACACS+ authorization (Telnet, SSHv2, V24, SCP) separate settings can be configured. However, if 'TACACS+ Authorization Mode' is set to 'Use Authentication Server Setup' (factory default), the authentication settings are used for all TACACS+ authorization inquiries.

For the authorization of console commands, option 'Command Authorization' must be enabled.

10.62.1. TACACS+ Authorization Settings

The following table contains a summary of all TACACS+ Authorization settings:

Designation in NEXMAN	Default value	Function
Authorization Mode	Use Authentication Server Setup	Defines if the TACACS+ Authentication settings or the following separate set of parameters shall be used for the authorization of user and console commands (Telnet, SSHv2, V24, SCP).
Command Authorization	disabled	Defines if authorization of console commands shall be enabled. If this option is disabled, the general access rights retrieved on user authorization will be used.
Server 1 Address		Four TACACS+ Authorization server IP addresses can be set, with the first address always indicating the primary TACACS+ Authorization server. Depending on the Server request algorithm, the other IP addresses are reserved for the backup TACACS+ Authorization servers or be requested alternating or in parallel (see field 'Server request algorithm' below). Via NEXMAN (Tabs TACACS+State' and 'MAC+Security State') and with the console command 'sh:ow t:acacs+' the status of the TACACS+ Authorization servers can be checked.
Server 2 Address		
Server 3 Address		
Server 4 Address		
Authorization TCP Port	49	The TCP port number on which the TACACS+ Authorization server receives authorization requests. The official number is 49.
Shared secret	<empty>	The Shared Secret is used as a password towards the TACACS+ Authorization server. This password must be identical both in the switch and in the TACACS+ Authorization server.
Request timeout	5	The maximum time period in seconds, the switch will wait for the answer of the TACACS+ Authorization server after a TACACS+ authorization request.
Server request algorithm	Strict-Priority	Defines the algorithm used to query the TACACS+ Authorization servers: **Strict-Priority:** The TACACS+ Authorization servers are strictly requested in order, independent of their status. It always starts from the first registered TACACS+ Authorization server. **Round-Robin:** With the Round-Robin algorithm the order of the registered TACACS+ Authorization servers will always be continued. For example, if an authorization happens with the Server 1, the next request starts with Server 2. After finishing the last registered TACACS+ Authorization server, it starts again with the first one. With this algorithm the connection and usage of all registered TACACS+ Authorization servers are guaranteed. **Parallel:** All registered TACACS+ Authorization servers will be requested in parallel. The first arriving response will be accepted by the switch.

10.63. TACACS+ Accounting

HW5 switches support the TACACS+ accounting protocol according to Draft IETF-opsawg-tacacs-15.

TACACS+ accounting can be used, among others, for the following tasks:

- Recording of the exact periods of time a TACACS+ user was active
- Recording of the related IP addresses
- Recording of the executed console commands

The following chapters provide a detailed description of the individual modes**.**

IMPORTANT:

For the accounting (Telnet, SSHv2, V24, SCP) separate TACACS+ settings can be configured. However, if 'TACACS+ Accounting Mode' is set to 'Use Authentication Server Setup', the authentication settings are used for all TACACS+ accounting inquiries.

For the accounting of console commands, option 'Command Authorization' must be enabled.

10.63.1. TACACS+ Accounting Settings

The following table contains a summary of all TACACS+ Accounting settings:

Designation in NEXMAN	Default Value	Function
Accounting Mode	disabled	Defines if the TACACS+ Accounting settings or the following separate set of parameters shall be used for the recording (Telnet, SSHv2, V24, SCP).
Server 1 Address		Four TACACS+ Accounting server IP addresses can be set, with the first address always indicating the primary TACACS+ Accounting server. Depending on the Server request algorithm, the other IP addresses are reserved for the backup TACACS+ Accounting servers or be requested alternating or in parallel (see field 'Server request algorithm'). Via NEXMAN (Tabs TACACS+ State' and 'MAC+Security State') and with the console command '`sh:ow t:acacs+`' the status of the TACACS+ Accounting servers can be checked.
Server 2 Address		
Server 3 Address		
Server 4 Address		
Accounting TCP Port	49	The TCP port number on which the TACACS+ Accounting server receives accounting requests. The official number is 49.
Shared secret	<empty>	The 'Shared Secret' is used as a password towards the TACACS+ Accounting server. This password must be identical in the switch and in the TACACS+ Accounting server.
Request timeout	5	The maximum time period in seconds, the switch will wait for the answer of the TACACS+ Accounting server after a TACACS+ accounting request.
Server request algorithm	Strict-Priority	Defines the algorithm used to query the TACACS+ Accounting servers: **Strict-Priority:** The TACACS+ Accounting servers are strictly requested in order, independent of their status. It always starts from the first registered TACACS+ Accounting server. **Round-Robin:** With the Round-Robin algorithm the order of the registered TACACS+ Accounting servers will always be continued. For example, if an accounting happens with the Server 1, the next request starts with Server 2. After finishing the last registered TACACS+ Accounting server, it starts again with the first one. With this algorithm the connection and usage of all registered TACACS+ Accounting servers are guaranteed. **Parallel:** All registered TACACS+ Accounting servers will be requested in parallel. The first arriving response will be accepted by the switch.

10.64. TACACS+ Console Authentication Modes

Six different authentication modes can be selected for the SSHv2, Telnet and V.24 console:

- Disabled: Telnet or V.24 console disabled
- Local: Local authentication
- Radius Only: Authentication through the RADIUS server only
- Radius first, then local: Authentication through RADIUS. If no server response, local authentication.
- TACACS+ Only: Authentication through the TACACS+ server only
- TACACS+ first, then local: Authentication through TACACS+. If no server response, local authentication.

Local (factory default):
Disabled:
See chapters *10.14. V.24 Console Authentication Mode,* *10.48. Telnet Console Authentication Mode* and *10.49. SSHv2 Console Authentication Mode.*

Radius Only:
Radius first, then local:
See chapter *10.56 RADIUS Console Authentication Modes*

TACACS+ only:
Instead of using the locally stored authentication data, authentication is performed by a central TACACS+ Authentication server.

Additionally, the user is authorized by a TACACS+ Authorization server for general access rights (read-write, read-only).

TACACS+ first, then local:
In this mode an authentication via TACACS+ Authentication server is attempted first. Only if no TACACS+ Authentication server responds depending on the set server request algorithm, the entered login name and the password are compared with the locally stored data.

Additionally, the user is authorized by a TACACS+ Authorization server for general access rights (read-write, read-only). Only if no TACACS+ Authorization server responds depending on the set server request algorithm, the local access rights are used.

TACACS+ authentication and authorization of users are as follows:

- The user enters name and password during console login.
- The switch sends the name to the TACACS+ Authentication server via TACACS+ authentication request.
- The TACACS+ Authentication server answers with a TACACS+ authentication reply and status “Send Password”.
- The switch sends the password to the TACACS+ Authentication server via TACACS+ authentication request.
- The TACACS+ Authentication server checks name and password, and answers with a TACACS+ authentication reply containg the status “Authentication Passed“ or “Authentication Failed”.
- If an authentication reply with status “Authentication Failed“ is received, the error message “Wrong Authentication” will be displayed at the console prompt on V.24 or Telnet consoles.
- If an authentication reply with status “Authentication Passed“ is received, the switch sends a TACACS+ authorization request to the TACACS+ Authorization server.
- If no TACACS+ Authentication server responds depending on the set server request algorithm (timeout), the error message “No Response From TACACS+ Authentication Server” will be displayed at the console prompt on V.24 or Telnet consoles. Moreover, an alarm will be shown in the Manager’s Device List.
- The TACACS+ Authorization server checks if the user can be authorized and which general access rights the user has, and answers with an TACACS+ authorization reply containing the status “PASS_ADD“ or “FAIL”.
- If an authentication reply with status “FAIL“ is received, the error message “Wrong Authorization” will be displayed at the console prompt on V.24 or Telnet consoles.
- If an authentication reply with status “PASS_ADD“ is received, the general access rights specified in the included *Nexans*-specific attribute ‘nx-access’ will be granted (NX-ACCESS-RW for admin access rights (R/W) or NX-ACCESS-RO for user access rights (R/O)). If such authentication reply received without this attribute or with an invalid ‘nx-access’ value, the error message “Wrong Authorization” will be displayed at the console prompt on V.24 or Telnet consoles.
- If no TACACS+ Authorization server responds depending on the set server request algorithm (timeout), the error message “No Response From TACACS+ Authorization Server” will be displayed at the console prompt on V.24 or Telnet consoles. Moreover, an alarm will be shown in the Manager’s Device List.
- If TACACS+ Accounting is enabled, the switch sends the user name to the TACACS+ Accounting server via TACACS+ accounting request.
- The TACACS+ Accounting server records the user login in a log file, and answers with an accounting reply containg the status “Success“ or “Error”.

10.64.1. TACACS+ Attributes for Console User Authentication

The following attributes are sent from the switch to the TACACS+ Authentication server for user authentication:

Attribute	Attribute contains …
Action	Authentication action to be performed. The only currently supported type is: Inbound Login (1)
Privilege Level	*Cisco* privilege level 0…15 of the requested user (unused by *Nexans* switches)
Authentication type	Authentication type to be used. The only currently supported type is: ASCII (1)
Service	Service protocol to be used. The only currently supported protocol is: PPP (3)
User	User name or password
Data	Data for authentication (not used)

The following TACACS+ Authentication attributes are read by the switch for user authentication:

Attribute	Attribute contains …
Status	The status of the authentication request: Send password (0x05) → Send password for user to TACACS+ Authentication server Authentication Passed (0x01) → User authentication succeded Authentication Failed (0x02) → User authentication failed
Flags	Status flags: Send password → 0x01 (NoEcho) Authentication Passed/Failed → 0x00
Server message	Message from TACACS+ Authentication server to be displayed: Send password → Password prompt (default “Password:”) Authentication Passed/Failed → -
Data	Data for authentication (not used)

10.64.2. TACACS+ Attributes for Console User Authorization

The following attributes are sent from the switch to the TACACS+ Authorization server for user authorization:

Attribute	Attribute contains …
Auth Method	Authorization method to be applied: TACACSPLUS (0x06)
Privilege Level	*Cisco* privilege level 0…15 of the requested user (unused by *Nexans* switches)
Authentication type	Authentication type to be used. The only currently supported type is: ASCII (1)
Service	Service protocol to be used. The only currently supported type is: PPP (3)
User	User name
Port	The TCP port number on which the TACACS+ Authorization server receives authorization requests. The official number is 49.
Remote Address	Remote IP address of the TACACS+ Authorization server
Arg[0…1] (AV-pairs):	service=shell → Shell authorization

	cmd=	→ Get general access rights for console commands

The following TACACS+ Authorization attributes are read by the switch for user authorization:

Attribute	**Attribute contains …**
Auth Status	The status of the authorization request: PASS_ADD (0x01) → Authorization succeeded FAIL (0x02) → Authorization failed
Data	Data for authorization (not used)
Arg[0…1] (AV-pairs):	priv-lvl=0…15 → *Cisco* privilege level 0…15 of the requested user (unused by *Nexans* switches) nx-access=<*general access rights*> → The authorization reply must contain this *Nexans*-specific attribute. It tells the switch whether the user shall be logged in as Admin account (R/W) or User account (R/O). The following attribute values are admissible: NX-ACCESS-RW → Admin access rights (R/W) NX-ACCESS-RO → User access rights (R/O)

10.64.3. TACACS+ Attributes for Console User Accounting

If TACACS+ Accounting is enabled, the following TACACS+ attributes are transmitted from the switch to the TACACS+ Accounting server for user accounting:

Attribute	**Attribute contains …**
Auth Method	Accounting method to be applied: TACACSPLUS (0x06)
Privilege Level	*Cisco* privilege level 0…15 of the requested user (unused by *Nexans* switches)
Authentication type	Authentication type to be used. The only currently supported type is: ASCII (1)
Service	Service protocol to be used. The only currently supported type is: PPP (3)
User	User name
Port	The TCP port number on which the TACACS+ Accounting server receives accounting requests. The official number is 49.
Remote Address	Remote IP address of the TACACS+ Accounting server
Arg[0…2] (AV-pairs):	task_id=<*id*> → Task ID to identify the AAA action timezone=UTC → Timezone for accounting records in log file (UTC) service=shell → Shell accounting

If TACACS+ Accounting is enabled, the following TACACS+ Accounting attributes are read by the switch:

Attribute	**Attribute contains …**
Auth Status	The status of the accounting request: Success (0x01) → Accounting succeeded Error (0x02) → Accounting failed
Data	Data for accounting (not used)

10.65. TACACS+ Console Command Authorization

If Console Command Authorization is enabled for TACACS+, each console command will be authorized via TACACS+ Authorization server.

TACACS+ authorization of console commands is as follows:

- The user enters the console command.
- The switch sends a TACACS+ authorization request with the console command to the TACACS+ Authorization server.
- The TACACS+ Authorization server checks if the user is allowed to execute the command, and answers with an authorization reply containing the status “PASS_ADD“ or “FAIL”.
- If an authentication reply with status “FAIL“ is received, the error message “Command not allowed for user ‘xyz’” will be displayed at the console prompt.
- If an authentication reply with status “PASS_ADD“ is received, the command will be executed.
- If no TACACS+ Authorization server responds depending on the set server request algorithm (timeout), the behavior depends on the TACACS+ Authentication mode configured for the respective console:

  TACACS+ only:
  Executing the console command is denied.

  TACACS+ first, then local:
  The general access rights retrieved on user authorization will be used to authorize the console command.
- If TACACS+ Accounting is enabled, and the command has been executed, the switch sends the console command to the TACACS+ Accounting server via TACACS+ accounting request.
- The TACACS+ Accounting server records the executed command in a log file, and answers with an accounting reply containg the status “Success“ or “Error”.

If Console Command Authorization is disabled, the general access rights retrieved on user authorization will be used to authorize console commands.

10.65.1. TACACS+ Attributes for Console Command Authorization

The following attributes are sent from the switch to the TACACS+ Authorization server for console command authorization:

Attribute	**Attribute contains …**
Auth Method	Authorization method to be applied: TACACSPLUS (0x06)
Privilege Level	*Cisco* privilege level 0…15 of the user, for whom the console command shall be authorized (unused by *Nexans* switches)
Authentication type	Authentication type to be used. The only currently supported type is: ASCII (1)
Service	Service protocol to be used. The only currently supported type is: PPP (3)
User	User name
Port	The TCP port number on which the TACACS+ Authorization server receives authorization requests. The official number is 49.
Remote Address	Remote IP address of the TACACS+ Authorization server
Arg[0…*n*] (AV-pairs):	service=shell → Shell authorization cmd=<*command*> → command (argument 0) cmd-arg=<*command argument i*> → command argument *i*, *i* = 1...(*n*-1) cmd-arg=<cr> → command terminator (“carriage return”) **Example:** `show config tacacs+` → cmd=show, cmd-arg=config, cmd-arg=tacacs+, cmd-arg=<cr>

The following TACACS+ Authorization attributes are read by the switch for console command authorization:

Attribute	Attribute contains …
Auth Status	The status of the authorization request: PASS_ADD (0x01) → Authorization succeeded FAIL (0x02) → Authorization failed
Data	Data for authentication (not used)

10.65.2. TACACS+ Attributes for Console Command Accounting

If TACACS+ Accounting is enabled, the following TACACS+ attributes are transmitted from the switch to the TACACS+ Accounting server for console command accounting:

Attribute	Attribute contains …
Auth Method	Accounting method to be applied: TACACSPLUS (0x06)
Privilege Level	*Cisco* privilege level 0…15 of the user, for whom the executed console command shall be recorded (unused by *Nexans* switches)
Authentication type	Authentication type to be used. The only currently supported type is: ASCII (1)
Service	Service protocol to be used. The only currently supported type is: PPP (3)
User	User name
Port	The TCP port number on which the TACACS+ Accounting server receives accounting requests. The official number is 49.
Remote Address	Remote IP address of the TACACS+ Accounting server
Arg[0…3] (AV-pairs):	task_id=<*id*> → Task ID to identify AAA action timezone=UTC → Timezone for accounting records in log file (UTC) service=shell → Shell accounting cmd=<*complete command*> <cr> → Complete console command + command terminator (“carriage return”) **Example:** `show config tacacs+` → cmd=show config tacacs+ <cr>

If TACACS+ Accounting is enabled, the following TACACS+ Accounting attributes are read by the switch for console command accounting:

Attribute	Attribute contains …
Auth Status	The status of the accounting request: Success (0x01) → Accounting succeeded Error (0x02) → Accounting failed
Data	Data for accounting (not used)

10.66. TACACS+ SCP Authentication Modes

Seven different authentication modes can be selected for SCP:

- Local: Local authentication
- Radius Only: Authentication through the RADIUS server only
- Radius first, then local: Authentication through RADIUS. If no server response, local authentication.

- TACACS+ Only: Authentication through the TACACS+ server only
- TACACS+ first, then local: Authentication through TACACS+. If no server response, local authentication.
- Use SSHv2 mode SSHv2 authentication mode is used
- Disabled: SCP Interface disabled

Use SSHv2 mode (Factory-Default):
Local:
Disabled:
See chapters *10.50 SCP Authentication Mode.*

Radius only:
Radius first, then local:
See chapter *10.58 RADIUS SCP Authentication Modes*

TACACS+ Only:
TACACS+ first, then local:
The authentication resp. authorization procedure is principally identical with the console authentication via TACACS+ server (see chapter *10.64 TACACS+ Console Authentication Modes*).

10.67. TACACS+ Server Configuration

Basically, one set of TACACS+ servers can be used for authentication, authorization and accounting. However, it is possible to configure separate server sets for each AAA service.

A TACACS+ server is a dedicated *Linux* or *Windows* PC with running a TACACS+ service or daemon.

10.67.1. TACACS+ Server for Linux

For *Linux* machines the TACACS+ daemon `tac_plus` version F4-0.04.27a or higher is recommended.

To run daemon `tac_plus` on *Linux* machines with *Debian* / *Genome* operating system, you must install package `tacacs+`:

```
sudo apt-get install tacacs+
```

To configure AAA on the TACACS+ daemon, you must edit the configuration file `tac_plus.conf`. By default, the configuration file of the TACACS+ daemon can be found under

```
/etc/tacacs+/tac_plus.conf
```

For details see the man pages of package `tac_plus` and of configuration file `tac_plus.conf`.

However, to enable user authentication you must enshure that at least the TACACS+ Authorization server configuration provides the *Nexans*-specific attribute ‘nx-access’ in the `exec` section of the user or group the user belongs to:

```
service = exec {
    priv-lvl = 0...15
    nx-access = {NX-ACCESS-RW | NX-ACCESS-RO}
}
```

Example:

```
# Define where to log accounting data, this is the default.
accounting file = /var/log/tac_plus.acct

# This is the key that clients have to use to access Tacacs+
key = TestKey


...

# users accounts
```

```
user = admin1 {
    member = read-write-user
    login = des VitaoDJb1.c7M
    name = "admin1 login"
}

user = user1 {
    member = read-only-user
    login = cleartext "nexans"
    name = "user1 login"
    cmd = show {
        # user1 can run the following show command
        permit terminal
        deny .*
    }
    cmd = ping {
        permit .*
    }
}


# We can also specify rules valid per group of users.
group = read-write-user {
    default service = permit
    service = exec {
        priv-lvl = 15
        nx-access = NX-ACCESS-RW
    }
    cmd = show {
        permit .*
    }
    cmd = conf {
        permit .*
    }

    enable = cleartext ena
}

group = read-only-user {
    service = exec {
        priv-lvl = 1
        nx-access = NX-ACCESS-RO
    }
    cmd = show {
        permit .*
    }
    cmd = conf {
        deny .*
    }
    cmd = exit {
        permit .*
    }
}
```

10.67.2. TACACS+ Server for Windows

For *Windows* machines the TACACS+ server `tacacs.net` version v1.1.2 or higher is recommended.

To run `tacacs.net` on *Windows* machines, you must install package `tacacs.net`.

This SW can be downloaded from the homepage www.tacacs.net/download.

To configure AAA in `tacacs.net`, you must edit the following configuration XML files, which by default can be found under *C:\ProgramData\TACACS.net\config*:

- `tacplus.xml`
- `clients.xml`
- `authentication.xml`
- `authorizatiom.xml`

For details see the online documentation under www.tacacs.net/documentation.

However, to enable user authentication you must enshure that at least the TACACS+ Authorization server provides the *Nexans*-specific attribute 'nx-access' in the `<AutoExec>` section of the user or group the user belongs to (configuration file `authorizatiom.xml`):

```
<AutoExec>
  <Set>priv-lvl=15</Set>
  <Set>nx-access={NX-ACCESS-RW | NX-ACCESS-RO}</Set>
</AutoExec>
```

Example:

`authentication.xml`:

```
<Authentication xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <UserGroups>
    <UserGroup>
      <Name>read-write</Name>
      <AuthenticationType>File</AuthenticationType>
        <Users>
            <User>
              <Name>admin1</Name>
              <LoginPassword ClearText="" DES="VitaoDJb1.c7M"> </LoginPassword>
              <EnablePassword ClearText="ena" DES=""></EnablePassword>
            </User>
            ...
          </Users>
    </UserGroup>

    <UserGroup>
      <Name>read-only-user</Name>
        <Users>
            <User>
              <Name>user1</Name>
              <AuthenticationType>File</AuthenticationType>
              <LoginPassword ClearText="nexans" DES=""> </LoginPassword>
              <EnablePassword ClearText="ena" DES=""></EnablePassword>
            </User>
            ...
          </Users>
    </UserGroup>
    ...
  </UserGroups>
</Authentication>
```

`authorizatiom.xml`:

```
<Authorizations xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <Authorization>
        <UserGroups>
            <UserGroup>read-write-user</UserGroup>
        </UserGroups>
        <AutoExec>
            <Set>priv-lvl=15</Set>
            <Set>nx-access=NX-ACCESS-RW</Set>
```

```
        </AutoExec>

        <Shell> <!--note that the login and exit commands are always permitted-->
            <Permit>.*</Permit> <!--This will allow all show commands -->
            <Deny>.*</Deny>     <!--This will deny all other commands -->
        </Shell>
        <Services>
            <Service>
                <Set>service=ppp</Set>
                <Set>protocol=ip</Set>
            </Service>
        </Services>
    </Authorization>

    <Authorization>
        <UserGroups>
            <UserGroup>read-only-user</UserGroup>
        </UserGroups>
         <AutoExec>
            <Set>priv-lvl=1</Set>
            <Set>nx-access=NX-ACCESS-RO</Set>
        </AutoExec>
        <Shell>
            <Permit>.*show.*</Permit> <!--This will allow all show commands -->
            <Permit>.*ping.*</Permit>
            <Deny>.*</Deny>           <!--This will deny all other commands -->
        </Shell>
    </Authorization>
</Authorizations>
```

10.68. Acess Control Lists (ACLs)

Access Control Lists (*ACLs*) consist of a set of rules to control network traffic. By simple rules, the switch can be configured to permit or deny IP addresses, protocols, MAC addresses in specific VLANs and/or per interface. The rules have priorities, that allow to define which rules will be matched first.

On HW5 switches ACLs can be configured as *static Access Control Lists* (*static ACLs*, *SACLs*) on the switch or sent by a RADIUS server as *dynamic Access Control Lists* (*dynamic ACLs*, *DACLs*).

Nexans switches support 200 rules that can be put together in 64 ACLs.

Every interface supports multiple ACLs, and every rule can be assigned to multiple ACLs.

If the user has defined conflicting or overlapping rules, the matching result and action applies depend on the rule's priority.

10.68.1. ACL General Configuration Steps

Basically, to apply an ACL to a port, the following steps must be performed:

1. Create ACL for the port
2. Create rules that apply for the ACL
3. Add rules to the ACL
4. Add ACL to the port (interface)

For this purpose, console commands are defined which are described in more detail in the subsequent chapters.

The NEXMAN provides an edit field “Acces Control List Commands” on tab “Acces Control List” where you can enter the corresponding console commands in the correct order.

10.68.2. ACL Global Settings

To use ACL for any port, ACL must be globally enabled. *Static* and *dynamic ACLs* can be enabled or disabled independently of each other:

```
acl {dynamic|static} {enable|disable}
```

To delete all static ACLs or stored dynamic ACLs from the RADIUS server, the following command must be entered, respectively:

```
acl {dynamic|static} clear
```

NOTE:

Every manipulating command of Static and Dynamic Access Control Lists must be confirmed by the renew command.

10.68.3. ACL Rules Definition

Nexans switches support IPv4, IPv6 and MAC-based rules. The rules are sorted in a specific order. The order is defined by the rule’s priority. When a packet matches a rule, the device stops the match process and performs the deny or permit action defined in the rule.

The rules definitions consist of the following attributes, where every unused parameter except ‘action’ can be replaced by the key word `any`:

Attribute	Default Value	Function
priority number	any	The priority of the rule. The lower the priority number, the higher is the priority of the rule. Valid values are: any | 1…200
VLAN	any	The VLAN the rule applies for. Valid values are: any | 1…4094
action	permit	The action defined by the rule: permit | deny
IPv4 / IPv6 protocol	any	**For IPv4 / IPv6 Layer 3 rules:** The IPv4 or IPv6 protocol the rule applies for. Valid values are: any | TCP | UDP | 1…*YYY*, where *YYY* is the protocol number defined by IANA in RFC 790.
source IP address	any	**For IPv4 Layer 3 rules:** The source IPv4 address the rule applies for.
source port number	any	**For IPv4 Layer 3 rules:** The source port number the rule applies for.
destination IP address	any	**For IPv4 / IPv6 Layer 3 rules:** The destination IPv4 or IPv6 address the rule applies for.
destination port number	any	**For IPv4 / IPv6 Layer 3 rules:** The destination port number the rule applies for.
MAC ethertype	any	**For MAC Layer 2 rules:** The MAC EtherType the rule applies for. Valid values are: any | 1…*YYY*, where *YYY* is the EtherType number defined by IANA in RFC 7042.
source MAC address	any	**For MAC Layer 2 rules:** The source MAC address the rule applies for.
destination MAC address	any	**For MAC Layer 2 rules:** The destination MAC address the rule applies for.

10.68.3.1. Create IPv4 / IPv6 Layer 3 Rules

Based on the source and/or destination IP addresses and protocols, *Nexans* switches support filtering of Layer 3 traffic. For this purpose, one of the subsequent IPv4 / IPv6 Layer 3 Rules must be created.

Create IPv4 TCP/UDP Layer 3 Rules

For TCP/UDP Layer 3 traffic it's possible to define source and destination IPv4 addresses, and source and destination port numbers of TCP/UDP protocols. The following command must be used for this:

```
rule create (1…200) vlan {(1…4095)|any} {permit|deny} ipv4 protocol {tcp|udp}
source {any|<ip-addr>[/ (1…32)]} port {any|(1…YYY)} destination {any|<ip-
addr>[/(1…32)]} port {any | (1…YYY)}
```

Create Other IPv4 Layer 3 Rules

To filter non-TCP/UDP IPv4 Layer 3 traffic, the IP protocol number defined by IANA will be used. The list of IP protocol numbers can be found in RFC 790. The associated command is:

```
rule create (1…200) vlan {(1…4095)|any} {permit|deny} ipv4 protocol
{any|(1…YYY)} source {any|<ip-addr>[/ (1…32)]} destination {any|<ip-addr>[/
(1…32)]}
```

To match complete IPv4 traffic, you must use the following command:

```
rule create (1…200) vlan {(1…4095)|any} {permit|deny} ipv4 any
```

Create IPv6 TCP/UDP Layer 3 Rules

For TCP/UDP IPv6 Layer 3 traffic the destination IPv6 address and the destination port number of TCP/UDP protocols can be defined. The following command must be used for this:

```
rule create (1…200) vlan {(1…4095)|any} {permit|deny} ipv6 protocol {tcp |
udp} destination {any | <ipv6-addr>[/ (1…128)]} port {any | (1…YYY)}
```

Create Other IPv6 Layer 3 Rules

To filter non-TCP/UDP IPv6 Layer 3 traffic, the IP protocol number defined by IANA will be used. The list of IP protocol numbers can be found in RFC 790. The associated command is:

```
rule create (1…200) vlan {(1…4095)|any} {permit|deny} ipv6 protocol {any |
(1…YYY) } destination {any | <ipv6-addr>[/ (1…128)]}
```

To match complete IPv6 traffic, you must use the following command:

```
rule create (1…200) vlan {(1…4095)|any} {permit|deny} ipv6 any
```

10.68.3.2. Create MAC Layer 2 Rules

To filter MAC Layer 2 traffic, the source and destination MAC addresses, and the EtherType number defined by IANA will be used. The list of EtherType numbers can be found in RFC 7042. The associated command is:

```
rule create (1…200) vlan {(1…4095)|any} {permit|deny} mac etype {any|1…YYY)}
source {any | <mac-addr>[/ (1…48)]} destination {any | <mac-addr>[/(1…48)]}
```

To match complete MAC Layer 2 traffic, you must use the following command:

```
rule create (1…200) vlan {(1…4095)|any} {permit|deny} mac any
```

10.68.3.3. Delete Rule

Every rule can be deleted by it’s priority number using the following command:

```
rule delete (1…200)
```

10.68.3.4. Overwrite Rule

By the creation of a rule the existing rule with the same priority number will be overwritten, and the rule’s assignments to ACLs will be removed.

10.68.4. ACL Definition

An ACL is defined by it’s unique name. The configuration of an ACL consists of a sequence of rules assigned to the ACL. ACLs can be assigned to ports or removed from ports.

10.68.4.1. Create ACL

To create an ACL, the following commands must be used:

```
acl create [<string max. 64 chars>] (max. 64 ACLs allowed)
```

10.68.4.2. Delete ACL

To delete an ACL, the following commands must be used:

```
acl delete [<string max. 64 chars>] (max. 64 ACLs allowed)
```

10.68.4.3. Add Rule to ACL

To add a rule to an ACL, the following command must be used:

```
acl a:dd [<string max. 64 chars>] r:ule (1..200)
```

10.68.4.4. Remove Rule from ACL

To remove it from an ACL, the following command must be used:

```
acl r:emove [<string max. 64 chars>] r:ule (1..200)
```

10.68.5. ACL Assignment to Interfaces

ACLs can be assigned to one or more interfaces. For this purpose, the ACL is added to the corresponding interfaces by referencing its unique name.

10.68.5.1. Add ACL to Interface

To add an ACL to an interface, the following command must be used:

```
interface {if-no range} acl add [<string max. 64 chars>]
```

10.68.5.2. Remove ACL from Interface

To remove an ACL from an interface, the following command must be used:

```
interface {if-no range} acl remove [<string max. 64 chars>]
```

10.68.6. Static ACLs

Static ACLs are statically defined on the ACL configuration and assigned to the ports.

There are two commands that show static Access Control Lists:

```
show acl static
```

or

```
show conf acl
```

10.68.7. Dynamic ACLs

Nexans switches support *dynamic* or *downloadable ACLs*. The RADIUS server can send them with the *Accept Command NAS-Filter-Rule* attribute (RFC-4849). Because the port with the attached device is not necessarily known to the RADIUS server, there is the possibility to implicitly assign the attached port to ACLs.

```
interface dacl [<ACL string max. 64 chars>]
```

The switch supports simultaneously static and dynamic ACLs. To avoid overlapping of rules belonging to static and dynamic ACLs, the switch removes port's assignment to static ACLs on the ports, where the successful 802.1x or MAC authentication with dynamic ACLs took place. On removal of the authenticated device, the dynamic ACLs stored for the device will be removed, too.

To show dynamic ACLs received from the RADIUS Server, the following command must be used:

```
show acl dynamic
```

Example:

```
# show acl dynamic
!--< Access Control List dynamic received from RADIUS server. >--------

If MAC Address
-- -----------------
6  00:C0:29:29:2E:98
acl create UDP_TRAFFIC
rule create 6 vlan 20 permit ipv4 protocol udp source any port 20 destination
any port 30
acl add UDP_TRAFFIC rule 6
interface dacl UDP_TRAFFIC

If MAC Address
-- -----------------
```

```
7  00:1E:13:8C:7C:78
acl create TCP_TRAFFIC
rule create 5 vlan 20 permit ipv4 protocol udp source any port 20 destination
any port 30
acl add TCP_TRAFFIC rule 5
interface dacl TCP_TRAFFIC
```

10.68.8. Active ACLs

The *active ACLs* are the resulting static and dynamic ACLs when applying the dynamic ACLs to the respective ports.

After receiving dynamic ACLs from the RADIUS Server, the switch performs the following steps to get the active ACLs:

- Build the static ACL configuration.
- Remove the ports from the configuration, where successful 802.1x or MAC authentication took place and the RADIUS Server sent the NAS-filter rules with dynamic ACL.
- Process the dynamic ACLs and the results are the active ACLs.

To show the active ACLs, the following command must be used:

```
show acl active
```

10.68.9. ACL Status

To show the assignments of ACLs to ports, the following command must be used:

```
show acl status
```

Example:

```
# show acl status
If            ACL      ACL
No Name       Assigned Name
-- ---------- -------- ----------------------------------------------------
6  TP-06      Dynamic  UDP_TRAFFIC
7  TP-07      Dynamic  TCP_TRAFFIC
8  TP-08      Static   SOME_STATIC_ACL
```

10.68.10. ACL Strategies

There are two general strategies for traffic filtering. The first strategy is to allow all traffic, and with ACL certain network traffic is banned. By default, the switch lets all packets through the switch engine, so with this strategy the administrator must ban certain traffic with deny rules. For example, to ban TCP IPv6 traffic, it is enough to set following ACL:

Example:

Allow all traffic and ban only TCP IPv6 traffic on port 5:

```
#acl create TCP_IPv6_TRAFFIC
#rule create 1 vlan any deny ipv6 protocol tcp source any port any destination
any port any
#acl add TCP_IPv6_TRAFFIC rule 1
#interface 5 acl add TCP_IPv6_TRAFFIC
```

The other strategy, that offers more security, is to permit certain traffic and all other packets are banned. On *Nexans* switches you must ban explicitly IPv4, IPv6 and Ethertype traffic, and the corresponding rules must have lowest priority and complete the ACL table.

Example:

On ports 6, 7, 8 and 9 allow only IPv4 ICMP packets and ban other traffic:

```
#acl create ICMP_PERMIT
#rule create 1 vlan any permit ipv4 protocol 1 source any destination any
#rule create 197 vlan any deny ipv6 any
#rule create 198 vlan any deny ipv4 any
#rule create 199 vlan any deny mac any
#acl add ICMP_PERMIT rule 1
#acl add ICMP_PERMIT rule 197
#acl add ICMP_PERMIT rule 198
#acl add ICMP_PERMIT rule 199
#interface 6-9 acl add ICMP_PERMIT
```

10.68.11. ACL Examples

10.68.11.1. Block SSH Traffic

Create a static ACL to block SSH traffic from IP address 192.168.0.3 on port 6 with priority 5:

```
#acl create SSH_DENY
#rule create 5 vlan any deny ipv4 protocol tcp source 192.168.03 port 22
destination any port 22
#acl add SSH_DENY rule 5
#interface 6 acl add SSH_DENY
```

10.68.11.2. Permit ICMP Traffic

Create a static ACL to permit ICMP traffic on port 9 with priority 6 (the ICMP protocol has EtherType 1).

```
#acl create ICMP_PERMIT
#rule create 6 vlan any permit ipv4 protocol 1 source any destination any
#acl add ICMP_PERMIT rule 6
#interface 9 acl add ICMP_PERMIT
```

10.68.11.3. Dynamic ACL Configuration on RADIUS Server (*Freeradius*)

On the RADIUS server *Freeradius* for *Linux* the per-user configuration is usually saved in the configuration file `/etc/freeradius/users`. To configure the *Freeradius* server to send NAS-filter rules with *Nexans* dynamic ACLs, you can use the command for implicit dynamic ACL port's assignment or explicit port's assignment:

```
#implicit port's assignment
CP-7945G-SEP001E138C7C78      Auth-Type := Accept
    Service-Type = Administrative-User,
    Nas-FILTER-Rule = "acl create TCP_PROTOCOL",
    Nas-FILTER-Rule += "rule create 5 vlan 20 permit ipv4 protocol tcp source
any port 20 destination any port 30",
    Nas-FILTER-Rule += "acl add TCP_PROTOCOL rule 5",
    Nas-FILTER-Rule += "interface dacl TCP_PROTOCOL "


#explicit port's assignment
CP-7945G-SEP001E138C7C78      Auth-Type := Accept
    Service-Type = Administrative-User,
    Nas-FILTER-Rule = "acl create TCP_PROTOCOL",
    Nas-FILTER-Rule += "rule create 5 vlan 20 permit ipv4 protocol tcp source
any port 20 destination any port 30",
    Nas-FILTER-Rule += "acl add TCP_PROTOCOL rule 5",
    Nas-FILTER-Rule += "interface 6 acl add TCP_PROTOCOL ",
```

10.69. Internet Group Management Protocol (IGMP)

The Internet Group Management Protocol (IGMP) is a network protocol of the internet protocol family and serves to organize multicast groups. It is based on the Internet Protocol (IP) and allows IP multicasting (group communication). IP multicasting is the simultaneous distribution of IP packets under one IP address to several stations. IGMP offers the possibility to dynamically manage groups. Management is not performed in the sending station, but in the routers or switches to which the receivers of a multicast group are directly connected. IGMP offers functions by which a station informs a router that it wants to receive multicast IP packets from a certain multicast group. The sender of multicast IP packets does not know which and how many stations are going to receive its packets. This is because it only sends a single data packet to its superordinate router. If necessary, the router duplicates the IP packet, if it has several outbound interfaces with receivers.

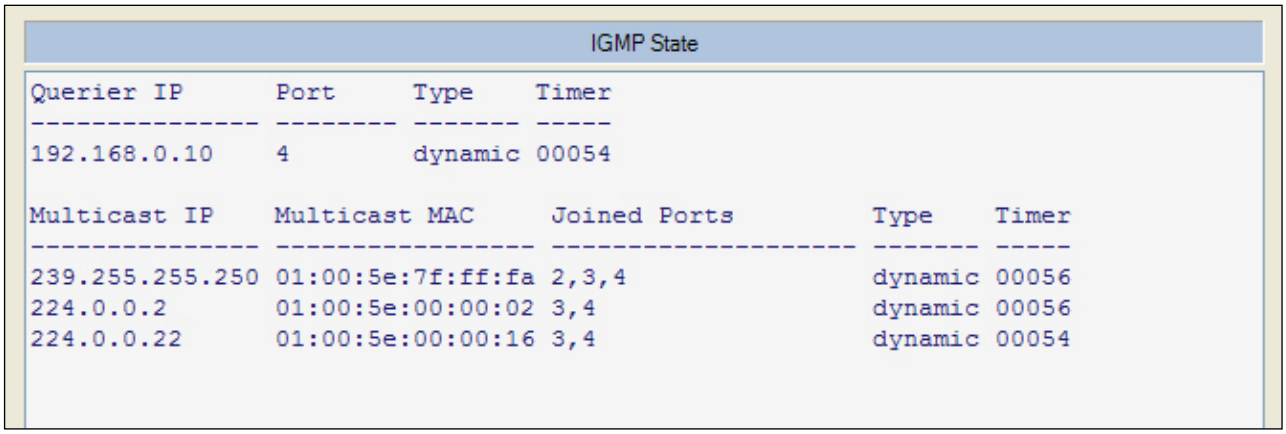
By means of IGMP Snooping you can prevent that multicast traffic is flooded on all switch ports. This will reduce the network load.

10.69.1. IGMP Snooping

With activated IGMP Snooping the switch is snooping into the IGMP traffic on its ports. Only ports which have joined a multicast group (via Membership report or Join Group) will be entered into the forwarding table for this multicast address. Ports leaving the group (via Leave-Group) will be removed from the table. Moreover, those groups are removed for which no Membership report has been received for a certain period of time.

Furthermore, the switch is snooping which port the IGMP Querier is connected to.

Via the "Show IGMP State" button in NEXMAN or the "show igmp status" console command it is possible to display the active querier and the IGMP forwarding table:



The following table shows a summary of all IGMP snooping settings:

Designation in NEXMAN	Default Value	Function
IGMP Snooping enable	disabled	If selected, the IGMP Snooping function is activated.
Snoop Table Ageing Time (seconds)	60	A group is deleted, if no membership report for this group has been received over the configured time period.
Accept IGMP Version 1	disabled	If selected, IGMP-V1 packets will be accepted and analysed. If disabled, these packets will be ignored.
Accept IGMP Version 2	enabled	If selected, IGMP-V2 packets will be accepted and analysed. If disabled, these packets will be ignored.
Accept MLD Version 1	disabled	If selected, MLD-V1 packets will be accepted and analysed. If disabled, these packets will be ignored.
Accept MLD Version 2	disabled	If selected, MLD-V2 packets will be accepted and analysed. If disabled, these packets will be ignored.

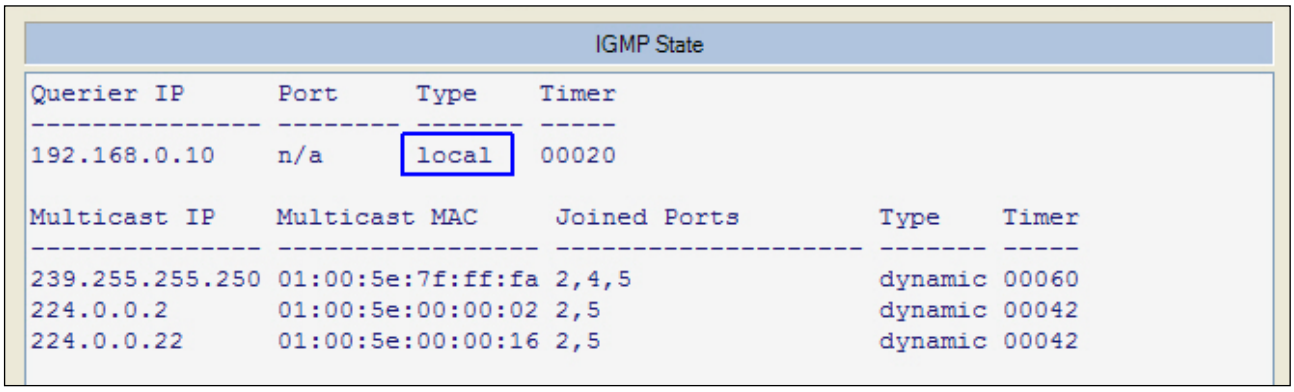
IGMP Immediate Leave Mode	Accept from User Ports only	This parameter defines the treatment of 'IGMP Immediate Leave Messages'. By sending this IGMP message a connected terminal unit may request its immediate leaving of a multicast group. Independent of the Immediate Leave possibility, ports will be automatically deleted from the multicast group after expiration of the above 'Snoop Table Ageing Time'. The following settings are possible: • Accept Leave messages from User Ports only • Accept all Leave messages • Ignore all Leave messages **Accept Leave messages from User Ports only:** This is the factory default. It accepts only Leave Messages received by user ports. Via the 'Link type' setting you can define which ports are user ports or uplink ports. If Spanning Tree is enabled, Leave Messages will only be accepted by edge ports. In particular with ring topologies this setting is required for an error-free operation. **Accept all Leave messages:** Leave Messages are principally accepted by each port. **Ignore all Leave messages:** Leave Messages are principally ignored

10.69.2. IGMP Querier

If the IGMP Querier is activated, the switch will send IGMP-V1/V2 query packets on all ports. Then all connected terminal units, which have joined a group, have to send a new membership report. Based on the membership reports the IGMP snooping function can update its forwarding table.

The applicable RFC stipulates that only one active querier is allowed per segment. If there are several queriers in the same segment activated on different switches, only the querier with the lowest IP address is allowed to continue the transmission. All other queriers have to withdraw.

If the current Nexans switch is working as an active querier, this will be indicated in the IGMP Status by the 'local' type:



NOTE:
It makes sense that the function of the querier in a network is performed by the core switch. The querier function on the Nexans switches should only be activated, if it is an isolated segment (e. g. for controlling machines via Ethernet/IP protocol) and if there is no core switch present.

The following table shows a summary of all IGMP querier settings:

Designation in NEXMAN	Default Value	Function

IGMP Querier enable	disabled	If selected, the IGMP querier function is activated.
Query Interval (seconds)	20	The interval for sending IGMP query packets.

10.70. Link Layer Discovery Protocol (LLDP)

The LLDP (Link Layer Discovery Protocol) is a vendor-independent Layer 2 protocol defined according to the IEEE-802.1AB standard and enabling the exchange of information between neighbouring devices.

A software component, the so-called LLDP agent, is working on each device supporting LLDP. This agent is sending periodically information on itself and continually receiving information from neighbouring devices. This happens completely independent from one another. That is why the LLDP is called a "one-way" protocol, which does not establish any communication to other devices.

The following table shows a summary of the LLDP settings:

Designation in NEXMAN	Default Value	Function
LLDP Mode	Disabled	Here you can choose between two different modes: • Disabled without LLDP filter No LLDP packets are sent by the switch, but the switch is transparent to LLDP packets. This means that LLDP packets received from connected devices are forwarded to other ports within the same VLAN. • Disabled with LLDP filter No LLDP packets are sent by the switch. In addition, the switch filters LLDP packets received from connected devices so that no LLDP packets are forwarded to other ports. • Enabled In line with the parameters described below, LLDP packets are sent on all ports. • Enabled with LLDP forwarding to Uplink In addition to the ‘Enabled’ setting, LLDP packets from terminal units, e. g. IP phones, if connected, are forwarded to the uplink. This means, that both the Nexans switch and all LLDP-compatible devices connected to it are displayed in the Neighbor Table of the core switch. IMPORTANT: For the forwarding to operate correctly, the 'Link Type' has to be set appropriately for all ports. Packets received on a User port are exclusively forwarded to Uplink/Downlink ports.
TX Message Interval (seconds)	30	The interval for sending LLDP packets.
TX Holdtime Multiplier	4	The 'TX Holdtime Multiplier' multiplied with the above 'TX Message Interval' equals the life time of the packet at the receiving station.

The following LLDP attributes are transmitted by the switch:

Attribute	Attribute contains...
Chassis ID TLV	MAC Address of Switch
Port ID TLV	Port Description (e.g... 'TP-1')
Time To Live TLV	TX Message Interval * TX Holdtime Multiplier
Port Description TLV	Port Description (e.g. 'TP-1')
System Name TLV	User defined switch name
System Description TLV	Device Description and Software Version

System Capabilities TLV	Bridge
Management Address TLV	IP Address
Port VLAN ID TLV	Default VLAN (Untagged)

10.71. LLDP for Media Endpoint Devices (LLDP-MED)

LLDP-MED is an extension of the LLDP standard according to ANSI standard TIA-1057. It has specifically been developed in order to exchange information between terminal equipment and switches.

In installations with LLDP-MED-enabled IP phones the Voice VLAN as well as the Layer 2 and Layer 3 priority values can be additionally transmitted via LLDP-MED to the IP phone. Here the Voice-VLAN ID configured on the corresponding port of the Nexans switch is used. The Layer 2 and Layer 3 Priority Values can separately be configured for the Application Type Voice and Voice Signaling.Thus an automatic configuration of the IP phone via LLDP-MED is possible.

Even if LLDP is enabled at the switch, the LLDP-MED TLVs shown below are only transmitted insite the LLDP packets if LLDP packets with LLDP-MED TLVs are received on the respective port. After a Link Down or if no LLDP-MED TLVs have been received for a longer period, the sending of the LLDP-MED TLVs is disabled again.

The following LLDP-MED attributes are transmitted by the switch:

TLV type	TLV contains …
LLDP-MED Capabilities TLV	Devicetyp and supported TLV types
Network Policy TLV	Voice VLAN ID Layer 2 priority value Layer 3 DSCP value
Extended Power Via MDI TLV	PoE type of the switch and PoE power in Watts that the switch can provide to the connected end device.
Location Identification TLV	Installation location of the switch

The following LLDP-MED attributes are analyzed by the switch:

Attribute	Attribute contains …
Network Policy TLV	Determination of the attribute subtype for which the Voice VLAN is needed.
Extended Power Via MDI TLV	PoE type of connected end device and requested power in watts.
Inventory TLV	The following Inventory TLVs are supported: HW revision FW revision SW revision Serial Number Manufactorer name Model Name

The following table shows an overview of the LLDP MED options of the Network Policy TLV:

Designation in NEXMAN	Default Value	Function
Layer 2 priority value Voice	0	Layer 2 Voice priority value that is send within the Network Policy (TIA-1057).
Layer 3 DSCP value Voice	0	Layer 3 Voice DSCP value that is send within the Network Policy (TIA-1057).
Layer 2 priority value Voice Signaling	0	Layer 2 Voice Signaling priority value that is send within the Network Policy (TIA-1057).
Layer 3 DSCP value Voice Signaling	0	Layer 3 Voice Signaling DSCP value that is send within the Network Policy (TIA-1057).

The following table shows an overview of the LLDP MED options of the Location Identification TLVs:

Designation in NEXMAN	Default Value	Function
Building (25)	<empty>	The name of a single building or structure
Unit (26)	<empty>	The name or number of a part of a building or structure
Place Type (29)	<empty>	The type of place. For example, a home, office, street, or other public space.

10.72. Cisco Discovery Protocol (CDP)

The CDP (Cisco Discovery Protocol) is a Layer 2 protocol offering the possibility of exchanging information between neighbouring devices.

Each message contains information such as device name, OS version, interface identifier, management IP addresses and packet hold time. If there is no periodic updating of the device information, the old information will be discarded after expiry of the hold time.

In installations with *Cisco* IP phones the Voice VLAN can be transmitted via CDP to the IP phone. Here the VLAN ID configured on the corresponding port of the Nexans switch is used. Thus, an automatic configuration of the *Cisco* IP phone is possible via CDP. Further information on configuring Nexans switches in a *Cisco* environment can be obtained from Nexans on request (keyword 'Cisco evaluation').

With switches with installed Power-over-Ethernet (PoE) option the available power, if any, is communicated to the terminal unit by CDP. This function is particularly relevant to *Cisco* access points with higher power consumption, since they do not boot correctly without the corresponding CDP information. The power requested via CDP by the terminal unit can be displayed using the ‘Show Neighbor Details’ function.

Important note: Since CDP is a CISCO proprietary protocol, generally the corresponding CISCO Private CDP-MIB cannot be supported. Instead, the discovery information collected via CDP on the standard LLDP-MIB can be read according to IEEE 802.1AB. However, as a precondition the CDP Mode must be set to “Enabled with entry in LLDP-MIB“.

The following table shows a summary of the CDP settings:

Designation in NEXMAN	Default Value	Function
CDP Mode	disabled	Here you can choose between three different modes: • Disabled without CDP filter No CDP packets are sent by the switch, but the switch is transparent to CDP packets. This means that LLDP packets received from connected devices are forwarded to other ports within the same VLAN. • Disabled with CDP filter No CDP packets are sent by the switch. In addition, the switch filters CDP packets received from connected devices so that no CDP packets are forwarded to other ports. • Enabled According to the parameters „TX Message Intervall“ und „TX Holdtime“, CDP packets are sent on all ports. IMPORTANT: Despite the 'Enabled' setting, Nexans Switch enables packets to be sent only when CDP packets are received from a neighbor device (e.g., *Cisco* core switch). This prevents CDP packets from being sent to the network in a non-*Cisco* environment. • Enabled with CDP forwarding to Uplink In addition to the 'Enabled' setting, CDP packets from connected end devices (such as IP phones) are forwarded to the uplink. This means that the core switch sees both the Nexans Switch and all connected

		CDP-capable devices in the neighbor table. IMPORTANT: For the forwarding to work correctly, the 'LinkType' must be set accordingly for all ports. Packets received on a 'user' ports will only be forwarded to 'uplink / downlink' ports. • Enabled with entry in LLDP-MIB In addition to the above setting 'Enabled', all CDP Neighbor entries can be queried via the LLDP-MIB. If LLDP is also activated, the LLDP-MIB contains both LLDP and CDP neighbors. The different entries in the lldpRemTable MIB tree are filled with the CDP TLVs as follows: lldpRemChassisIdSubtype(4) = Fixed value: local(7) lldpRemChassisId(5) = CDP TLV: Device-ID lldpRemPortIdSubtype(6) = Fixed value: local(7) lldpRemPortId(7) = CDP TLV: Port-ID lldpRemPortDesc(8) = CDP TLV: Port-ID lldpRemSysName(9) = CDP TLV: Device-ID lldpRemSysDesc(10) = CDP TLV: Platform lldpRemSysCapSupported(11) = Fixed value: Bridge lldpRemSysCapEnabled(12) = Fixed value: Bridge
TX Message Interval (seconds)	60	The interval for sending CDP packets. IMPORTANT: The switch only sends CDP packets if he receives CDP packets from his neighbour device.
TX Holdtime (seconds)	180	The 'TX Holdtime' defines the life time of the packet at the receiving station.

NOTE: The current firmware version V3.55 only supports the sending of CDP packets. This allows the Nexans switch to be indicated in the CDP Neighbor Table of the core switch.

10.73. Rapid Spanning Tree Protocol (RSTP)

The Rapid Spanning Tree Protocol (RSTP) is a network protocol designed to disable redundant paths in local networks or to enable them again, if needed (failure of a connection).

10.73.1. RSTP – General functional description

Networks should have one path only to each possible destination, in order to avoid that data packets (frames) are duplicated and arrive several times at the destination, which might cause failures in the above network layers and reduce the performance of the network. On the other hand, redundant network paths may be desired as backup in case of failures. The Spanning Tree algorithm fulfils both requirements.

For communication between the switches the Bridge protocol is used. The packets of this protocol are called Bridge Protocol Data Unit (BPDU).

First a so-called Root Bridge is chosen among the Spanning Tree-capable switches in the network. This Root Bridge will be the centre (root) of the tree to span. To achieve this, all switches send their Bridge ID to a specified multicast address. The Bridge ID is 8 bytes long (2 bytes for Bridge Priority and 6 bytes for the MAC address). The switch with the lowest ID will become the Root Bridge. In case of identical Bridge Priority values the MAC address of the switch is used (namely the switch with the lowest MAC address). From the Root Bridge the paths are determined, via which the other switches can be reached in the network. If redundant paths are available, the switches there need to set the corresponding port to 'Blocking'. The paths, on which communication is allowed, are determined on the basis of path cost which is transmitted by the switch there. The cost depends on the distance to the Root Bridge and on the available uplink to the destination. For example, a 10 Mbps uplink incurs higher cost than a 100 Mbps uplink to the same destination and thus would be discarded. In the same way each subnet in the switched LAN can only be reached via one single bridge, which is called the Designated Bridge. In a graphical representation this system presents itself like a tree of network paths - this is why this algorithm is called a 'spanning tree'.

All switches inform the switches, which are one level below them in the hierarchy, at the Hello Time interval (typically 2 seconds), that they are still available. If these Hello packets are missing, something must have changed in the topology of the network and the network must reorganise itself. With the old Spanning Tree Protocol this recalculation of the tree lasted up to 50 seconds in the worst case. During this time the

Spanning Tree-capable switches were not allowed to pass on any other packets than Spanning Tree information in the network. This was one of the weakest points of the Spanning Tree algorithm, because it is possible to signal a topology change using faked Spanning Tree packets and thus to block the whole network for up to 30 seconds. In order to remove this potential safety defect, but also to restore the operation of the network rapidly in case of real changes to the topology, the Rapid Spanning Tree Protocol (RSTP) was standardized. RSTP is based on the idea that the network structure is not immediately deleted upon signalled topology changes, but that work goes on as usual and alternative paths are calculated. Only then a new tree will be built. Thus the downtime of the network can be reduced from 30 seconds to values in the order of milliseconds. In the 2004 revision of the 802.1D standard, which was last revised in 1998, the old STP was dropped completely in favour of the RSTP.

The RSTP implementation in the Nexans switch is based on the current IEEE802.1D-2004 standard, which shows some improvements compared to the first RSTP revision IEEE802.1w.

10.73.2. RSTP - Global configuration parameters

Designation in NEXMAN	Default Value	Function
RSTP global enable	disable	Only if the Spanning Tree Protocol has been globally enabled here, all ports, which also have the Spanning Tree enabled, will be included in the calculation of the topology. Moreover, in case of a global activation of Spanning Tree all BPDU packets will be blocked and forwarded only to the CPU of the switch. IMPORTANT: If Spanning Tree has been globally disabled here, the switch will be transparent for the BPDU packets and any received BPDU packets will be forwarded to all ports.
Protocol version	STP and RSTP	The following two settings are possible: • STP and RSTP Here the RSTP protocol is preferably applied to all enabled ports. Only if STP packets are received on a port, the old STP protocol will automatically be used for this port. However, in this case the benefits of RSTP, such as short switchover times, are lost. • STP compatible Only the old STP protocol is used on all enabled ports. In this case the benefits of RSTP, such as short switchover times, are lost.
Bridge priority	32768	Here the switch priority can be set from 0 and 61440 (in steps of 4096). The switch with the lowest priority will become the Root Bridge. If two switches have the same priority, the switch with the lowest MAC address will become the Root.

Hello time (seconds) (1...10)	2	This setting fulfils two functions: a) Interval for sending BPDU packets: Indicates the interval within which all RSTP switches regularly send BPDU packets on all Designated Ports. When using the old STP protocol a Non-Root-Bridge will only generate BPDU packets, if it receives BPDU packets on its Root port. b) Timeout for RSTP For RSTP the port statuses will time out after 3 x Hello Time (typically 3 x 2 = 6 seconds). **IMPORTANT:** **As per IEEE802.1D standard the 'Hello time' value must be smaller or equal: ('Max. age/hops' ÷ 2) – 1** **If the 'Hello time' value is too big, it will automatically be corrected down to ('Max. age/hops' ÷ 2) – 1** NOTE: This setting is distributed by the Root Bridge to all other switches and thus ignored on all Non-Root Bridges.
Max. Age/hops (6...50)	20	This setting fulfils two functions: a) Max. number of switches for RSTP and STP: The Root Bridge sends BPDU packets with a age/hops value of '0' at the Hello-Time interval. Each following switch increases the age/hops value of the received BPDU by one and itself then sends BPDUs with the new (increased) age/hops value. If a switch receives a BPDU, whose age/hops value exceeds the Max. age/hops value, this BPDU will be discarded. b) Timeout for STP: When using the old STP protocol the port statuses will time out after expiration of the Max. age/hops value. NOTE: For RSTP the port statuses will already time out after 3 x Hello Time. **IMPORTANT:** **As per IEEE802.1D standard the 'Max. age/hops' value must be smaller or equal:** **2 x ('Forward delay' - 1)** **If the 'Max. age/hops' value is too big, it will automatically be corrected down to 2 x ('Forward delay' - 1).** NOTE: This setting is distributed by the Root Bridge to all other switches and thus ignored on all Non-Root Bridges.
Forward delay (seconds) (4...30(	15	The Forward Delay value indicates how long the switches shall wait in order to change the state of a port from Blocking to Learning and from Learning to Forwarding (2 x Forward Delay). If the switch is configured for RSTP under Protocol Version and if on the port a corresponding switch answers with RSTP packets, the changeover from Blocking to Forwarding will be performed by the RSTP protocol (without waiting for Forward Delay). If a port is configured as an Edge Port (PortFast), the Forward Delay is also ignored and the port is set to Forwarding immediately after a link-up. NOTE: This setting is distributed by the Root Bridge to all other switches and thus ignored on all Non-Root Bridges.
Transmit hold count (1...10)	6	Defines the maximum number of BPDU packets which may be sent per second and per port. This function shall protect the network from flooding with BPDU packets in case of errors.
Re-enable time for BPDU-Disabled ports (seconds)	0	Ports, which were disabled due to a received BPDU can optionally be re-enabled automatically after a time period of 1 to 60000 seconds. If the time is set to “0”, the port has to be re-enabled manually.

Debugging mode	Disable	If the debugging mode is enabled, detailed information on spanning tree status changes are written into the local log. IMPORTANT: This function should only be enabled after consultation with the manufacturer's support team.

10.73.3. RSTP - Port configuration parameters

Designation in NEXMAN	Default Value	Function

Spanning Tree mode	enable	Only if RSTP is enabled for the respective port, this port will be included in the calculation of the topology. Ports, for which Spanning Tree is disabled, will principally not send any BPDU packets, and received BPDU packets will be ignored and not forwarded to other port. Note on CISCO PVST+ packets: Ports, for which spanning tree is disabled, additionally block outgoing PVST+ packets. However, incoming PVST+ packets will not be blocked and forwarded to all ports in the same VLAN for which spanning tree is enabled. If the reception and forwarding of PVST+ packets shall be prevented, the spanning tree mode of the corresponding port should be set to “Disabled (BPDU disables Port)”. In this case the port will be disabled as soon as a spanning tree packet is received. Here you can select from three different modes: • Enabled The ports sends and receives BPDU packets and is included in the topology calculation. • Enabled (Ring Loop Protection) Same as “Enabled”, but additionally a periodic check is executed as to whether a ring loop exists. This security feature prevents that a loop is generated in the ring due to a fault in the spanning tree topology calculation. IMPORTANT: This feature should only be used for ring topologies and may only be enabled on one single switch in the ring and on one ring port. If a ring loop is detected, the port with enabled “Ring Loop Protection” will be disabled. In this case RING-LOOP-DISABLED will be indicated as the port’s link status and a Port Error Disable alarm will be send. Disabled ports have to be re-enabled manually. • Disabled (BPDU filter) The port does not send any BPDU packets and received BPDU packet are ignored. • Disabled (BPDU disables Port) The port does not send any BPDU packets and received BPDU packets will disable the port. In this case BPDU-DISABLED will be indicated as the port’s link status and a Port Error Disable alarm will be send. Optionally, disabled ports can automatically be re-enabled after a settable “Re-Enable Time for BPDU-Disabled Ports”. The time value can be set in the range from 1 to 60000 seconds. IMPORTANT: If Spanning Tree has been globally disabled, the switch will be transparent for the BPDU packets and any received BPDU packets will be forwarded to all ports of the same vlan.
Priority	128	Here the port priority can be set from 0 and 240 (in steps of 16). The port priority (4 bits) and the port number (12 bits) together form the Port ID. When comparing two Port IDs the one with the lower numerical value is the higher 'better' priority. The usual notation for the Port ID is: Port-Priority / Port Number

Path cost mode	Auto (RSTP)	This parameter can be used to determine the path cost of the port. Three different modes are available for selection: • Auto (RSTP) Here the path cost is automatically determined on the basis of the actual speed of the port. To this purpose, the default values proposed in the IEEE802.1D-2004 standard are used: 10Mbps = 2.000.000 100Mbps = 200.000 1Gbps = 20.000 10Gbps = 2.000 • Auto (STP) Here, too, the path cost is determined on the basis of the actual speed of the port. However, the default values from the old STP standard are used: 10Mbps = 100 100Mbps = 19 1Gbps = 4 10Gbps = 2 • Manual This option allows you to manually set the desired path cost (see Manual Path Cost parameter). In this case the speed of the port is ignored.
Manual path cost	Depending on maximum data rate of the port	If the Path Cost Mode is set to Manual, any value between 1 and 200,000,000 can be entered as path cost.
Edge Port	No	This parameter allows you to predefine, whether on this port no further switch with Spanning Tree protocol is expected (presumably a terminal device is connected). The setting used here will only serve as an initial value immediately after a link-up on the respective port. Due to the Auto-Edge function, which is enabled by default, the switch permanently checks whether the default value agrees with reality and adjusts the actually used Edge Port mode, if necessary (see Edge Port state parameter in Chapter *10.73.5. RSTP - Port state parameters*). Two different modes are available as default values: • No After a link-up it is first assumed that a switch with Spanning Tree protocol is connected to the respective port. So the port is initially set to Blocking and it is checked whether a switch is really answering by sending BPDU packets. If no switch answers within 15 seconds, the currently used Edge Port mode will automatically be changed to 'Yes' (see Edge Port state parameter in Chapter *10.73.5. RSTP - Port state* parameters). • Yes (PortFast) After a link-up it is first assumed that NO switch with Spanning Tree protocol is connected to the respective port (typically a terminal device). For that reason the port is immediately set to Forwarding. However, BPDU packets are sent nevertheless. If then a switch answers with BPDU packets, the currently valid Edge Port mode will automatically be changed to 'No' (see Edge Port state parameter in Chapter *10.73.5. RSTP - Port state parameters*).

Point-to-Point link	Yes (forced)	This parameter defines whether the port is connected to a switched port of a neighbouring switch or to a hub (half-duplex). Ports which are connected to a hub and which are no Edge Ports delay the rapid reconfiguration of the switch. In this case it is assumed that several Spanning Tree bridges are connected to the hub making a rapid switchover impossible. Three different modes are available as default values: • Yes (forced) (factory default) Independent of the current duplex mode it is defined that the port is connected to a switched port of a neighbouring switch. • No (forced) Independent of the current duplex mode it is defined that the port is connected to a hub segment. • Auto Depending on the current duplex mode, the actually used Point-to-Point mode is set. For a full- duplex connection a point-to-point link is assumed and for a half-duplex connection a connected hub segment is assumed (see Point-to-Point Link state parameter in Chapter *10.73.5. RSTP - Port state* parameters).

10.73.4. RSTP - Global state parameters

Description	Function
Root Bridge ID	This is the Bridge ID of the Root Bridge. A Bridge ID consists of eight bytes as an unsigned integer value. When comparing two Bridge IDs the one with the lower numerical value is the higher 'better' priority. The first two bytes contain the bridge priority. The last six bytes contain the MAC address and thus ensure the uniqueness of the Bridge ID in case of identical priority. The switch with the lowest numerical Bridge ID will become the Root Bridge. The usual notation for a Bridge ID is: Bridge Priority / MAC Address
Bridge State	Indicates whether this switch has the function of the Root Bridge or of a Designated Bridge.
Root Port	The port number of the Root Port. The Root Port is the port next to the Root Bridge. NOTE: The Root Bridge is the only switch without Root Port. In this case the value 0 is indicated as Root Port.
Root Cost	The path cost from the Root Port to the Root Bridge. NOTE: The Root Bridge is the only switch without Root Port. In this case the value 0 is indicated as Root Cost.
Learned Max Age	The Max Age learned by the Root Bridge.
Learned Hello Time	The Hello Time learned by the Root Bridge.
Learned Forward Delay	The Forward Delay learned by the Root Bridge.
Topology Changes	The number of topology changes. A topology change can be initiated by: • The addition of a data path • The failure of a data path • The addition of a Spanning Tree switch • The failure of a Spanning Tree switch A topology change is automatically detected and the network is reconfigured to restore a tree and that all devices in the tree can be reached. In this process not even preliminary loops occur.
Time since last Topology Change	The time which has elapsed since the last topology change.

10.73.5. RSTP - Port state parameters

Description	Function
State	Shows the current Spanning Tree state of the respective port. The following statuses are possible: • Forwarding The port is included in the active topology and forwards data. • Blocking The port is not included in the data transmission of the active topology. Only BPDU packets are sent and received. • Learning The port is not included in the data transmission of the active topology, but MAC addresses are learned. Only BPDU packets are sent and received. • No Link The port does not receive a link signal and thus is not included in the data transmission of the active topology.
Path Cost	Shows the path cost used for this port. For further information see Path Cost Mode parameter in Chapter *10.73.3. RSTP - Port configuration parameters*
Designated Root	This is the Bridge ID of the Root Bridge.
Designated Cost	Shows the path cost of this segment to the Root Bridge.
Designated Bridge	The Bridge ID of the switch, from which this port receives the best BPDUs. The usual notation for a Bridge ID is: Bridge Priority / MAC Address
Designated Port	The Port ID of the port via which the BPDUs are sent by the Designated Bridge. The usual notation for the Port ID is: Port Priority / Port Number
Port Role	Shows the role of the port in the Spanning Tree topology: • Root Port The Root Port is the port next to the Root Bridge based on the path cost. The Root Bridge is the only switch without Root Port. • Designated Port A Designated Port points downstream, i.e. from the Root-Bridge, and has the most favourable path cost to the segment in which it is situated. • Alternate Port An Alternate Port represents a (alternative) path to the Root and is not included in the active topology. If the Root Port fails, it is possible to rapidly switch over to the Alternate Port. • Backup Port A Backup Port is a path to a segment, to which this switch already has connected a Designated Port (with better path cost). That means, this port is not included in the active topology. If the Designated Port fails, it is possible to rapidly switch over to the Backup Port.
Edge Port	Shows if the port operates as Edge Port. Via the Edge Port configuration parameter (see Chapter *10.73.3. RSTP - Port configuration parameters*)) the initial value can be predefined immediately after a link-up. Due to the Auto Edge function, which is enabled by default, the switch permanently checks whether the configured default value agrees with reality and adjusts the actually used Edge Port mode, if necessary. In order to be detected as Edge Port all sorts of devices, such as routers, servers, PCs a.s.o., may be connected to the respective port. However, it is important that these devices do not have any Spanning Tree functionality and thus do not send any BPDU packets.

Point-to-Point Link	Shows, if the port operates as point-to-point link. Via the Point-to-Point Link configuration parameter (see Chapter *10.73.3. RSTP - Port configuration* parameters) the mode can be fixed or assigned dynamically using the Auto option. If Auto is selected, a point-to-point link is assumed for a full- duplex connection, while for a half-duplex connection a connected hub segment is assumed and the point-to-point state is indicated as No. In this case it is assumed that several Spanning Tree switches are connected to the hub making a rapid switchover in case of faults impossible.
Spanning Tree Protocol detected	Shows if BPDU packets are sent and received on the port according to the old STP standard. This may be due to two causes: a) Although the switch is configured for RSTP under Protocol Version, BPDU packets according to the old STP standard are received on the port. In this case the switch will set the respective port into the compatibility mode and then itself send STP packets, too. However, thus the benefits of the Rapid Spanning Tree will be lost for the whole switch. b) The switch is configured for STP Only under Protocol Version and BPDU packets according to the old STP standard are received on the port, too.

10.73.6. RSTP – Configuration notes

The following rules have to be observed when setting up a Spanning Tree network:

- All infrastructure components in the network, which do not actively support the Spanning Tree Protocol, must be transparent for Spanning Tree messages (BPDUs) and forward all BPDUs without any change to all ports.

- Media converters, which are looped into the Spanning Tree data path, must not learn MAC addresses. Frequently such converters are simple two-port switches with corresponding address tables. In case of faults this may result in an extension of the reconfiguration time of the Spanning Tree of up to the media converter's Address Ageing Time (mostly 5 minutes).

- Moreover, media converters, which are looped into the Spanning Tree data path, have to have a link between fiber-optic and twisted-pair port. This means, that a link failure on the fiber-optic side must be passed through to the twisted-pair side and vice versa. Otherwise it will not be possible to detect a link failure at sufficient speed and the normal STP timers will run.

- The absolute maximum number of switches, which may connected in a ring, is 50. However, this requires the ‘Max. age/hops’ RSTP parameter to be increased from the factory default of 20 to 50. Experience has shown that not more than 30 switches should be connected in a single ring. The reasons are as follows:
  - Minimisation of switchover times in case of error.
  - Minimisation of packet delay times (each switch performs store-and-forward with the corresponding delay).
  - More stability of the Spanning Tree Protocol on bad fiber links with packet loss.

10.73.7. RSTP - Configuration notes regarding *Cisco* PVST

The following configuration hints are to be observed if a Nexans switch with RSTP according to IEEE802.1D is connected to a *Cisco* switch port via Per-VLAN-STP (PVST):

- VLAN 1 must be enabled on the corresponding *Cisco* switch port. In this case it doesn’t matter, whether it is configured as a native VLAN or as a tagged VLAN.

- VLAN 1 must be enabled on the Nexans port, as well. This can e. g. be configured as a default VLAN for the corresponding port. If the trunking mode of the respective port is set to 802.1Q-Tagging, it is sufficient, if VLAN 1 is entered in the VLAN table.

If the above hints are observed, all VLANs will be correctly blocked and no loop can occur in the network. If, in case of a link failure a standby port needs to be switched from Blocking to Forwarding, this happens with the Nexans switch simultaneously for all VLANs within some milliseconds. On the Cisco side, however, only VLAN 1 will be switched through at the corresponding speed. For all other VLANs of the corresponding trunk port the switchover from Blocking to Forwarding is performed via the PVST Timer and typically takes about 15 – 30 seconds. The reason is that on the Nexans switch only one Spanning Tree instance is running, so that the *Cisco* switch can affect a fast switchover for one Per-VLAN-STP instance only.

- The Spanning Tree Mode of the *Cisco* switch needs to be set to Rapid-PVST+. The Cisco CLI command is: spanning-tree mode rapid-pvst.

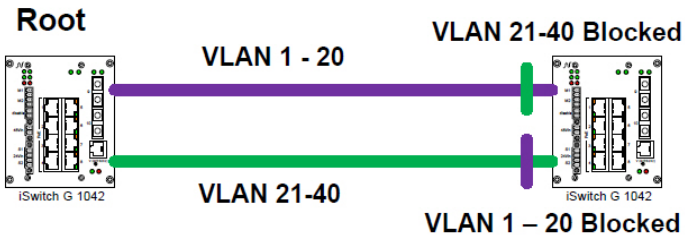
NOTE: Many *Cisco* switches also support the Multiple Spanning Tree protocol according to IEEE802.1s or IEEE802.1Q. Since this protocol is also supported by Nexans switches, a uniform vendor-independent Spanning Tree topology can be created.

10.74. Multiple Spanning Tree Protocol (MSTP)

10.74.1. MSTP - Global Function Principle

The Multiple Spanning Tree Protocol (MSTP) enables multiple VLANs to be mapped on the same spanning tree instance. Unlike the Per-VLAN-Spanning Tree this makes it possible to reduce the Spanning Tree instances, which would be required for a high number of VLANs. MSTP extends the RSTP standard. Using MSTP, load balancing can be implemented, since it is possible to divide up different VLANs independently from one another.

MSTP provides the big advantage of load balancing. For example, if you imagine a redundant link between 2 bridges, using RSTP/STP the complete data traffic would be transmitted via one link, because the redundant path was blocked. If MSTP is used with the same topology, load balancing can be implemented.



In the following example, VLAN 1 – 40 are available. In order to benefit from the MSTP advantages, two VLAN instances have been created. The first instance contains VLAN 1 – 20, the second VLAN 21 – 40. Using a purposeful configuration the VLAN instances are blocked at different locations and data traffic is thus distributed over both links. Only, if one link fails, data traffic will be transmitted via one link again.

MSTP is designed to define MST regions where bridges can communicate and manage several Spanning Tree instances. A region comprises a group of switches having the same MST Configuration Name, MST Configuration Revision Number and the same configuration of VLANs and Spanning Tree instances. MSTP instances do not have any direct contact with the outside world. Here, one would assume an incompatibility of MST with STP and RSTP. However, this is not the case and will be explained later. On each switch supporting MST the following attributes can be set thus creating different MST instances:

A Configuration Name, consisting of numbers and letters (32 bytes).

A Configuration Revision Number (2 bytes).

A table with 4096 elements, which contains the assignments of all potential 4096 VLANs to the individual instances.

In order to enable VLAN-To-Instance Mapping, the protocol must be able to determine the regional boundaries. In order to make this possible, the region information is transmitted within the BPDUs frames. However, the individual BPDUs do not contain any detailed information on the VLAN-To-Instance Mapping, since the switches only need to know whether they are in the same region as their neighbours.

The transmitted BPDU includes a summary of the VLAN-To-Instance Mapping, derived by a mathematic hash function, as well as the Configuration Name and the Revision Number. When a switch receives such a BPDU, it compares the VLAN summary, the name and the revision number with its own values. If one of these values should not match, the port, via which the BPDU was received, is at the boundary to another region.

An MSTP bridge must be able to manage at least two instances: the so-called Internal Spanning Tree (IST) instance 0 (which always exists on all ports) and at least one Multiple Spanning Tree Instance (MSTI).

In order to understand the role of IST, it must be clear, that MSTP is part of the IEEE standard. Consequently, MSTP will have to support the 802.1q standard. However, this standard has only one STP instance called Common Spanning Tree (CST). The IST instance is an RSTP instance which enables communication between CST and MSTP. The IST instance represents the complete MSTP region as a virtual bridge. In Figure 10-1 IST Instance 1 we see a topology with one CST and one IST instance. When you have a look at the blocked connections, you will see that the Default configuration of RSTP should block

the link between Switch A and Switch B. Moreover, you will expect that the second circuit will be blocked somewhere within the MST region and not in the link between Switches C and D.

However, since the IST instance is seen as a virtual bridge running in a single Spanning Tree instance (CST), you should imagine this topology as illustrated in Figure **10-2** IST Instance 2. Here you can easily see that the link to Switch B is considered to be an alternate port and thus will be blocked. Moreover, now it is understandable why the link between C and D is blocked.

Thus, the whole MSTP region appears as one single virtual CST bridge to the outside world. In the BPDU frames transmitted by Switch C the Path Cost as well as the Message Age will be increased as if only one single switch was passed. Additionally Switch C inserts its Bridge-ID in the Sender Bridge-ID field.

Figure 10-1 IST Instance 1

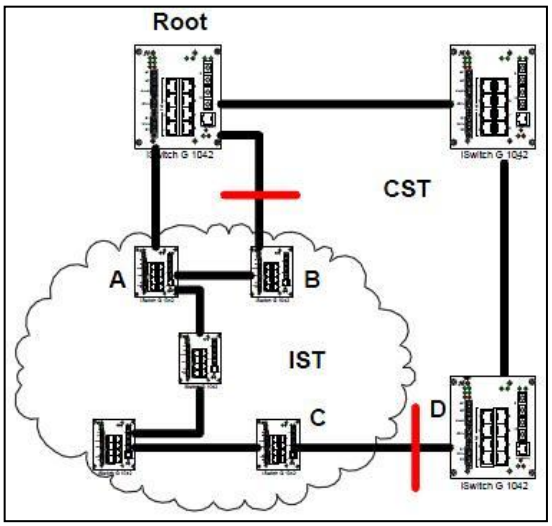
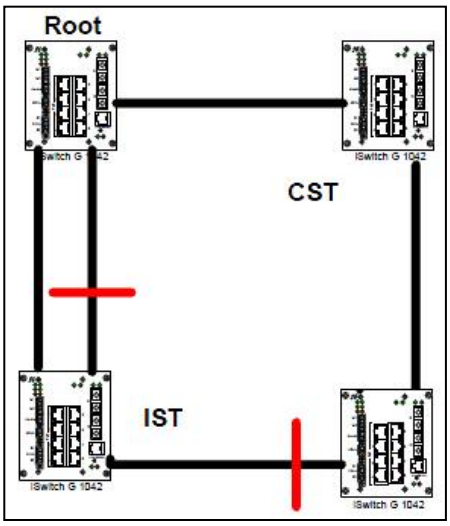


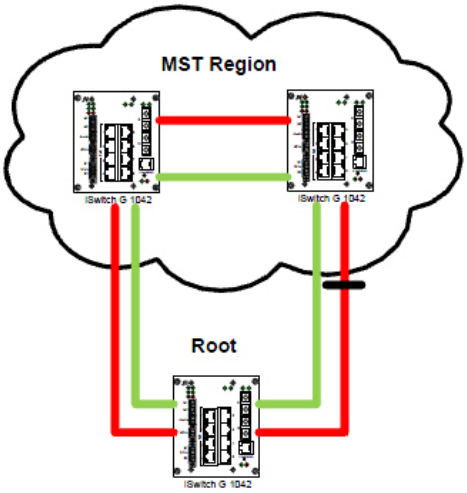
Figure 10-2 IST Instance 2



MSTIs are RSTP instances existing only within an MSTP region. Unlike the IST instance, MSTs do not have any contact with the neighbouring region or with STP/RSTP instances. They do not send any BPDU packets outside the region and will thus not be included in RSTP calculations outside of this region. Within the MSTP region the MSTIs send BPDUs, which can be considered as normal RSTP BPDUs. Each of these BPDUs contains additional information on all MSTIs. Each switch will send one BPDU only. Contrary to what one might expect, no BPDU is sent for each instance. The first field of information of these BDPUs contains information on the IST instance, followed by some MSTI information, the co-called MRecord. The MRecord contains information to calculate the RSTP topology of the MSTIs

The only contact of an MSTP region with the outside world is via the IST instance. Figure 3 Interact with the Outside World provides the following scenario: The red line is the IST instance. Since it is present everywhere, it will, of course, be blocked at one location. Now we assume, that within the MST region, VLANs 10 to 50 are mapped and additionally these VLANs are allowed everywhere in the network topology, e. g. by trunking. Since no BPDU packets are sent from the two switches, which are situated within the MSTP region, to the Root Bridge, one might expect that a loop occurs here, because there is no blocked path for these VLANs. In order to prevent this from happening, the MSTIs follow the IST instance at the boundary ports. Consequently not only the IST instance, but also the MST instance will be blocked. The result is that also VLAN 10 to 50 does not generate a loop, either.

3 Interact with the Outside World



For detailed information on the configuration of MSTP please contact Nexans Support.

10.74.2. MSTP - Indentifier Setup

Designation in NEXMAN	Default Value	Function
MSTP Name (1…32 chars)	NEXANS-<MAC-Address>	The name of the MSTP region. By factory default this is set to "NEXANS-" with the MAC adress attached, i.e.. "NEXANS-00C029241234"
MSTP Revison (0…65535)	0	The revision of the MSTP region.

10.74.3. MSTP - Instance Setup

Designation in NEXMAN	Default Value	Function
Instance ID	-	The ID of the MSTP instance.
Bridge Priority	32768	The bridge priority of the MSTP instance.
Mapped VLANs	-	The VLANs assigned to the MSTP instance.
Instance ID Offset	0	This value defines the acceptable instance ID range. According to the standard the instance IDs may be in the range of 1 – 4094. The switch supports a subrange of 250 IDs. For example: If the offset is set to 1000, IDs from 1000 to 1250 can be configured. For an offset of 0 (default) IDs from 1 to 125 can be configured.

10.74.4. MSTP - Globale Statusparameter

Designation in NEXMAN	Default Value	Function

MSTP Digest	In order for two neighbouring switches to belong to the same region, both switches must have the same MSTP name, the same MSTP revision and the same MSTP digest. The so-called MSTP digest is calculated from the configuration of the individual MSTP instances. Only if all MSTP instances are identically configured on both switches, the two MSTP digest values are identical, too.

10.74.5. MSTP - Instance Status Parameter

Description	Function
State	Shows the current Spanning Tree state of the respective port. The following statuses are possible: • Forwarding The port is included in the active topology and forwards data. • Blocking The port is not included in the data transmission of the active topology. Only BPDU packets are sent and received. • Learning The port is not included in the data transmission of the active topology, but MAC addresses are learned. Only BPDU packets are sent and received. • No Link The port does not receive a link signal and thus is not included in the data transmission of the active topology.
Role	Shows the role of the port in the Spanning Tree topology: • Root Port The Root Port is the port next to the Root Bridge based on the path cost. The Root Bridge is the only switch without Root Port. • Designated Port A Designated Port points downstream, i.e. from the Root-Bridge, and has the most favourable path cost to the segment in which it is situated. • Alternate Port An Alternate Port represents a (alternative) path to the Root and is not included in the active topology. If the Root Port fails, it is possible to rapidly switch over to the Alternate Port. • Backup Port A Backup Port is a path to a segment, to which this switch already has connected a Designated Port (with better path cost). That means, this port is not included in the active topology. If the Designated Port fails, it is possible to rapidly switch over to the Backup Port. • Master The Master port identifies a port presenting the transition from one region to another region.
Cost	Shows the path cost used for this port.
Prio.	Shows the priority used for this port.
Designated Cost	Shows the path cost to the Root Bridge.
P2P	Shows, if the port operates as point-to-point link

Category	Indicates the connection category: • Edge The port operates as an edge port, i. e. no BPDU packets of the connected device will be received. • Internal The connected device also supports MSTP and belongs to the same region. In order for two neighbouring switches to belong to the same region, both switches must have the same MSTP name, the same MSTP revision and the same MSTP digest. • Boundary (RSTP) The connected device either also supports MSTP, but does not belong to the same region, or it supports RSTP and thus principally does not belong to the same region. • Boundary (STP) The connected device supports STP and thus principally does NOT belong to the same region.

10.75. Link Aggregation

10.75.1. Link Aggregation - General Function

Link Aggregation (IEEE 802.1AX) is a network protocol used to increase the available bandwidth by combining several physical interfaces to form one logical unit. At the same time Link Aggregation can be used to provide redundancy.

Both static and dynamic Link Aggregation, also called LACP (Link Aggregation Control Protocol), is available. Unlike static Link Aggregation, with dynamic Link Aggregation so-called LACPDUs (Link Aggregation Control Protocol Data Units) are sent between the two endpoints. LACPDUs are used for confirming the configuration and for detecting the failure of a physical link.

In order to guarantee the proper functioning of Link Aggregation, the following preconditions must be fulfilled:

- All ports of an LAG must have the same Link State FDX.
- All ports of an LAG must have the same data rate.
- No other redundancy protocol must be enabled on the corresponding ports.
- Link Aggregation works only between two endpoints, unless two different endpoints run as a virtual unit.

10.75.2. Link Aggregation - Global Setup

Designation in NEXMAN	Default Value t	Function
Link Aggregation global enable	Disabled	Only if Link Aggregation is enabled globally, the configured LAGs will become active.
Link Aggregation Protocol Timeout	Slow	Configuration of the LACP timeout for received and the time interval for sent LACP packets. The following timeout modes can be configured: • Slow (Timeout 30 sec.) This is the default setting and compatible with most LACP partners. This setting should be used in particular when connecting to a multi-chassis link aggregation (MLAG) core switch. • Fast (Timeout 1 sec.) Certain end devices, especially servers, require this setting.

10.75.3. Link Aggregation – Group Setup

Designation in NEXMAN	Default Value	Function
Mode	Deleted	The following LAG Modes can be configured: • Deleted The LAG does not exist. • Static For this LAG-ID the static Link Aggregation is enabled. As soon as a port, which is assigned to this LAG, has an active link, it will be used actively for Link Aggregation. • LACP Unlike the Static mode, the configuration is checked, when LACP is used. An active link will only be used actively in an LAG, if it was confirmed by both switches. • Disabled The configured LAG is disabled.
Name (1…15 chars)	Empty	The name of the LAG.
Edit Member Ports	-	The ports assigned to this LAG-ID.
Delete LAG	-	Deletes the LAG and its configuration.

10.76. Media Redundancy Protocol (MRP)

The Medium Redundancy Protocol (MRP) is a deterministic IEC 62439 standard protocol for ring topologies. MRP uses a Redundancy Manager (RM), which monitors the ring and closes the ring in case of a failure of a redundancy Client. Each switch supports up to five rings as a Redundancy Manager and one single instance as a Redundancy Client. Test packets sent by the RM enable to determine whether the ring is closed. If the sent test packets get lost, the ring must be interrupted.

In an MRP ring the user must define a Redundancy Manager. In case of an active ring topology, one of its ports is in Blocking State. If one RM port is in Blocking State, it sends and receives test packets as well as Link-Change (LC) packets, but does not forward any data traffic.

The LC packets are sent by Redundancy Clients (RC) and explained later. The RM sends the test packets mentioned in both ring directions. If three of these packets get lost, i. e. the sent packets are not received by the RM, the RM assumes that the ring is interrupted at one location.

If an interruption of the ring is detected, the RM will send Topology Change (TC) packets to the Redundancy Clients (RC).

If an RC receives a Topology Change packet sent by the RM, it will delete its forwarding database after expiration of the interval indicated in the packet.

The Redundancy Clients are also configured by the user. They also play an important role in the topology of the network. If an RC detects that one of its ports, which is situated in the ring topology, changes its status, i. e. from Link-Up to Link-Down or vice versa, it will send LC packets. If the RM receives such an LC packet, it will send its TC packets in order to initialize the deletion of the forwarding database.

If there is an interruption of the ring with the MRP, we can distinguish between three different cases:

The interruption of the ring occurred between the master's Forwarding Port and the first client. Now the blocked port of the master will be set to Forwarding. If the interruption is cancelled and the ring is thus restored, this port stays in Forwarding State. The sort of "new" port changes into Blocking State. Contrary to the initial situation, Blocking and Forwarding ports are swapped. The advantage is that there is no reconfiguration time available (unlike with e. g. RSTP). Thus any renewed packet loss is avoided.

The interruption of the ring does not occur immediately at the two ring ports of the master. Since the complete ring can be reached now, the port which was previously blocked, changes into Forwarding State. If the ring is closed again, this port will change into Blocking State.

The interruption occurs at the Blocking Port, in which case the port statuses will not change.By means of different reconfiguration behaviours a renewed packet loss is avoided in two cases.

NOTE:
Up to and including firmware version V5.03go, a memory card card with an MRP license must be present in the switch. From firmware version V5.03gp MRP can also be activated without a corresponding memory card since the MRP patent expired in May 2019.

10.76.1. MRP – Global Setup

Designation in NEXMAN	Default Value	Function
MRP global enable	Disabled	Only, if the MRP is globally enabled here, all ports with enabled MRP will be included in the monitoring of the ring topology. IMPORTANT: If the MRP is globally disabled here, the switch will behave transparent to MRP-BPDU packets, and received MRP-BPDU packets will be forwarded to all ports.
Max. recovery time	500ms	Here two settings are possible: 200ms or 500ms. These are the guaranteed MRP recovery times.

10.76.2. MRP – Instance Setup

Designation in NEXMAN	Default Value	Function
Instance ID	-	The ID of the MRP instance.
Admin Role	Disabled	Three settings are possible: • Disabled The MRP instance is disabled. • Manager The MRP instance is a Redundancy Manager. • Manager (with Ring Port 1 Priority) The MRP instance is a Manager (with Ring Port 1 Priority). Unlike in the Standard Manager Mode, for a closed ring topology Ring Port 1 is generally switched to “forwarding” and Ring Port 2 to “blocking”. • Client The MRP instance is a Redundancy Client. NOTE: On the switch only one Client instance is permitted.
Domain-ID	FF - FB	Domain-ID is a Universally Unique Identifier (UUID), which unambiguously identifies an MRP ring in the network. Each instance has to be configured with the unique identifier. The identifier is automatically generated with the first settable byte. Example: Domain-ID 55 corresponds to the UUDI 55FFFFFF-FFFF-FFFF-FFFF- FFFFFFFFFFFF
VLAN-ID	0	The VLAN-ID assigned to the MRP instance. With VLAN-ID 0 no VLAN is assigned and the MRP packets are sent without a VLAN tag. IMPORTANT: With the configured VLAN-ID this VLAN must not correspond to the Default-VLAN of the ports used.
Ring-Port 1 **Ring-Port 2**	0	The ports assigned to the MRP instance. If the Ring-Port is set to 0, no port is assigned to the instance. Each port may only be configured on one instance. IMPORTANT: Both ports of the instance have to be configured with the same Default VLAN-ID and enabled Trunking 802.1q.

10.76.3. MRP – Status Parameters

Description	Function
ID0-ID4	Shows, if the instance has been configured and whether the ring is open or closed. If <Ring Open> is displayed, a switch or a line in the ring is down.
UUID	The ‚Universally Unique Identifier‘.
Transitions/Last change	Shows, how long the ring topology has not changed.
Remote Manager	Only for Redundancy Client instances, this parameter indicates the MAC address of the Redundancy Manager.
Link/Admin State	The link status of the MRP ports.
Role	The Port Role shows, if the port has been set by the MRP as Primary or Secondary.
VLAN	Configured VLAN-ID for the MRP protocol.

Default-VLAN	Default VLAN ID of the port.
Egress VLAN	The VLAN-ID used for sending MRP packets.

For detailed information on the configuration of the MRP please contact Nexans Support.

10.76.4. MRP – MRP to Spanning Tree network coupling

In order to couple an MRP ring redundantly with a Spanning Tree topology, the “MRP to Spanning Tree Network Coupling” command is used to guarantee that under no circumstances a switching loop will occur in the network.

The following explanations refer to the Variant A or Variant B topology:

If both rings (Spanning Tree / MRP) are closed, the link of the MRP rings between switches C and D is set to Blocking. Spanning Tree is configured in such a way that the link between switches A and C is set to Blocking.

If now a link fails in the MRP ring, e. g. between switches F and G, this link will be set to Forwarding between switches C and D. At this point there will be no change in the Spanning Tree topology. If the MRP ring is closed again, the link which was set to Forwarding will return to the Blocking state and the topology is back to its original state.

If the link between switches C and D fails in addition to the link between switches F and G, the Spanning Tree topology is changed. In this case the link between the switches A and C will change into the Forwarding state after losing three Hello packets.

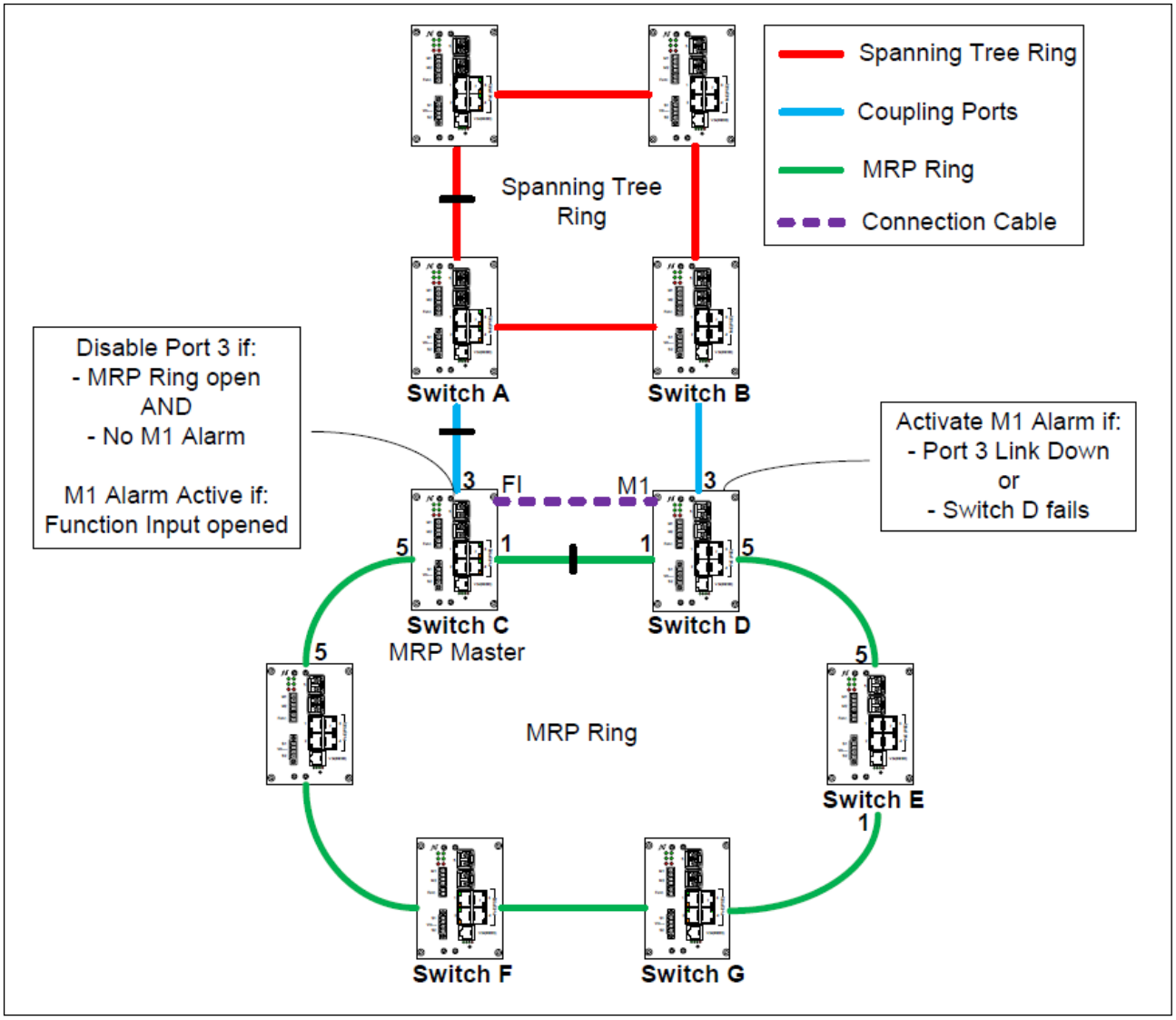
If the link between switches C and D or F and G is restored, the Spanning Tree can detect this only by receiving a “Hello Time” BPDU. Depending on the Spanning Tree configuration this might take several seconds and result in a switching loop.

In order to counteract this behaviour, port 3 of switch C is set to “Admin Disabled” as soon as the MRP ring is open again. Now this port will be re-enabled only, if M1 has an active alarm or the MRP ring is closed again.

There are two scenarios available to trigger an M1 alarm:

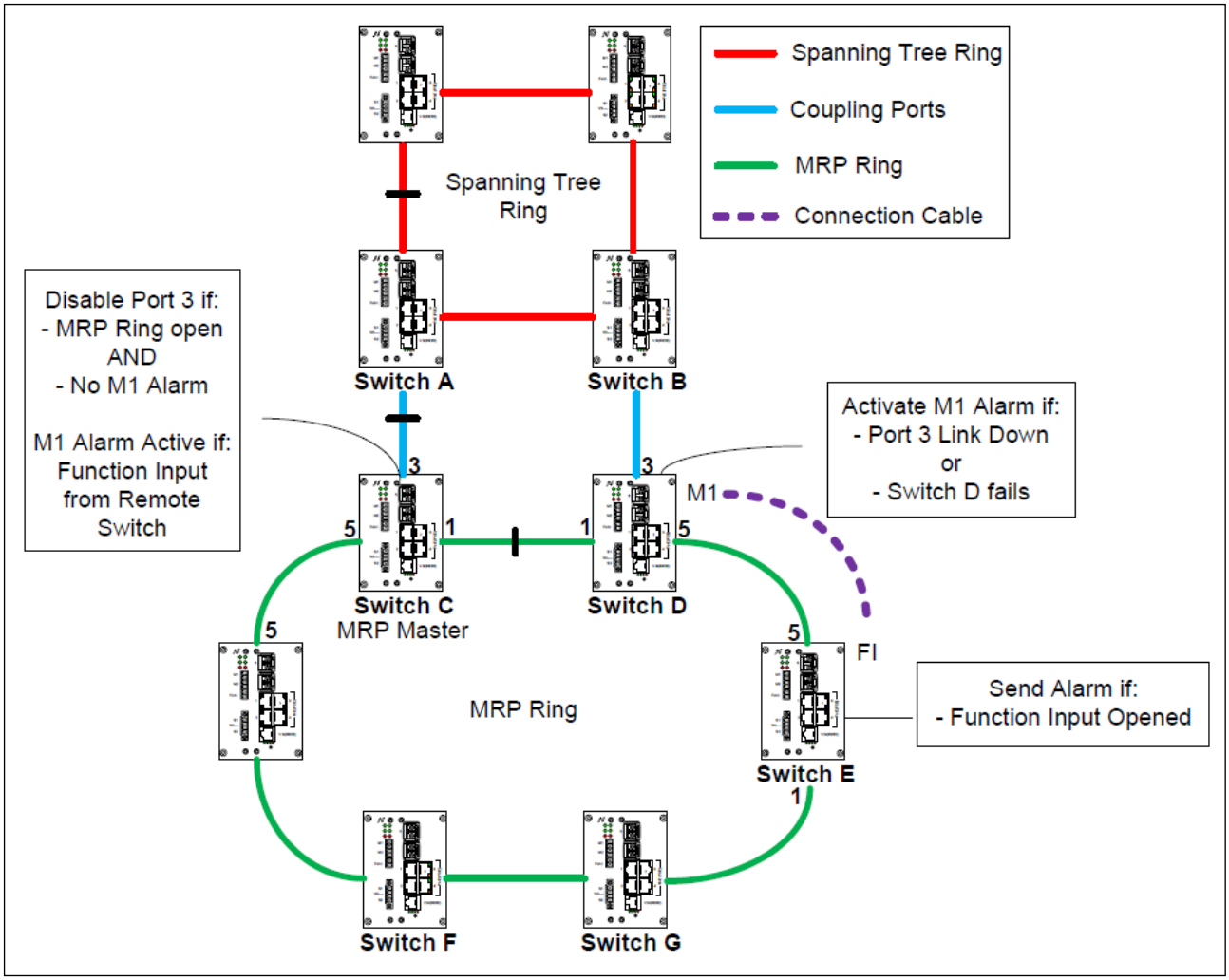
Variant A)

The functional input of switch C is connected with the M1 alarm output of switch D. M1 of switch D is triggered when port 3 has a Link Down. Thus the Spanning Tree topology would be isolated with an open ring or if switch D is disabled. Switch C is configured in such a way that the M1 alarm is enabled as soon as the functional input is open.



Variant B)

The M1 alarm of switch D is connected with the functional input of switch E. M1 of switch D is triggered when port 3 has a Link Down. Thus the Spanning Tree topology would be isolated with an open ring or if switch D is disabled. Switch E sends an alarm to a configured Alarm Group, when the functional input is open. Switch C is configured in such a way that the M1 alarm is enabled, if an active alarm is present in the configured Alarm Group.



Variant "**A**" is the preferred variant. However, the on-site conditions may not allow you to connect the functional input of switch C with the M1 alarm output of switch D. This problem might also occur with Variant B. However, this can be counteracted by adding a switch which is only used for transmitting alarms.

10.77. Zeroloss Redundancy

The Nexans Zeroloss Redundancy Protocol guarantees that no packet loss occurs in ring topologies for a defined Ethertype. Normally an interruption and the following reconfiguration of the topology results in lost packets. Zeroloss guarantees that for the defined Ethertype at least 1000 packets per second will be transmitted without any loss. One application example is the transmission of GOOSE packets using Ethertype 88B8 in IEC 61850 networks.

10.77.1. Zeroloss – Global Setup

Designation	Default Value	Function
Zeroloss global enable	Disabled	Only if Zeroloss is enabled here, the switch will participate in the Zeroloss procedure. IMPORTANT: If Zeroloss is disabled here, the switch will not participate in the Zeroloss procedure and packets might get lost, if the ring is interrupted.

10.77.2. Zeroloss – Port Setup

Designation	Default Value	Function
Zeroloss Role	Disabled	Here are three options configurable: • Disabled Zeroloss is disabled for this port • Ringport The ringports built the Zeroloss Ring. • User Port To this port data is sent tot he Zeroloss Ring.
Ethertype (8800…FFFF))	88B8	Here the Ethertype is determined, which shall be sent via the user port into the Zeroloss ring.

10.78. DHCP Relay / Snooping

10.78.1. DHCP Snooping

If DHCP Snooping is set to “Enable”, it will be enabled on all ports whose link type is set to “Userport” or “Userport with Active Loop Protection”. As soon as a packet from a DHCP server is received on these ports, the switch will set the respective port’s Admin State to “Disabled by DHCP Snooping”. Thus, it is possible to prevent a DHCP server from being connected to the switch’s user ports.

Optionally, disabled ports can automatically be re-enabled after a settable “Re-enable time for DHCP Snoopig Disabled ports”. The time value can be set in the range from 1 to 60000 seconds.

10.78.2. DHCP Snooping – Global Setup

Designation in NEXMAN	Default Value	Function
DHCP Snooping enable	Disabled	Using this function DHCP Snooping is globally enabled. If the option is set to Disable, any DHCP packets are allowed on the user ports.
Re-enable time for DHCP Snoopig Disabled ports	0	Ports, which were disabled due to DHCP Snooping can optionally be re-enabled automatically after a time period of 1 to 60000 seconds. If the time is set to “0”, the port has to be re-enabled manually.

10.78.3. DHCP Relay Agent

The DHCP Relay Agent (Option 82) allows you to distribute the DHCP requests from the connected terminal units to the individual DHCP servers. This is possible, because the switch inserts a DHCP option, consisting of the Remote-ID and the Circuit-ID, into the DHCP requests of terminal units. The DHCP Relay Agent is configured per port and supports up to three DHCP servers per port.

10.78.4. DHCP Relay Agent – Global Setup

Designation in NEXMAN	Default Value	Function
DHCP Relay Agent global enable	Disabled	Here the DHCP Relay Agent is globally enabled. If the Option is set to Disable, the DHCP requests from the terminal units will be forwarded unchanged.
Filter original Client DHCP requests	Disabled	By enabling this option the original DHCP requests from the terminal units will be filtered from the network. If this option is disabled and the request is in the Management VLAN of the switch, the switch will generate a DHCP request with Option 82 additionally to the original request from the terminal unit.
Remote ID	Port No	The Remote ID is part of Option 82 and identifies the terminal unit. The following parameters can be generated as part of the Remote ID: • Port No The number of the port. • Port MAC The MAC address of the port. • VLAN-ID If trunking is disabled on the port, the Default VLAN ID of the port will be inserted as part of the Remote ID. If trunking is enabled on the port, the VLAN ID from the received DHCP request will be inserted as part of the Remote ID. • User defined A user-defined text. IMPORTANT: The value of the Remote ID can be taken from the DHCP Relay Agent Status. The first byte of the Remote ID is reserved for this purpose and is used by the switch as Format Byte.
Circuit ID	Port No	The Circuit ID is the second part of Option 82 and identifies a network. Here the same parameters as for the Remote ID can be configured.

10.78.5. DHCP Relay Agent – Port Setup

Designation in NEXMAN	Default Value	Function
Role	DHCP Transparent	Three settings are possible: • DHCP Transparent All DHCP requests are forwarded unchanged by the switch. • DHCP Option 82 Client The requests from the terminal units over this port will be processed by the switch and forwarded using the Option 82. • DHCP Server A DHCP server is connected to this port.
Server IP 1 **Server IP 2** **Server IP 3**	0.0.0.0	Up to three DHCP servers can be configured. IMPORTANT: The servers must be reachable via the management VLAN.

10.78.6. DHCP Relay Agent – Global Status

Shows the current DHCP Relay Agent Status. If the parameters are correctly set, the status must be on "running". Additionally it is shown, if the original DHCP requests from terminal units will be filtered.

10.78.7. DHCP Relay Agent – Port Status

Description	Function
Role	Shows the configured role.

Remote ID	Here the Remote ID is shown, which is inserted by the switch for DHCP requests. The flags only show, the parts the Remote ID consists of, and are no part of the Remote ID.
	The following flags are shown:
	`F : ID Format byte [1 byte]`
	`P: Port Number [1 byte]`
	`M: Port MAC for RemoteID or Host MAC for CircuitID [6 bytes]`
	`U: User addon [0...15 bytes]`
	`V: Default VLAN-ID if trunking disabled [2 bytes]`
	`Dynamic VLAN ID if trunking enabled`

Circuit ID	Here the Circuit ID is shown, which is inserted by the switch for DHCP requests.

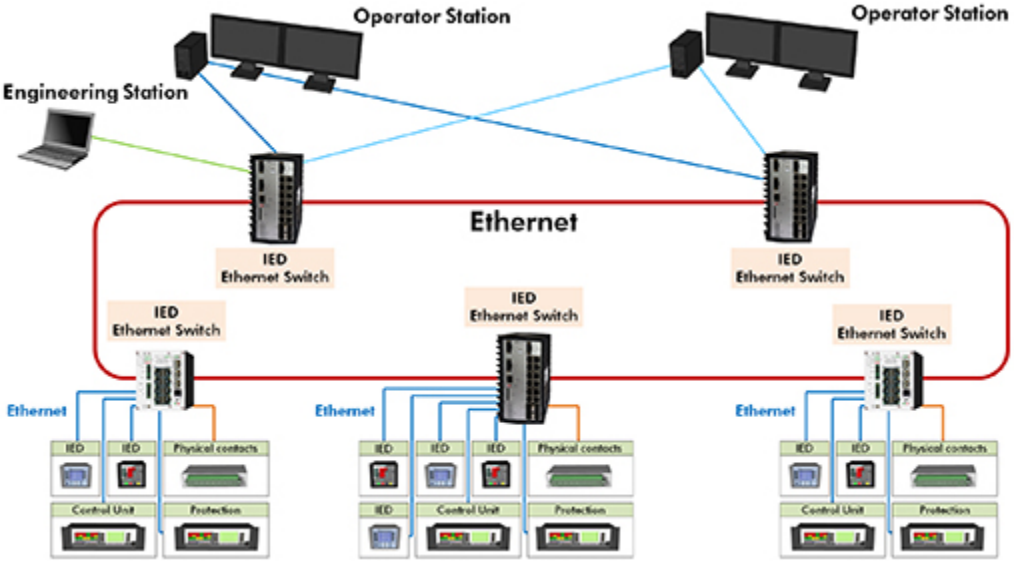
For detailed information on the configuration of the DHCP Relay Agent please contact Nexans Support.

10.79. IEC61850 protocol support

10.79.1. IEC61850 overview

IEC 61850 uses TCP/IP as the protocol which provides all benefits of modern Ethernet communication infrastructure. Implementation of IEC 61850 provides the possibility for many devices within power substations (equipped with surveillance, control, measurement and monitoring units, etc.) to communicate together and transmit special information without additional convertors or specialized sub-networks. Nexans IEC 61850 Ethernet switches become part of a universal standardized network for the exchange of EID's data, services and network information according to IEC 61850-8-1 / -9-1 / 9-2. Nexans IEC61850 Stack

passed all KEMA certification tests which are based on IEC 61850, that confirms interoperability and compatibility with all network devices and power station components from various vendors.



10.79.2. IEC61850 access mode

The IEC61850 access mode allows you to enable the IEC61850 protocol stack. The following settings are available:

- IEC61850 disabled
- Read/Write
- Read/Only

Disabled:
This is the factory default setting. In this mode the IEC61850 protocol stack is diabled.

Read/Write:
In this mode the IEC61850 protocol stack access is enabled with read/write access rights.

Read/Only:
In this mode the IEC61850 protocol stack access is enabled with read/only access rights.

10.79.3. IEC61850 objects

The IEC61850 protocoll stack supports the following objects:

Variable	**Data type**	**Description**	**Access rights** read: R write: W constant: C
LLN0.NamPlt.vendor	MMS_VISIBLE_STRING	Vendor name: NEXANS	C
LLN0.NamPlt.swRev	MMS_VISIBLE_STRING	IEC 61850 software version	C
LPHD1.Tmp.mag.f	MMS_STRUCTURE	Switch temperature	R
LPHD1.Tmp.range	MMS_INTEGER	1=normal, 2=high, 3=low, 4=high-high, 5=low-low	R
LPHD1.Tmp.rangeC.hhLim	MMS_STRUCTURE	Threshold value for temperature measurements	R
LPHD1.Tmp.rangeC.hLim	MMS_STRUCTURE	Threshold value for temperature measurements	R

LPHD1.Tmp.rangeC.llLim	MMS_STRUCTURE	Threshold value for temperature measurements	R
LPHD1.Tmp.rangeC.lLim	MMS_STRUCTURE	Threshold value for temperature measurements	R
LPHD1.Tmp.rangeC.min	MMS_STRUCTURE	Threshold value for temperature measurements	R
LPHD1.Tmp.rangeC.max	MMS_STRUCTURE	Threshold value for temperature measurements	R
LPHD1.PhyHealth.stVal	MMS_INTEGER	Physical device health state (1 = OK, 2 = Warning, 3 = Alarm)	R
LPHD1.TmpAlm.stVal	MMS_BOOLEAN	Temperature alarm (1 = triggered)	R
LPHD1.PwrSupAlm.stVal	MMS_BOOLEAN	Power supply alarm, internal or external (1 = triggered)	R
LPHD1.PhyNam.vendor	MMS_VISIBLE_STRING	Vendor name	C
LPHD1.PhyNam.hwRev	MMS_VISIBLE_STRING	Hardware revision	C
LPHD1.PhyNam.swRev	MMS_VISIBLE_STRING	Firmware revision	R
LPHD1.PhyNam.serNum	MMS_VISIBLE_STRING	Device serial number	C
LPHD1.PhyNam.model	MMS_VISIBLE_STRING	Device model name	C
LPHD1.LdpEna.setVal	MMS_BOOLEAN	LLDP enable	R
LPHD1.LocChsIdTyp.stVal	MMS_INTEGER	Type of local chassis identifier 'LocChsId' according to IEEE 802.1AB	R
LPHD1.LocChsId.stVal	MMS_VISIBLE_STRING	Type of local chassis identifier according to IEEE 802.1AB	R
LPHD1.LocAddrTyp.stVal	MMS_INTEGER	Type of system local management address 'LocAddr' according to IEEE 802.1AB	R
LPHD1.LocAddr,.stVal	MMS_VISIBLE_STRING	local system management address according to IEEE 802.1AB	R
GGIO1 – General purpose I/O			
GGIO1.Beh.stVal	MMS_INTEGER(8)	LN state - always on	C
GGIO1.SPCSO1.stVal	MMS_BOOLEAN	Digital output 1 - operate state. This object reflects the value set by the below GGIO1.SPCSO1.Oper command. This object is only valid if the „Alarm Output M1 Mode“ is s et to „Controlled by IEC 61850 protocol“	R
GGIO1.SPCSO1.Oper		Digital output 1 - operate command This object is only valid if the „Alarm Output M1 Mode“ is set to „Controlled by IEC 61850 protocol“	W/R
GGIO1.SPCCO1.stVal	MMS_BOOLEAN	Digital output 1 - current state	R

GGIO1.SPCSO2.stVal	MMS_BOOLEAN	Digital output 2 - operate state This object reflects the value set by the below GGIO1.SPCSO2.Oper command. This object is only valid if the „Alarm Output M2 Mode" is set to „Controlled by IEC 61850 protocol"	R
GGIO1.SPCSO2.Oper		Digital output 2 - operate command This object is only valid if the „Alarm Output M2 Mode" is set to „Controlled by IEC 61850 protocol"	W/R
GGIO1.SPCCO2.stVal	MMS_BOOLEAN	Digital output 2 - current state	R
GGIO1.Ind1.stVal	MMS_BOOLEAN	Digital input 1 – state	R
GGIO1.Ind2.stVal	MMS_BOOLEAN	Digital input 2 – state	R
GGIO1.Ind3.stVal	MMS_BOOLEAN	Digital input 3 – state	R
GGIO1.Ind4.stVal	MMS_BOOLEAN	Digital input 4 – state	R
LBRI[1..Max Port] – Bridge			
LBRI1.Beh.stVal	MMS_INTEGER	LN state - always on	C
LBRI1.NamPlt.vendor	MMS_VISIBLE_STRING	Vendor name: NEXANS	C
LBRI1.NamPlt.swRev	MMS_VISIBLE_STRING	Firmware revision	C
LBRI1.NamPlt.configRev	MMS_VISIBLE_STRING	Configuration revision	C
LBRI1.NamPlt.lnNs	MMS_VISIBLE_STRING	(Tr)IEC 61850-90-4:2012	C
LBRI1.RstpEna.setVal	MMS_BOOLEAN	Rapid spanning tree protocol - enable/disable	W
LBRI1.RstpPrio.setVal	MMS_INTEGER(32)	Rapid spanning tree protocol – bridge priority	W
LBRI1.RstpRoot.stVal	MMS_BOOLEAN	Rapid spanning tree protocol – root	R
LBRI1.Mrp.stVal	MMS_INTEGER(8)	MRP ring state (1 – open / 2 – closed / 3 - not-supported)	R
LBRI1.PortRefx.setSrcRef	MMS_VISIBLE_STRING	Object reference of port LN (LPCPx)	C
LBSP[1..Max Port] – Bridge spanning tree port			
LBSP1.Beh.stVal	MMS_INTEGER	LN state - always on	C
LBSP1.NamPlt.vendor	MMS_VISIBLE_STRING	Vendor name: NEXANS	C
LBSP1.NamPlt.swRev	MMS_VISIBLE_STRING	Firmware revision	C
LBSP1.NamPlt.configRev	MMS_VISIBLE_STRING	Configuration revision	C
LBSP1.NamPlt.lnNs	MMS_VISIBLE_STRING	(Tr)IEC 61850-90-4:2012	C
LBSP1.RstpTrunk.setVal	MMS_BOOLEAN	If true, the port is set to participate in RSTP (is trunk), otherwise it is edge	W/R

LCCH[1..Max Port] – Logical channel			
LCCH1.ChLiv.stVal	MMS_BOOLEAN	Physical channel status (1 = up / 0 = down)	R
LCCH1.PortRef.setSrcRef	MMS_VISIBLE_STRING	Object reference of port LN (LPCPx)	C
LCCH1.RedCfg.setVal	MMS_INTEGER(8)	Redundancy configuration: 1 - none, 2 – prp. 3 – hsr, nrp=4, rstp=5	W
LCCH1.DftPortVid.setVal	MMS_INTEGER	VLAN – Default port VID	W
LCCH1.DftPortPrio.setVal	MMS_INTEGER	VLAN – Default port priority	W
LPCP[1..Max Port] – Physical communication port			
LPCP1.NamPlt.vendor	MMS_VISIBLE_STRING	Vendor name: NEXANS	C
LPCP1.NamPlt.swRev	MMS_VISIBLE_STRING	Firmware revision	C
LPCP1.NamPlt.configRev	MMS_VISIBLE_STRING	Configuration revision	C
LPCP1.AutoNgt.stVal	MMS_BOOLEAN	SPS: autonegotiation mode active	R
LPCP1.Mau.stVal	MMS_INTEGER	INS: medium access unit	R
LCPC1.PortNum.setVal	MMS_INTEGER	ING: port number	C
LPCP1.AutoNgtCfg.setVal	MMS_BOOLEAN	SPG: enable/disable auto negotiation	W
LPCP1.MauCfg.setVal	MMS_INTEGER	ING: manual MAU mode setting	W
LPCP1.MauCfgCap1.setVal	MMS_INTEGER	ING: MAU mode capability 1	C
LPCP1.MauCfgCap2.setVal	MMS_INTEGER	ING: MAU mode capability 2	C
LPCP1.AdminCfg.setVal	MMS_BOOLEAN	SPG: enable/disable port	W
LPLDx – Port link discovery			
LPLD1.Beh.stVal	MMS_INTEGER	1=ON, 2=ON-blocked, 3=test, 4=test/blocked, 5=off	C
LPLD1.NamPlt.vendor	MMS_VISIBLE_STRING	Vendor name: NEXANS	C
LPLD1.NamPlt.swRev	MMS_VISIBLE_STRING	Firmware revision	C
LPLD1.NamPlt.configRev	MMS_VISIBLE_STRING	Configuration revision	C
LPLD1.NamPlt.lnNs	MMS_VISIBLE_STRING	(Tr)IEC 61850-90-4:2012	C
LPLD1.RemPortDesc.stVal	MMS_VISIBLE_STRING	Remote port description	R
LPLD1.LocPortDesc.stVal	MMS_VISIBLE_STRING	Local port description	R
LPLD1.RemPortId.stVal	MMS_VISIBLE_STRING	Remote port ID	R
LPLD1.LocPortId.stVal	MMS_VISIBLE_STRING	Local port ID	R
LPLD1.RemPortIdTyp.stVal	MMS_INTEGER	Remote port ID Type	R
LPLD1.LocPortIdTyp.stVal	MMS_INTEGER	Local port ID Type	R
LPLD1.RemChsIdTyp.stVal	MMS_INTEGER	Remote chassis ID Type	R
LPLD1.RemChsId.stVal	MMS_VISIBLE_STRING	Remote chassis ID	R
LPLD1.RemSysDesc.stVal	MMS_VISIBLE_STRING	Remote system description	R
LPLD1.RemAddrTyp.stVal	MMS_INTEGER	Remote Address Type	R
LPLD1.RemAddr.stVal	MMS_VISIBLE_STRING	Remote Address	R

LPLD1.PortRef.setSrcRef	MMS_VISIBLE_STRING	Object reference of port LN (LPCPx)	C

11. Power-over-Ethernet (PoE) Functional Description

11.1. PoE General Functional Description

11.1.1. PoE Measured Values

The following PoE measured values are continually detected on the PoE adapter and can be displayed, if necessary:

For each port:
- Output voltage (in V)
- Output current (in mA)
- Output power (in W)
- Powerclass / max. Power (W) (not support by all types of PoE adapters)

For PoE power supply:
- Input voltage (in V)
- Input current (in mA)
- Input power (in W)

NOTE:
The individual port output currents are measured via measuring resistors in the negative branch of the PoE output signals. Thus, to ensure correct current readings there must be no short-circuit between negative PoE voltage and ground in the connected PoE terminal. This will usually never happen, because PoE devices typically work stand-alone. Only in special cases, e.g. if a serial cable is temporarily connected to an access point for configuration purposes, short-circuit to ground may occur. Although such short-circuit does NOT destroy the Nexans PoE adapter, zero values will be indicated for the current and power readings.

11.1.2. PoE Power Setup

Here five settings are possible:

- Off
- On (Forced)
- Auto 802.3af
- Auto 802.3af High-Power (Ignores Power Class)
- Auto 802.3at High-Power

Off:
With this setting PoE voltage is **switched off** permanently.

Overload-Off:
With this setting the switch has detected that the selected power limit was exceeded and thus automatically switched off PoE voltage.

On:
With this setting PoE voltage is **switched on** permanently.

This setting is needed e.g. in order to supply terminal equipment with power which does not conform to the IEEE802.3af standard.

CAUTION:
If non-PoE terminal equipment is connected to a port with permanently enabled PoE voltage supply, this may destroy the Ethernet interface of the respective terminal equipment.

Auto 802.3af:
This setting is only supported by **Type AF** PoE adapters.
The setting enables PoE voltage according to the **IEEE802.3af** standard. This means, that the TP adapter will only switch through 48V voltage supply, if conforming terminal equipment is plugged onto the respective port. Upon removal of the terminal equipment the integrated Zero-Current Detection switches off the port's voltage supply again.

IMPORTANT NOTE:

The pins of the terminal equipment must be assigned according to IEEE802.3af and the terminal equipment must support the Discovery Feature defined in the standard. Some vendors claim that their terminal equipment provides Inline Power according to IEEE802.3af, although this equipment only supports the pin assignment of the standard. If you nevertheless want to connect such terminal equipment, you must select the {On} setting.

Auto 802.3af High-Power (Ignores Power Class):
This mode has been specially designed for such terminal units, which still operate on the old IEEE802.3af standard, but nevertheless require a higher power than 15.4W. In this case the power class reported by the terminal unit is ignored and principally 30W is made available.
This setting is needed e. g. by certain *Cisco* access points, which do not negotiate the required power via the IEEE802.3at standard but via CDP and the *Cisco* 'Intelligent Power Management'. If such an access point is to be operated on a Nexans PSE+ port, CDP must additionally be enabled in the Nexans switch. Then the switch will send the required information via CDP to the access point.

Auto 802.3at High-Power:
This setting is supported by PoE ports with PSE+ functionality according to IEEE802.3at only. The connected terminal unit (Powered Device, PD) can be provided with a power of up to 30W. In order for the terminal unit to be allowed to draw the full power, this must also support IEEE802.3at and additionally report Power Class 4 to the switch. However, if the terminal unit reports a lower power class, a maximum of 15.4 Watt will be provided and possibly the voltage disabled if the power is exceeded.

11.1.3. PoE Power Limit per Port

Here you can define for each port which maximum power any connected terminal equipment may consume. If the set power limit is exceeded, the PoE output voltage of the respective port is switched off and, for firmware versions with SNMP support, a Port PoE Overload event is sent. A special measurement procedure prevents the port from being disabled when single power peaks occur.

11.1.4. PoE Input Power Limit

Here you can define which maximum overall power may be taken from the PoE power supply. If the set power limit is exceeded, one port after the other will be switched off, starting with the highest port number, until the power consumption is within the limit again. This means that port TP-1 has highest priority and will always be the last to be disabled. However, only those ports will be switched off, which actually have a PoE load connected.
Moreover, in case of an overload, the firmware versions with SNMP support will send a Switch PoE Overload event.

11.1.5. PoE Input Voltage Alarm Limits

If the PoE power supply voltage should fall below the configured Low Limit or rise above the configured Upper Limit, all PoE output voltages will be temporarily disabled. The ports' settings will not be modified, i.e. the ports will automatically be enabled again, when the correct voltage supply has been re-established.

11.1.6. PoE Power Source

This setting is available for Office switches only which can be operated using PoE via the TP uplink port and are additionally able to pass the power partially on to the connected devices. The respective switches can be identified by means of the addition "PD-F" (IEEE802.3af, max. 12.95 Watts) and "PD-F+" (IEEE802.3at, max. 25.5 Watts) to their article description and can optionally be operated via the TP uplink or an external power supply. A simultaneous power supply via the TP uplink and an external power supply is not allowed and might damage the switch.

The following modes are available:

- AF Power from TP uplink, Max. 2x Class-1 or 1x Class-2 devices allowed (Factory Default)
- AF Power from TP uplink, Max. 2x Class-1 or 2x Class-2 devices allowed
- AT Power from TP uplink, max. 20 W allowed (Port power limits not forced)
- AT Power from TP uplink, max. 20 W or 1x Class-4 allowed (Port power limits not forced)

- External power supply

AF Power from TP uplink, Max. 2x Class-1 or 1x Class-1 devices allowed:
The switch is supplied with PoE voltage via the TP uplink port according to IEEE802.3af (max. 12.95 Watts). The maximum allowable PoE power output of all PoE ports is limited to 8 Watts. Moreover, prior to enabling the PoE voltage on the individual ports, the power classes of the connected PoE devices are verified. The switch will allow a maximum of two Class-1 end devices (2 x 3.84 Watts) or one single Class-2 end device (1x 6.49 Watts). If more Class-1 and/or Class-2 devices than allowed are connected, no PoE voltage will be enabled on the corresponding ports and the PoE indicator LED lights up red.

AF Power from TP uplink, Max. 2x Class-1 or 2x Class-1 devices allowed:
This mode is analogue to the previous mode but allows a maximum of two Class-2 devices to be connected. If, in fact, two Class-2 end devices are connected, the user must ensure that both devices together consume a maximum power of 8 Watts. If this power consumption is exceeded, a hardware reboot of the switch is possible, because the feeding core switch might turn off the voltage feed of the TP uplink port due to overload.
As a protective measure the settable power limit per port is limited to a maximum of 4 Watts. This means that the switch will immediately disable the voltage, if the end device's power consumption exceeds 4 Watts. In addition, the port changes into the PoE Overload Failure error condition and needs to be re-activated manually. Depending on the sensitiveness of the core switch in terms of its short-time exceeding the maximum power output, the protective circuit in the core switch might be enabled before the Nexans switch was able to disable the PoE voltage. The actual interoperation between the individual core switch, the Nexans switch and the connected terminal devices should be tested on site.

AT Power from TP uplink, max. 20 W allowed (Port power limits not forced):
This mode is only available for Office switches with "PD-F+" PoE+ adapter.

The switch is supplied with PoE voltage via the TP uplink port according to IEEE802.3at (max. 25.5 Watts). The maximum allowable PoE power output of all PoE ports is limited to 20 Watts. Moreover, prior to enabling the PoE voltage on the individual ports, the power classes of the connected PoE devices are verified. The switch allows Class-1, Class-2 and Class-3 devices. The number of accepted end devices depends solely on the resulting total power output. If the PoE power output of all PoE ports of 20 Watts is exceeded, no PoE voltage will be enabled on the corresponding ports and the PoE indicator LED lights up red.

AT Power from TP uplink, max. 20 W or 1x Class-4 allowed (Port power limits not forced):
This mode is only available for Office switches with "PD-F+" PoE+ adapter.

This mode is analogue to the previous mode, but one Class-4 device can alternatively be connected. If, in fact, one Class-4 terminal device is connected, the user must ensure that the device consume a maximum power of 20 Watts. If this power consumption is exceeded, a hardware reboot of the switch is possible, because the feeding core switch might turn off the voltage feed of the TP uplink port due to overload.
As a protective measure, the switch will immediately disable the voltage if the power consumption of the Class 4 device exceeds 20 Watts. In addition, the port changes into the PoE Overload Failure error condition and needs to be re-activated manually. Depending on the sensitiveness of the core switch in terms of its short-time exceeding the maximum power output, the protective circuit in the core switch might be enabled before the Nexans switch was able to disable the PoE voltage. The actual interoperation between the individual core switch, the Nexans switch and the connected terminal devices should be tested on site.

External power supply:
The switch is connected to an external power supply. The power classes are not verified, and power is limited exclusively in line with the maximum allowable power consumptions set per port and per switch.

11.1.7. PoE Reset Command

The PoE Reset command switches the PoE output voltage for the respective port off for six seconds and switches it automatically on again.

This function is quite useful for rebooting a connected access point, etc.

11.1.8. Programming of the Yellow Port LEDs on the Desk Switch

The yellow Port LED on the desk switch versions can be programmed to light up when the PoE feature has been enabled for the port in question. The setting of the LED has no influence on the port's function.

For the yellow Status-LED the following settings are possible:

1) Show Duplex - LED lights up when the port is in full duplex operating mode.
2) Off - LED is permanently off.
3) On - LED is permanently on.
4) Show POE - LED lights up when PoE for the respective port is enabled.

NOTE:

Setting 4) is the factory default, if a PoE adapter is installed.

12. Release Notes

From release V3.64 all release notes (Device Manager, Switch Basic Configurator and the Switch Firmware) are located in a separate manual called ***Nexans Switch Management - Release Notes***.

Subject to modifications.

Nexans Deutschland GmbH • Advanced Networking Solutions
Bonnenbroicher Str. 2-14 • 41238 Mönchengladbach • Tel +492166 27-2985 • Fax +492166 27-2499
E-Mail: sales.ans@nexans.com • **www.nexans.de/ans**


GigaSwitch V3