



Nexans Switch Management

mit Firmware-Version **V6.04H** oder höher

Handbuch

KD674D30

MERKMALE

- o Modulares bzw. On-Board High-Performance Management für Nexans Switche
- o Konfigurationsverwaltung und -archivierung über *Nexans Switch Manager* (NEXMAN)
- o Manuelles und automatisches Firmware-Update mittels *Nexans Switch Manager* (NEXMAN)
- o Automatisches Laden einer Switch-Konfiguration per DHCP/BootP Option möglich
- o Automatisches Laden einer neuen Firmware per DHCP/BootP und Kommando-Datei möglich
- o Passwortschutz mit zwei Access Leveln für Zugriff mittels WEB, Telnet/SSH/V.24 und NEXMAN
- o Automatische Vergabe der IP-Adresse über DHCP oder feste Einstellung der IP-Adresse möglich
- o Globaler Management Zugriffsschutz über Accessliste mit bis zu 16 IP Ranges
- o Management Status-LED für die Anzeige des Betriebszustandes
- o Konfiguration wird nichtflüchtig im Flash gespeichert
- o Anzeige der Gerätedaten wie Produktname, Seriennummer, Herstellungsdatum, Temperatur, usw.
- o Ports zu- und abschaltbar
- o Autonegotiation oder feste Einstellung der Übertragungsparameter pro TP-Port möglich
- o Fehlerzähler pro Port zur Erkennung von Duplex Fehleinstellungen
- o Unterstützung von 256 VLAN-ID's im Bereich 1 bis 4095
- o Untagged Default-VLAN pro Port einstellbar
- o Frame Tagging (Trunking) nach IEEE802.1Q pro Port zu- und abschaltbar
- o Priorisierung pro Port möglich
- o Vier Ausgangsqueues pro Port für die Priorisierungsgewichtung mit Strict oder Weighted Schema
- o Bandbreitenbegrenzung pro Port für Rx- und Tx-Frames getrennt einstellbar
- o Portsecurity über manuelle Vorgabe von bis zu drei MAC Adressen pro Port
- o Portsecurity durch automatisches Lernen von bis zu drei MAC Adressen pro Port
- o Loop/Broadcast Limiter zum Schutz von unbeabsichtigten oder böswilligen Paketstürmen
- o Switch Statusanzeige und Konfiguration über Web-Browser (HTTP und HTTPS)
- o Passwortschutz mit zwei Access Leveln (R/W bzw. R/O) für Zugriff mittels Web-Browser
- o Switch Statusanzeige und Konfiguration über SNMPv1/v2/v3 und CLI (SSH, TELNET, V.24)
- o Passwortschutz mit zwei Access Leveln (R/W bzw. R/O) für Zugriff mittels Telnet
- o Bis zu acht SNMP-Trap und Syslog Destination IP-Adressen mit jeweils 30 verschiedenen Event Typen
- o CLI und NEXMAN Authentifizierung über RADIUS Server
- o Portsecurity mit Authentifizierung der zugelassenen MAC Adressen über RADIUS Server
- o Portsecurity nach IEEE802.1X mit Authentifizierung über RADIUS Server
- o Redundanz per Rapid Spanning Tree, Multiple Spanning Tree, Media Redundancy Protocol, Link Aggregation oder HSR
- o Zero Touch Configuration
- o CLI und NEXMAN Authentifizierung und Accounting über TACACS+ Server
- o CLI Befehls-Authorisierung über TACACS+ Server
- o Access Control Lists (ACLs)
- o Skripting

INHALT

MERKMALE	1
INHALT	2
1. Unterstützte Normen und Standards	11
1.1. IEEE / ANSI / IEC / ISO / IETF / IANA:	11
1.2. RFCs:	11
1.3. SNMP MIBs:	13
2. Switchausführungen	14
2.1. Unterstützte Switchtypen	14
2.2. Unterstützte Frame- und MTU-Längen, Jumbo Frame Unterstützung	15
2.3. Core Switching Latenzzeiten	15
2.4. Core Switching Kapazitäten	16
2.5. Core Switch Paket Buffer Größen	16
3. Management Modul und Firmware-Versionen	17
3.1. Management Modul Versionen	17
3.2. Firmwarefamilien	18
3.2.1. Office Firmwarefamilien	18
3.2.2. Industrie Firmwarefamilien	18
3.3. Management Status-LED	18
3.3.1. Status-LED bei Office-Switchen Typ 'GigaSwitch V3 / V5'	19
3.3.2. Management Status-LED bei Industrie-Switchen vom Typ 'iSwitch 74X / 104x'	20
3.3.3. Management Status-LED bei Industrie-Switchen vom Typ 'iGigaSwitch 54X'	20
3.3.4. Status-LED bei Industrie-Switchen vom Typ 'iGigaSwitch 100x und 16XX'	21
3.4. Management Konfigurations-Schalter bzw. -Taster	22
3.4.1. Konfigurations- und Reset-Taster bei Switch Typen 'GigaSwitch V3 / V5'	22
3.4.2. Konfigurations-Taster bei Desk-Switchen vom Typ 'GigaSwitch Desk V3 / V5'	24
3.4.3. Konfigurations-Taster bei Industrie Switchen Typ 54X, 74x und 104x	25
3.4.4. Konfigurations-Taster bei Industrie Switchen Typ 100x und 16XX	26
3.5. Management Konfigurationsschalter deaktivieren	28
3.6. Management Betriebs-Modi	29
3.6.1. Booten mit Flash Konfiguration (Normalbetrieb)	29
3.6.2. Booten mit fester IP-Adresse	29
3.6.3. Booten mit Factory-Default Einstellungen	30
3.6.4. Booten mit Factory-Default Einstellungen und fester IP-Adresse	30
3.6.5. Booten mit Customer-Default Einstellungen	30
3.6.6. Booten ohne Customer-Reboot Einstellungen	30
4. Memory Card (MC)	31
4.1. Memory Card Schreibschutz bei HW5 Industrie-Switchen	31
4.2. Memory Card MAC-Adresse	31
4.3. Memory Card MRP-Lizenz	32
4.4. Memory Card Switch-Konfiguration	32
4.5. Memory Card Firmware-Update	33
4.6. Memory Card Mode	34
4.7. Memory Card bei Industrie Switchen vom Typ iSwitch 74x / 104X	35
4.8. Memory Card bei Industrie Switchen vom Typ iSwitch 100x / 16XX	36
4.9. Memory Card bei Kabelkanal-Switchen vom Typ 'GigaSwitch V3 / V5'	36

5. Einstellung der IP-Adresse	38
5.1. Einstellung der IP-Adresse mittels Nexans Basic Configurator	38
5.1.1. Start des Basic Configurator im (Local Mode)	38
5.1.2. Start des Basic Configurator (MAC Address Mode)	39
5.2. Einstellung der IP-Adresse mittels V.24 Console.....	40
5.3. Einstellung der IP-Adresse per DHCP	43
5.4. Einstellung des Switch Namen per DHCP	44
5.5. Einstellung der IP-Adresse per Konfigurationsschalter.....	45
5.5.1. Einstellung der IP-Adresse per Konfigurationsschalter und Web Browser.....	45
5.5.2. Einstellung der IP-Adresse per Konfigurationsschalter und TELNET Console.....	47
6. Switch Konfiguration.....	49
6.1. Switch Konfiguration mittels Nexans Switch Manager (NEXMAN)	49
6.1.1. Firmwarevoraussetzungen	49
6.1.2. Login.....	49
6.1.3. Konfiguration	49
6.2. Switch Konfiguration mittels Web-Browser (HTTP / HTTPS).....	50
6.2.1. Authentifizierung / Login.....	50
6.2.2. Konfiguration	51
6.3. Switch Konfiguration mittels V.24 Console.....	52
6.3.1. Anschluss bei Switches mit RJ11-Buchse	52
6.3.2. Anschluss beim Industrie-Switch mit RJ45-Buchse	53
6.3.3. Anschluss beim GigaSwitch V3 und GigaSwitch 5xx Desk	55
6.3.4. Firmwarevoraussetzungen	56
6.3.5. Authentifizierung / Login.....	56
6.3.6. Konfiguration	57
6.4. Switch Konfiguration mittels Telnet bzw. SSH Console	58
6.4.1. Authentifizierung / Login.....	58
6.4.2. Konfiguration	59
6.5. Switch Konfiguration mittels SNMP.....	60
6.5.1. Authentifizierung / Communities	60
6.5.2. Konfiguration	60
7. Firmware-Update und Switch-Konfiguration	61
7.1. Firmware-Update	61
7.1.1. Duale Firmware-Speicherung.....	61
7.1.2. Firmware-Update per Nexans Switch Manager (NEXMAN) ausführen	61
7.1.3. Firmware-Update per Telnet/SSH/V.24 Console ausführen	61
7.1.4. Firmware-Update automatisch per DHCP/BootP ausführen.....	62
7.1.5. Firmware-Update per PC Console und SCP.....	63
7.1.6. Firmware-Update per PC Console und TFTP	63
7.2. Switch-Konfiguration verwalten	65
7.2.1. Dateiformate der Switch-Konfiguration	65
7.2.2. Switch-Konfiguration per NEXMAN verwalten	65
7.2.3. Switch-Konfiguration per Telnet/SSH/V.24 Console und TFTP sichern	65
7.2.4. Switch-Konfiguration per Telnet/SSH/V.24 Console und TFTP laden	67
7.2.4.1. Konfiguration aus Kommando-Datei laden	67
7.2.4.2. Konfiguration aus Binär-Datei laden	68
7.2.5. Switch-Konfiguration automatisch per DHCP/BootP und TFTP laden	69

7.2.6. Switch-Konfiguration per PC Console und TFTP lesen und schreiben	70
7.2.7. Switch-Konfiguration per PC Console und SCP lesen und schreiben	71
7.2.7.1. CLI Konfiguration per PC Console und SCP lesen.....	71
7.2.7.2. CLI Konfiguration per PC Console und SCP schreiben.....	71
7.2.7.3. Binär-Konfiguration per PC Console und SCP lesen.....	71
7.2.7.4. Binär-Konfiguration per PC Console und SCP schreiben.....	71
7.2.7.5. Customer-CLI Konfigurationen per PC Console und SCP lesen.....	72
7.2.7.6. Customer-CLI Konfiguration per PC Console und SCP schreiben.....	72
7.2.8. Switch-Konfiguration ab Werk	72
7.3. Zero Touch Configuration.....	73
7.3.1. Zero Touch Configuration-Einstellungen.....	74
7.3.2. Controller IP-Adresse über DHCP Option 43 ermitteln.....	75
7.3.3. Controller IP-Adresse über DHCP Optionen 6 und 15 ermitteln.....	75
7.3.4. Statische Controller IP-Adresse	75
7.4. Skripting.....	76
7.4.1. Skript-Dateien.....	76
7.4.1.1. CLI-Skript einem Event für Statusänderung an Ports zuordnen.....	77
7.4.1.2. CLI-Skript von einem Event für Statusänderung an Ports entfernen.....	77
7.4.2. Skripting per NEXMAN.....	77
7.4.3. Skript-Datei per PC Console und SCP lesen und schreiben.....	77
7.4.3.1. Skript-Datei per PC Console und SCP lesen	77
7.4.3.2. Skript-Datei per PC Console und SCP schreiben	77
7.4.4. Skripting Beispiele	77
7.4.4.1. Switch-Name bei Link-Up / Link-Down Event ändern.....	77
7.4.4.2. Admin-Status und VLANs bei Link-Up / Link-Down Event ändern	78
7.5. TFTP Authentifizierung per SNMP	78
8. Rücksetzen auf Werkseinstellungen	80
8.1. Rücksetzen auf Werkseinstellungen per Konfigurationsschalter	80
9. Liste der Status- und Konfigurationsparameter.....	82
9.1. Hinweise zur Console Kommando Syntax	82
9.2. Aktuelle Konfiguration auf der Console ausgeben	83
9.3. Reset-Befehle	84
9.4. State > Global + Link State.....	85
9.5. State > MAC + Security State.....	88
9.6. State > PoE State	89
9.7. State > Radius State	90
9.8. State > TACACS+ State	90
9.9. Device Info.....	91
9.10. Port Setup.....	93
9.11. IPv4 / IPv6 Setup.....	97
9.12. Management > Agent	99
9.13. Management > Local Accounts	102
9.14. Management > Access Global	103
9.15. Management > Access SNMP	106
9.16. Management > Access IEC61850.....	109
9.17. Management > Banner	110
9.18. Management > Zero Touch Configuration	110

9.19. Management > Skripting	110
9.20. Global	111
9.21. VLAN > VLAN-Table	112
9.22. VLAN > VLAN Setup	113
9.23. Discovery	114
9.24. Prioritisation	116
9.25. Alarms > Alarm Destinations	117
9.26. Alarms > Global Alarms.....	118
9.27. Alarms > Alarm Inputs	119
9.28. Alarms > Alarm Inputs for 160X	120
9.29. Alarms > Alarm Outputs	120
9.30. Alarms > SFP Alarms	122
9.31. Security > Security Setup	122
9.32. Security > RADIUS Global Authentication	123
9.33. Security > RADIUS Management Authentication.....	125
9.34. Security > RADIUS Accounting	126
9.35. Security > IEEE802.1X	128
9.36. Security > TACACS+ Authentication.....	130
9.37. Security > TACACS+ Authorization.....	130
9.38. Security > TACACS+ Accounting	131
9.39. Security > Access Control List.....	132
9.40. Multicasts.....	134
9.41. Time Client > SNTP Setup	135
9.42. Time Client > Powersave Setup	136
9.43. Redundancy > Spanning Tree.....	137
9.44. Redundancy > Multiple Spanning Tree	141
9.45. Redundancy > Link Aggregation	141
9.46. Redundancy > MRP	142
9.47. Redundancy > ZeroLoss	143
9.48. DHCP Relay / Snooping	144
10. Funktionsbeschreibung Switch	145
10.1. Ermittlung von Switchtyp und Managementversion	145
10.1.1. Abfrage per WEB	145
10.1.2. Abfrage per SNMP	145
10.1.3. Abfrage per Telnet/SSH/V.24-Console	145
10.1.4. Abfrage per NEXMAN	146
10.2. Ermittlung der aktiven MAC Adresse	147
10.3. Switch Name / Location / Contact / Domain.....	147
10.4. Banner	148
10.5. Admin / User Accounts beim Management Zugriff.....	148
10.6. Passwort Encryption.....	148
10.7. Passwort strength checker	149
10.8. Konfiguration der IP- und VLAN-Parameter.....	150
10.9. ARP Tabelle	150
10.10. Manager Authentication Mode	150
10.11. HTTP Setup	151
10.11.1. HTTP Authentication Mode	151

10.11.2. HTTP TCP Port	151
10.12. HTTPS Setup	151
10.12.1. HTTPS Authentication Mode	151
10.12.2. HTTPS TCP Port	152
10.12.3. HTTPS Allowed TLS Versions	152
10.13. V.24 Console Interface	152
10.14. V.24 Console Authentication Mode	152
10.15. Console Password Mode	153
10.16. Encrypt password mode	153
10.17. Console logout time	153
10.18. Global Access / Access policy	153
10.19. Accesslist / Accesslist-Mode	153
10.20. Link Setup	154
10.20.1. Link-Typ	154
10.20.2. Admin State	155
10.20.3. Shutdown if no link	155
10.20.4. Speed / Duplex Setup	156
10.20.5. Automatic Powersave	157
10.20.6. Energy-Efficient Ethernet (EEE)	157
10.20.7. Extended Powersave	158
10.20.8. Autocrossover/Autopolarity	158
10.20.9. Client Remove Alarm	158
10.21. Link / EEE State	158
10.22. Send Link Alarms	159
10.23. Kabel Diagnose bei Twisted-Pair Ports	159
10.24. Remote Fault	159
10.25. SFP Info, Diagnose und Alarme	159
10.26. Error Counter	161
10.27. Reset all Port Counters	162
10.28. Switch Zeiten	162
10.28.1. System Up Time	162
10.28.2. Time since last link change	162
10.28.3. Network Time Protokoll - SNTP	162
10.29. Switch Temperatur	163
10.29.1. Temperatur Alarm Grenzwerte	163
10.29.2. Übertemperatur Powersave Funktion	163
10.30. Switch Betriebsspannungen	163
10.31. VLAN Unterstützung	164
10.31.1. VLAN Table	164
10.31.2. VLAN Table Mode	164
10.31.3. Fabric Attach	165
10.31.4. Globale VLAN Port Isolation	165
10.31.5. Pro-Port VLAN Port Isolation	166
10.31.6. Tagging Ethertype (Q-in-Q)	166
10.31.6.1. Q-in-Q mit zwei Nexans Switchen	166
10.31.6.2. Q-in-Q mit drei Nexans Switchen	168
10.31.7. Port Trunking Mode	168

10.31.8. Port Default-VLAN-ID	169
10.31.9. Port Voice-VLAN-ID.....	169
10.31.10. Port VLAN-Tagging	170
10.31.11. Port Active Default-VLAN-ID	170
10.31.12. Port Active Voice-VLAN-ID.....	171
10.31.13. Port Active Trunking Mode	171
10.31.14. Port Active VLAN-Tagging	171
10.31.15. RADIUS Unsecure VLAN-ID	171
10.31.16. RADIUS Guest VLAN-ID	171
10.31.17. RADIUS Inaccessible VLAN-ID	172
10.31.18. IEEE802.1X Authentication Failure VLAN-ID.....	172
10.32. VLAN Portmirror	172
10.33. Global LED Mode	172
10.34. Portmonitor	173
10.35. IEEE802.1X Transparenz.....	173
10.36. Portsecurity.....	173
10.36.1. Portsecurity - Failure Action	174
10.36.2. Portsecurity - Voice VLAN Authentication Mode	175
10.36.3. Portsecurity - Allowed MACs Overflow Address	175
10.36.4. Portsecurity - Security State	175
10.36.5. Portsecurity – Renew-Befehl	176
10.36.6. Portsecurity - Modus {Auto allow one, two or three MAC-Address(es)}	177
10.36.7. Portsecurity - Modus {Manual setting three MAC-Addresses}	177
10.36.8. Portsecurity - Modus {Manual setting three Vendor MAC-Addresses}	177
10.36.9. Portsecurity - Modus {Learn and fix one or two MAC-Address(es)}	177
10.36.10. Portsecurity - MAC Adressen	177
10.36.11. Portsecurity - MAC State.....	178
10.36.12. Portsecurity - MAC Adressen Ageing.....	179
10.37. MAC Adressen Tabelle.....	179
10.38. Quality of Service (QoS) / Priorisierung	180
10.38.1. Priorisierungsschema	180
10.38.2. Priorisierung nach IEEE802.1p	180
10.38.3. IEEE802.1p VLAN based Priority Override	181
10.38.4. Priorisierung nach IPv4/IPv6	182
10.38.5. Port Default 802.1p Priorityvalue	184
10.39. Address Ageing Time der Fowarding Tabelle	185
10.40. Port Name	185
10.41. Port Typ	185
10.42. Programmierung der Port Status-LEDs.....	186
10.43. Bandwidth-Limiter	186
10.43.1. Limiter RX/TX Bitrate	186
10.43.2. Limiter Packet Type.....	187
10.44. Flow Control	187
10.45. Layer-2 Discovery Funktionen.....	188
10.45.1. Periodisches Senden von Life und Autodiscover Paketen	188
10.45.2. Basic Configurator abschalten	188
10.46. Funktionseingänge bei Industrie und Office Switchen	188

10.46.1. Funktionseingang Alarm Mode	189
10.47. Alarmausgänge bei Industrie Switchen	189
10.48. Telnet Console Authentication Mode	190
10.49. SSHv2 Console Authentication Mode	191
10.50. SCP Authentication Mode	191
10.51. Console Password Mode.....	192
10.52. Statistic- / RMON-Counter	192
10.53. SNMP Unterstützung.....	193
10.53.1. SNMP Protocol Version.....	193
10.53.2. SNMP Access Mode	194
10.53.3. SNMPv1/v2c Communities.....	194
10.53.4. SNMPv1 MAC Table Mode	195
10.53.5. SNMPv3 Engine ID	195
10.53.6. SNMPv3 User Setup	195
10.53.7. SNMP MIB Übersicht	195
10.54. Alarm Destination Table	204
10.55. RADIUS Authentication	208
10.55.1. RADIUS Global Authentication-Einstellungen	209
10.55.2. RADIUS Management Authentication-Einstellungen	212
10.56. RADIUS Console Authentication Modes	213
10.56.1. RADIUS Attribute zur Consolen-Authentifizierung.....	214
10.57. RADIUS Manager Authentication Modes	214
10.58. RADIUS SCP Authentication Modes	215
10.59. Portsecurity mit Authentifizierung per RADIUS Server	215
10.59.1. Portsecurity Modi {RADIUS allow ...}.....	215
10.59.2. Portsecurity Modus {IEEE802.1X allow one MAC-Address}.....	219
10.59.3. Portsecurity Modus {IEEE802.1X PC+Voice allow two MAC-Addresses}.....	224
10.59.4. Portsecurity Modus {IEEE802.1X Multi-User allow three MAC-Addresses}.....	224
10.59.5. Portsecurity Modus {IEEE802.1X allow all MAC-Addresses}	225
10.59.6. Portsecurity Option {IEEE802.1X Radius MAC Bypass}	225
10.59.7. Portsecurity Option {Toggle Link}.....	227
10.59.8. Portsecurity Option {EAP Packets within Voice-VLAN}	227
10.59.9. Portsecurity Modus {IEEE802.1X Supplicant mit MD5}.....	227
10.60. RADIUS Accounting	227
10.60.1. RADIUS Accounting-Einstellungen.....	227
10.60.2. RADIUS Attribute zum Accounting.....	229
10.61. TACACS+ Authentication	230
10.61.1. TACACS+ Authentication-Einstellungen	230
10.62. TACACS+ Authorization	231
10.62.1. TACACS+ Authorization-Einstellungen.....	231
10.63. TACACS+ Accounting	232
10.63.1. TACACS+ Accounting-Einstellungen	232
10.64. TACACS+ Console Authentication Modes.....	233
10.64.1. TACACS+ Attribute zur User-Authentifizierung	234
10.64.2. TACACS+ Attribute zur User-Authorisierung	235
10.64.3. TACACS+ Attribute zum User-Accounting	236
10.65. TACACS+ Console Command Authorization.....	236

10.65.1. TACACS+ Attribute zur Consolen-Befehls-Authorisierung	237
10.65.2. TACACS+ Attributes zum Consolen-Befehls-Accounting	238
10.66. TACACS+ SCP Authentication Modes	238
10.67. TACACS+ Server-Konfiguration	239
10.67.1. TACACS+ Server für <i>Linux</i>	239
10.67.2. TACACS+ Server für <i>Windows</i>	240
10.68. Access Control Lists (ACLs)	242
10.68.1. ACL Allgemeine Konfigurationsschritte	242
10.68.2. ACL Globale Einstellungen	242
10.68.3. ACL Regel-Definition	242
10.68.3.1. IPv4 / IPv6-Layer-3-Regel erstellen	243
10.68.3.2. MAC-Layer-2 Regel erstellen	244
10.68.3.3. Regel löschen	244
10.68.3.4. Regel überschreiben	244
10.68.4. ACL-Definition	244
10.68.4.1. ACL erstellen	244
10.68.4.2. ACL löschen	244
10.68.4.3. Regel zu ACL hinzufügen	244
10.68.4.4. Regel von ACL entfernen	245
10.68.5. ACL-Zuweisung zu Interfaces	245
10.68.5.1. ACL zu Interface hinzufügen	245
10.68.5.2. ACL von Interface entfernen	245
10.68.6. Statische ACLs	245
10.68.7. Dynamische ACLs	245
10.68.8. Aktive ACLs	246
10.68.9. ACL-Status	246
10.68.10. ACL-Strategien	246
10.68.11. ACL-Beispiele	247
10.68.11.1. SSH-Verkehr blockieren	247
10.68.11.2. ICMP-Verkehr zulassen	247
10.68.11.3. Dynamische ACL-Konfiguration auf RADIUS-Server (<i>Freeradius</i>)	247
10.69. Internet Group Management Protocol (IGMP)	248
10.69.1. IGMP Snooping	248
10.69.2. IGMP Querier	249
10.70. Link Layer Discovery Protocol (LLDP)	250
10.71. LLDP for Media Endpoint Devices (LLDP-MED)	251
10.72. Cisco Discovery Protocol (CDP)	252
10.73. Rapid Spanning Tree Protocol (RSTP)	254
10.73.1. RSTP - Allgemeine Funktionsweise	254
10.73.2. RSTP - Globale Konfigurationsparameter	255
10.73.3. RSTP - Port Konfigurationsparameter	257
10.73.4. RSTP - Globale Statusparameter	260
10.73.5. RSTP - Port Statusparameter	261
10.73.6. RSTP - Konfigurationshinweise	262
10.73.7. RSTP - Konfigurationshinweise in Verbindung mit <i>Cisco PVST</i>	262
10.74. Multiple Spanning Tree Protocol (MSTP)	264
10.74.1. MSTP - Allgemeine Funktionsweise	264

10.74.2. MSTP - Identifier Setup	266
10.74.3. MSTP - Instance Setup	266
10.74.4. MSTP - Globale Statusparameter	267
10.74.5. MSTP - Instance Statusparameter	267
10.75. Link Aggregation.....	269
10.75.1. Link Aggregation - Allgemeine Funktionsweise	269
10.75.2. Link Aggregation - Global Setup	269
10.75.3. Link Aggregation – Group Setup	270
10.76. Media Redundancy Protocol (MRP)	271
10.76.1. MRP – Global Setup.....	271
10.76.2. MRP – Instance Setup	272
10.76.3. MRP – Statusparameter	272
10.76.4. MRP – MRP to Spanning Tree network coupling	273
10.77. Zeroloss Redundancy.....	275
10.77.1. Zeroloss – Global Setup.....	276
10.77.2. Zeroloss – Port Setup.....	276
10.78. DHCP Relay / Snooping	276
10.78.1. DHCP Snooping	276
10.78.2. DHCP Snooping – Global Setup	276
10.78.3. DHCP Relay Agent.....	276
10.78.4. DHCP Relay Agent – Global Setup.....	277
10.78.5. DHCP Relay Agent – Port Setup	278
10.78.6. DHCP Relay Agent – GlobalStatus.....	278
10.78.7. DHCP Relay Agent – Port Status.....	278
10.79. IEC61850 Protokoll Unterstützung	278
10.79.1. IEC61850 Übersicht	278
10.79.2. IEC61850 Access Mode	279
10.79.3. IEC61850 Objects	279
11. Funktionsbeschreibung PoE (Power-over-Ethernet).....	284
11.1. Funktionsbeschreibung PoE Allgemein.....	284
11.1.1. PoE-Messwerte	284
11.1.2. PoE Power Setup	284
11.1.3. PoE Powerlimit pro Port	285
11.1.4. PoE Input Power Limit.....	285
11.1.5. PoE Input Voltage Alarm Limits	285
11.1.6. PoE Power Source	285
11.1.7. PoE Reset-Befehl	287
11.1.8. Programmierung der gelben Port-LEDs beim Desk Switch	287
12. Release Notes	288

1. Unterstützte Normen und 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 (ehemals IEEE 802.3ad)
IEEE 802.1D	MAC Bridges
IEEE 802.1D	Rapid Spanning Tree Protocol (ehemals 802.1w)
IEEE 802.1D	Class of Service (ehemals 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 (ehemals 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	SMIPv1
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 Fields (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 (ehemals 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. Switchausführungen

Zur eindeutigen Unterscheidung ist jede funktional unterschiedliche Switchausführung einem eigenen **Switchtyp** zugeordnet.

Der aktuelle Switchtyp kann über WEB, Telnet/SSH/V.24-Console, SNMP und NEXMAN abgefragt werden (siehe Kapitel 10.1. Ermittlung von Switchtyp und Managementversion).

2.1. Unterstützte Switchtypen

Die nachfolgende Liste zeigt alle von den aktuellen Firmware Releases unterstützten Switchtypen und deren Bezeichnung.

WICHTIG:

Die in diesem Handbuch beschriebenen Funktionen werden nicht von allen Switchtypen bzw. Firmware-Versionen unterstützt.

Office Switch:

- 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

Industrie 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 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. Unterstützte Frame- und MTU-Längen, Jumbo Frame Unterstützung

In der nachfolgenden Tabelle sind die maximalen Frame- und MTU-Längen verschiedener Switchtypen angegeben. Die maximale MTU-Länge ergibt sich dabei aus der maximalen Frame-Länge abzüglich insgesamt 18 Bytes für Destination-Adresse, Source-Adresse, Type/Length-Feld und Checksumme (CRC).

Switch Typ	Max. Frame Länge 10/100/1000 MBit/s	Max. MTU Länge 10/100/1000 MBit/s	Jumbo Frame Unterstützung
iSwitch 74x iSwitch G 10xx	1632	1614	Nein
GigaSwitch V3 GigaSwitch 64x Desk V3 FiberSwitch 100 V3 FiberSwitch 1000 V3 iGigaSwitch HW3 GigaSwitch V5 GigaSwitch 64x Desk V5 iGigaSwitch HW5	9600	9582	Ja

HINWEIS ZU JUMBO FRAME UNTERSTÜTZUNG:

Auch wenn es keinen IEEE-Standard für die maximale Länge von Jumbo Frames gibt, wird im Allgemeinen die Verwendung von maximal 9000 Byte für Jumbo-Frames empfohlen. Dies stellt die Kompatibilität zwischen verschiedenen Switchherstellern sicher. Die für Nexans Switches zulässigen 9600 Bytes bieten somit genügend Spielraum für zukünftige Erweiterungen der Paketlänge, insbesondere für Anwendungen mit zusätzlichen VLAN Tags.

2.3. Core Switching Latenzzeiten

In der nachfolgenden Tabelle sind die Latenzzeiten gemäß RFC1242 angegeben. Typischerweise sind die Werte für LIFO (Last in – First Out) für Store-and-Forward Switches relevant. Die Werte für FIFO (First in – First Out) sind aus Gründen der Vollständigkeit ebenfalls aufgeführt, jedoch werden diese üblicherweise für Cut-Through Switches verwendet.

Switch Typ	100 MBit/s 64 Byte FIFO / LIFO	100 MBit/s 1518 Byte FIFO / LIFO	1 GBit/s 64 Byte FIFO / LIFO	1 GBit/s 1518 Byte FIFO / LIFO
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 Kapazitäten

In der nachfolgenden Tabelle sind die Switching Kapazitäten verschiedener Switchtypen angegeben. Die aufgeführten Switche können dabei an allen Ports unabhängig voneinander zeitgleich senden und empfangen (nicht-blockierend).

Switch Typ	Port Kapazität	Core Switching Kapazität nicht-blockierend
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	10x 2 GBit/s	30 GBit/s
iGigaSwitch 12xx/16xx	16x 2 GBit/s	50 GBit/s
GigaSwitch V3 GigaSwitch V5	5-7x 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 Paket Buffer Größen

In der nachfolgenden Tabelle sind die Größen der Paket Buffer verschiedener Switchtypen angegeben. Der Paket Buffer wird dabei dynamisch auf alle Ports verteilt.

Switch Typ	Buffer Größe
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 Modul und Firmware-Versionen

3.1. Management Modul Versionen

Abhängig vom Herstellungszeitraum und Funktionsumfang sind verschiedene Hardwareversionen des Management Modules im Einsatz (HW0, HW1, HW2, HW3 und HW5), wobei die Hardwareversionen HW0, HW1 und HW2 nicht mehr produziert werden. Ferner stehen für Office bzw. Industrie Switche separate Ausführungen mit unterschiedlichen Temperaturbereichen zur Verfügung.

Die folgende Tabelle zeigt eine Übersicht der Management Modul Versionen HW3 und HW5:

Hardwareversion	HW3 Office	HW3 Industrial	HW5 Office	HW5 Industrial
Bezeichnung	Management Module Vers. 3	Industrial Management Module Vers. 3	Office Management Hardware Vers. 5	Industrial Management Hardware Vers. 5
Sub Versionen Siehe Anm. 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	
Artikel Nummer	88301504	88301505	Nur On-Board	Nur On-Board
Bundle Code	ES3	PRO3		Ohne
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	Ohne		256 MByte	
Ethernet Anbindung des Management Prozessors	Externer Prozessor 100Mbps Anbindung		Interner Prozessor Direkter Speicherzugriff	
Firmware Update	Update in separaten FLASH Bereich. Korruption ausgeschlossen.		Duale Firmware Speicherung im internen FLASH. Korruption ausgeschlossen.	
Applikations Software	Nexans Applikations Code		Nexans Applikations Code 100% rückwärtskompatibel mit HW3 Switches	

Anm. 1) Die Sub-Version kennzeichnet die Ausführung der Hardware (z.B. steckbares Modul bzw. On-Board). Die Sub-Version wird ab Firmware- und Manager-Version V3.66 unter Device-Info angezeigt.

3.2. Firmwarefamilien

Die verschiedenen Firmware-Versionen werden abhängig vom Funktionsumfang und Switchtyp in folgende Firmwarefamilien zusammengefasst:

- Firmwarefamilien für Office Switche
- Firmwarefamilien für Industrie Switche

Die aktuell auf dem Switch installierte Firmware-Version kann über WEB, Telnet/SSH/V.24-Console, SNMP und NEXMAN abgefragt werden (siehe [10.1.Ermittlung von Switchtyp und Managementversion](#)).

Eine Übersicht aller Switchparameter befindet sich im Kapitel [9. Liste der Status- und Konfigurationsparameter](#). Hier ist dokumentiert, welche Parameter per Web, Telnet/SSH/V.24-Console, SNMP bzw. NEXMAN angezeigt bzw. konfiguriert werden können.

WICHTIG:

Die in diesem Handbuch beschriebenen Funktionen werden nicht von allen Switchtypen, Management Modulen bzw. Firmware-Versionen unterstützt.

3.2.1. Office Firmwarefamilien

Eine Übersicht der verfügbaren Firmware-Versionen zeigt die folgende Tabelle:

Mgmt Hardware Vers.	Bundle Kennung	Firmware Name	Image Dateiname	Bemerkungen
HW5	-	HW5-F40-P07-OFFICE	hw5-f40-p07-office-vx.xx.swu	Für alle HW5 Office ⁽¹⁾ Switche
HW3	ES3	HW3-F21-P06-OFFICE	hw3-f21-p06-off-vx.xx.img	Für alle HW3 Office ⁽¹⁾ Switche

Für eine Liste aller Office Switche siehe Kapitel [2.1. Unterstützte Switchtypen](#).

3.2.2. Industrie Firmwarefamilien

Eine Übersicht der verfügbaren Firmware-Versionen zeigt die folgende Tabelle:

Mgmt Hardware Vers.	Bundle Kennung	Firmware Name	Image Dateiname	Bemerkungen
HW5	-	HW5-F47-P16-INDUSTRIAL	hw5-f47-p16-industrial-v5.xx.swu	Für alle HW5 Industrie ⁽¹⁾ Switche mit 16 Ports
HW5	-	HW5-F46-P10-INDUSTRIAL	hw5-f46-p10-industrial-vx.xx.swu	Für alle HW5 Industrie ⁽¹⁾ Switche mit bis zu 10 Ports
HW3	PRO3	HW3-F30-P16-INDUSTRIAL	hw3-f30-p16-ind-vx.xx.img	Für alle HW3 Industrie ⁽¹⁾ Switche mit 16 Ports
HW3	PRO3	HW3-F22-P10-INDUSTRIAL	hw3-f22-p10-ind-vx.xx.img	Für alle HW3 Industrie ⁽¹⁾ Switche mit bis zu 10 Ports

(1) Für eine Liste aller Industrie Switche siehe Kapitel [2.1. Unterstützte Switchtypen](#).

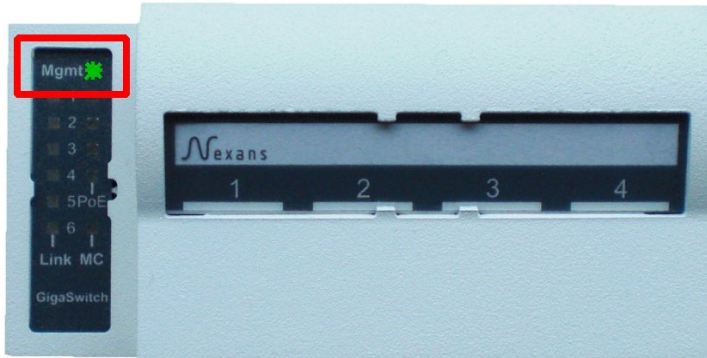
3.3. Management Status-LED

Nach dem Einschalten des Systems wird ein Selbsttest durchgeführt, der die Hardware des Switches und des Management Moduls überprüft. Sollte bei dieser Prüfung ein Fehler erkannt werden, so wird dies über die Status-LED angezeigt.

3.3.1. Status-LED bei Office-Switchen Typ 'GigaSwitch V3 / V5'

Die Lage der Status-LED zeigen die folgenden Abbildungen.

GigaSwitch V3:



GigaSwitch V5:



GigaSwitch V3 / V5 Desk:



Das On-Board Management besitzt eine Multi-Colour Status-LED mit der Bezeichnung 'Mgmt' und folgender Farbzuordnung:

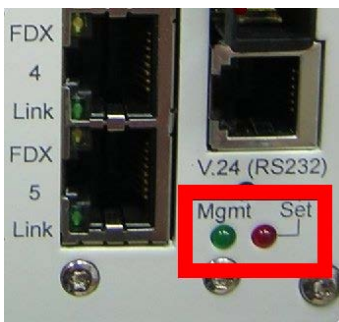
Blau:	Switch bootet
Blau blinkend:	Switch flasht neue Firmware
Grün blinkend:	Bootvorgang abgeschlossen und DHCP wartet auf eine gültige IP Adresse
Grün:	Bootvorgang abgeschlossen und IP Adresse per DHCP erhalten bzw. manuell konfiguriert
Rot:	Bootvorgang abgeschlossen und Switch läuft mit fixer IP Adresse 172.23.44.111
Rot blinkend:	Fehlerzustand, Switch oder Management Modul ggf. defekt

Während des Bootvorgangs leuchtet die Status-LED blau. Sobald alle Tests ohne Fehler abgearbeitet sind und eine gültige IP Adresse vorliegt wird die Status-LED auf grünes Dauerlicht umgeschaltet. Sollte die LED ganz aus bleiben oder rot blinken, so ist ein Fehler beim Bootvorgang oder Selbsttest aufgetreten. In diesem Fall ist der Switch auszutauschen.

3.3.2. Management Status-LED bei Industrie-Switchen vom Typ 'iSwitch 74X / 104x'

Industrie Switches besitzen zur Anzeige des Management-Status zwei LEDs, die mit dem Text **Mgmt** bzw. **Set** gekennzeichnet sind.

Die beiden LEDs befinden sich unten rechts auf der Frontplatte:

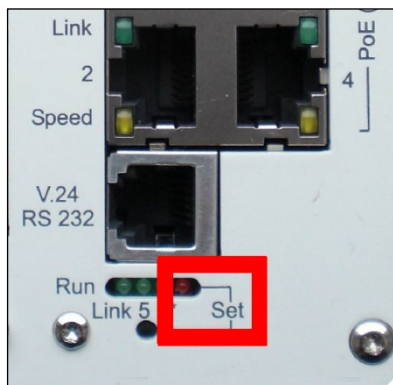


Während des Bootvorgangs muss die rote Set-LED für einige Sekunden leuchten und sobald alle Tests fehlerfrei abgearbeitet sind, wird diese ausgeschaltet und stattdessen die grüne Mgmt-LED eingeschaltet. Sollte die grüne Mgmt-LED nach ca. 30 Sekunden nicht aufleuchten oder die rote Set-LED blinken, so ist ein Fehler beim Bootvorgang oder Selbsttest aufgetreten. In diesem Fall ist das Management Modul bzw. der Switch auszutauschen.

3.3.3. Management Status-LED bei Industrie-Switchen vom Typ 'iGigaSwitch 54X'

Industrie-Switches vom Typ **iGigaSwitch** besitzen ausschließlich eine rote Set-LED zur Anzeige des Management-Status.

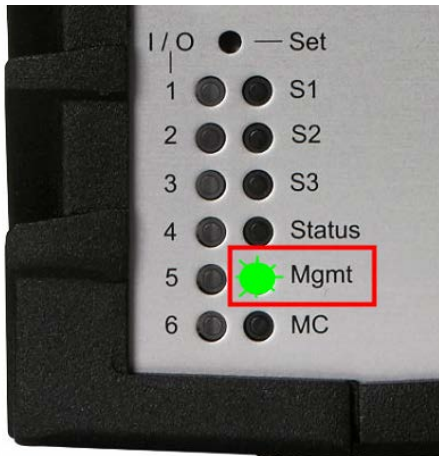
Die Lage der Set-LED zeigt die folgende Abbildung:



Während des Bootvorgangs muss die rote Set-LED für einige Sekunden leuchten und sobald alle Tests fehlerfrei abgearbeitet sind, wird diese wieder ausgeschaltet. Sollte die Set-LED ganz aus bleiben oder blinken, so ist ein Fehler beim Bootvorgang oder Selbsttest aufgetreten. In diesem Fall ist das Management Modul bzw. der Switch auszutauschen.

3.3.4. Status-LED bei Industrie-Switchen vom Typ 'iGigaSwitch 100x und 16XX'

Die Lage der Status-LED zeigen die folgenden Abbildungen.



Das On-Board Management besitzt eine Multi-Colour Status-LED mit der Bezeichnung 'Mgmt' und folgender Farbzuoordnung:

Blau:	Switch bootet
Blau blinkend:	Switch flasht neue Firmware
Grün blinkend:	Bootvorgang abgeschlossen und DHCP wartet auf eine gültige IP Adresse
Grün:	Bootvorgang abgeschlossen und IP Adresse per DHCP erhalten bzw. manuell konfiguriert
Rot:	Bootvorgang abgeschlossen und Switch läuft mit fixer IP Adresse 172.23.44.111
Rot blinkend:	Fehlerzustand, Switch oder Management Modul ggf. defekt

Während des Bootvorgangs leuchtet die Status-LED blau. Sobald alle Tests ohne Fehler abgearbeitet sind und eine gültige IP Adresse vorliegt wird die Status-LED auf grünes Dauerlicht umgeschaltet. Sollte die LED ganz ausbleiben oder rot blinken, so ist ein Fehler beim Bootvorgang oder Selbsttest aufgetreten. In diesem Fall ist der Switch auszutauschen.

3.4. Management Konfigurations-Schalter bzw. -Taster

Der Konfigurations-Schalter bzw. -Taster dient zum auswählen der folgenden Betriebsmodi:

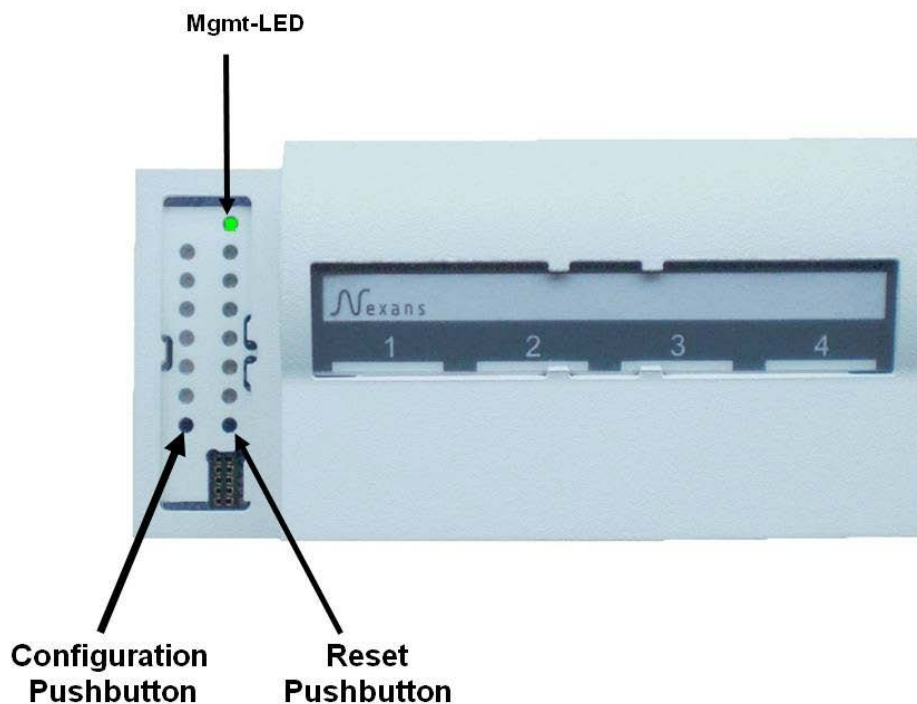
- Booten mit Flash Konfiguration (Normalbetrieb)
- Booten mit fester IP-Adresse
- Booten mit Factory-Default Einstellungen
- Booten mit Factory-Default Einstellungen und fester IP-Adresse (optional)

Für eine detaillierte Erläuterung der verschiedenen Modi siehe Kapitel [3.6. Management Betriebs-Modi](#).

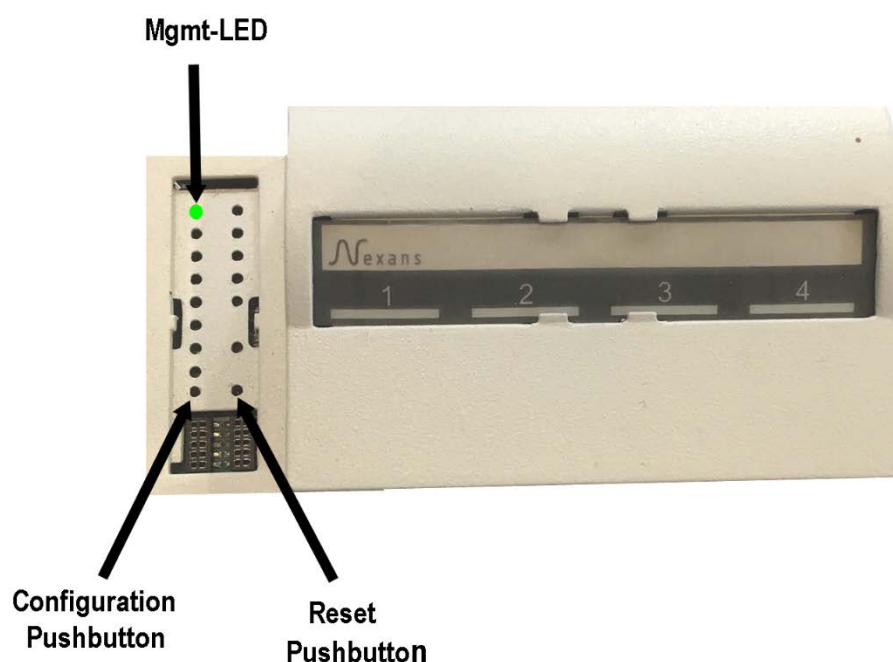
3.4.1. Konfigurations- und Reset-Taster bei Switch Typen 'GigaSwitch V3 / V5'

Die Konfigurations- und Reset-Taster sind über zwei kleine Löcher unterhalb der LED-Abdeckung zugänglich (siehe Abbildung unten). Die Betätigung der Taster kann durch einen dünnen Stift, z.B. eine aufgebogene Büroklammer, erfolgen.

GigaSwitch V3:



GigaSwitch V5:



Diese Switchtypen besitzen folgende zwei Taster:

Konfigurations-Taster

Reset-Taster

Konfigurations-Taster:

HINWEIS:

Falls Funktionen des Konfigurations-Tasters per Management deaktiviert wurden, ist entsprechend Kapitel [3.5 Management Konfigurationsschalter deaktivieren](#) vorzugehen.

Durch Drücken und Festhalten des Konfigurations-Tasters (min. 3 Sekunden) schaltet der Switch in den Konfigurationsmodus, der durch das Erlöschen der Mgmt-LED angezeigt wird. Sobald die Mgmt-LED dauerhaft aus ist, muss der Taster wieder losgelassen werden. Ein schnelles blaues Blinken der Mgmt-LED zeigt nun an, dass die Funktion Nummer 1 ausgewählt ist.

Durch kurze Betätigungen des Tasters (min. 0,1 Sekunde) kann nun die gewünschte Funktion ausgewählt werden, die jeweils über die entsprechende Farbe der LED angezeigt wird:

Funktion	Farbe	Funktion	siehe Kapitel
1	Blau	Booten mit Flash Konfiguration	3.6.1. Booten mit Flash Konfiguration (Normalbetrieb)
2	Rot	Booten mit fester IP-Adresse	3.6.2. Booten mit fester IP-Adresse
3	Weiß	Booten mit Factory-Default Einstellungen	3.6.3. Booten mit Factory-Default Einstellungen
4	Cyan	Booten mit Customer-Default Einstellungen	3.6.5 Booten mit Customer-Default Einstellungen
5	Magenta	Booten ohne Customer-Reboot Einstellungen	3.6.6 Booten ohne Customer-Reboot Einstellungen

Um die gewählte Funktion auszuführen, muss der Taster anschließend für min. 3 Sekunden gedrückt und festgehalten werden. Als Quittung, dass das Management den Befehl akzeptiert hat, geht die LED aus, blinkt nochmals kurz und erlischt dann. Nun kann der Taster wieder losgelassen werden und der Switch bootet um den Befehl auszuführen.

HINWEIS:

Der Konfigurationsmodus wird automatisch verlassen, wenn für mehr als 30 Sekunden keine Betätigung des Tasters ausführt wird.

HINWEIS:

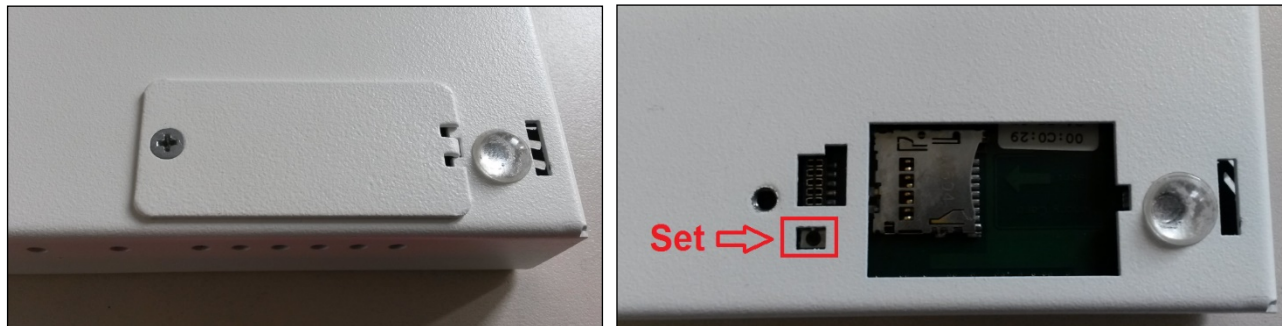
Die Funktion vier und fünf werden nur angezeigt, wenn die entsprechende Konfiguration hinterlegt ist.

Reset-Taster:

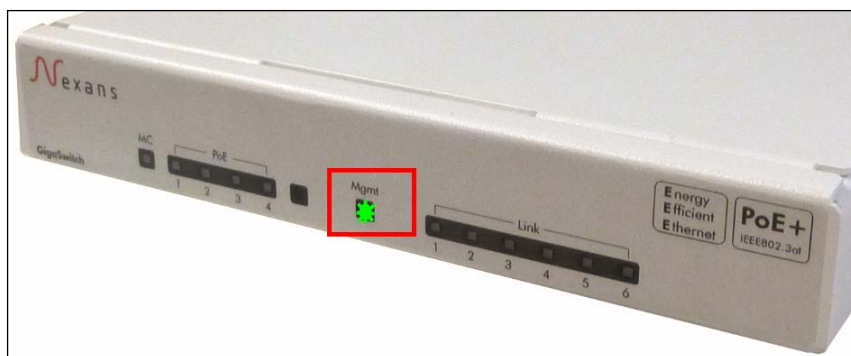
Gleichzeitiges drücken des Reset- und Konfigurations-Tasters löst einen Hardware-Reset aus.

3.4.2. Konfigurations-Taster bei Desk-Switchen vom Typ 'GigaSwitch Desk V3 / V5'

Bei Desk-Switchen vom Typ **GigaSwitch Desk** ist das Management Modul von außen nicht zugänglich. Deshalb befindet sich hier der Konfigurations-Taster hinter einer Abdeckung auf der Unterseite des Switches.



Die Managment LED ist Frontseitig zu sehen:

**HINWEIS:**

Falls Funktionen des Konfigurations-Tasters per Management deaktiviert wurden, ist entsprechend Kapitel [3.5 Management Konfigurationsschalter deaktivieren](#) vorzugehen.

Durch Drücken und Festhalten des Konfigurations-Tasters (min. 3 Sekunden) schaltet der Switch in den Konfigurationsmodus, der durch das Erlöschen der Mgmt-LED angezeigt wird. Sobald die Mgmt-LED dauerhaft aus ist, muss der Taster wieder losgelassen werden. Ein schnelles blaues blinken der Mgmt -LED zeigt nun an, dass die Funktion Nummer 1 ausgewählt ist.

Durch kurze Betätigungen des Tasters (min. 0,1 Sekunde) kann nun die gewünschte Funktion ausgewählt werden, die jeweils über die entsprechende Farbe der LED angezeigt wird:

Funktion	Farbe	Funktion	siehe Kapitel
1	Blau	Booten mit Flash Konfiguration	3.6.1. Booten mit Flash Konfiguration (Normalbetrieb)
2	Rot	Booten mit fester IP-Adresse	3.6.2. Booten mit fester IP-Adresse
3	Weiß	Booten mit Factory-Default Einstellungen	3.6.3. Booten mit Factory-Default Einstellungen
4	Cyan	Booten mit Customer-Default Einstellungen	3.6.5 Booten mit Customer-Default Einstellungen
5	Magenta	Booten ohne Customer-Reboot Einstellungen	3.6.6 Booten ohne Customer-Reboot Einstellungen

Um die gewählte Funktion auszuführen, muss der Taster anschließend für min. 3 Sekunden gedrückt und festgehalten werden. Als Quittung, dass das Management den Befehl akzeptiert hat, geht die LED aus, blinkt

nochmals kurz und erlischt dann. Nun kann der Taster wieder losgelassen werden und der Switch bootet um den Befehl auszuführen.

HINWEIS:

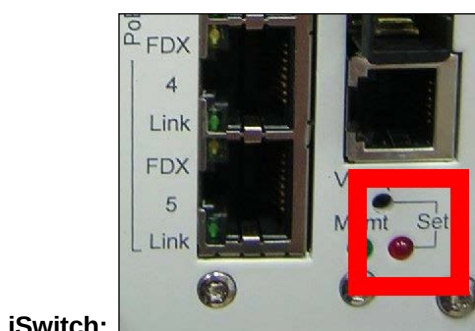
Der Konfigurationsmodus wird automatisch verlassen, wenn für mehr als 30 Sekunden keine Betätigung des Tasters ausführt wird.

HINWEIS:

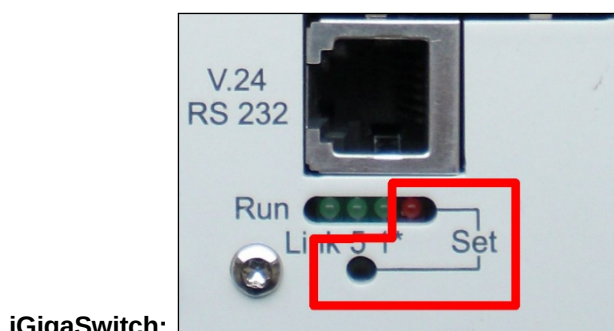
Die Funktion vier und fünf werden nur angezeigt, wenn die entsprechende Konfiguration hinterlegt ist.

3.4.3. Konfigurations-Taster bei Industrie Switchen Typ 54X, 74x und 104x

Bei Industrie-Switchen befindet sich der Konfigurations-Taster unten rechts auf der Frontplatte und ist mit dem Text **Set** gekennzeichnet:



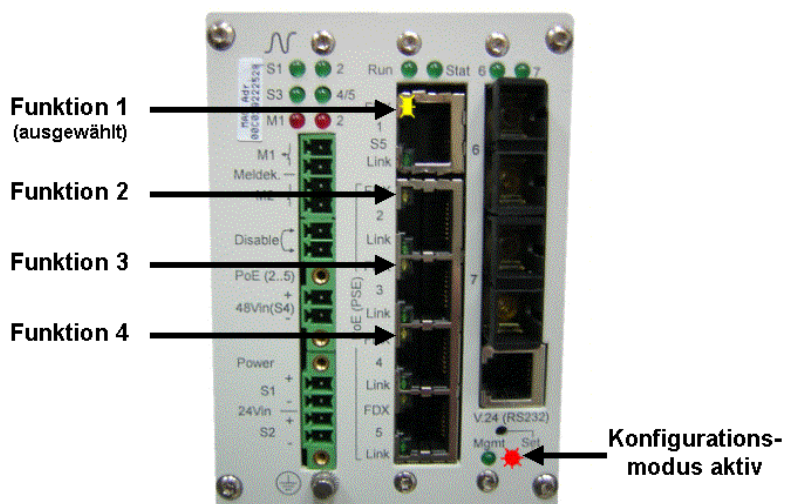
iSwitch:



iGigaSwitch:

Der Konfigurations-Taster ist über ein kleines Loch zugänglich. Die Betätigung des Tasters kann durch einen dünnen Stift, z.B. eine aufgebogene Büroklammer, erfolgen.

Durch Drücken und Festhalten des Tasters (min. 3 Sekunden) schaltet der Switch in den Konfigurationsmodus, der durch das Leuchten der roten Set-LED angezeigt wird. Sobald die Set-LED leuchtet, muss der Taster wieder losgelassen werden. Die gelbe LED der TP-Buchse 1 zeigt nun an, dass die **Funktion 1** ausgewählt ist:



Durch kurze Betätigungen des Tasters (min. 0,1 Sekunde, aber max. 2 Sekunden) kann nun die gewünschte Funktion ausgewählt werden, die jeweils über die entsprechenden gelben LEDs der TP-Buchsen angezeigt wird:

Funktion	LED	Funktion	siehe Kapitel
1	TP1	Booten mit Flash Konfiguration	3.6.1. Booten mit Flash Konfiguration (Normalbetrieb)
2	TP2	Booten mit fester IP-Adresse	3.6.2. Booten mit fester IP-Adresse

Funktion	LED	Funktion	siehe Kapitel
3	TP3	Booten mit Factory-Default Einstellungen	<u>3.6.3. Booten mit Factory-Default Einstellungen</u>
4	TP4	Booten mit Factory-Default Einstellungen und fester IP-Adresse	<u>3.6.4. Booten mit Factory-Default Einstellungen und fester IP-Adresse</u>
5	TP1 + TP2	Booten mit Customer-Default Einstellungen	<u>3.6.5 Booten mit Customer-Default Einstellungen</u>
6	TP3 + TP4	Booten ohne Customer-Reboot Einstellungen	<u>3.6.6 Booten ohne Customer-Reboot Einstellungen</u>
Hardware Reset	-	Durch Drücken und Festhalten des Tasters für mehr als 30 Sekunden wird ein Hardware-Reset des Switches ausgelöst und anschließend mit der Flash Konfiguration gebootet. HINWEIS: Der Hardware Reset wird von Switchen vom Typ 'iGigaSwitch' nicht unterstützt.	

Um die gewählte Funktion auszuführen, muss der Taster anschließend für min. 3 Sekunden gedrückt und festgehalten werden. Als Quittung, dass der Switch den Befehl akzeptiert hat, blinkt die Set-LED kurz und erlischt dann. Nun kann der Taster wieder losgelassen werden und der Switch bootet um den Befehl auszuführen.

HINWEIS:

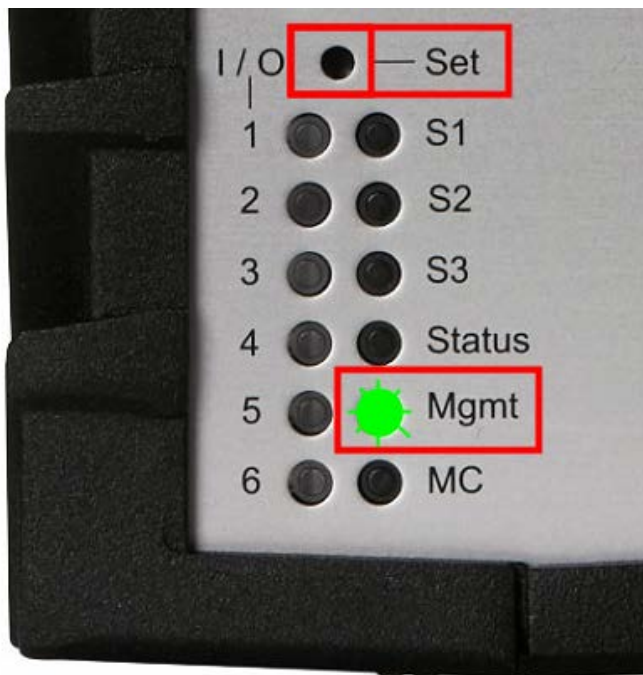
Der Konfigurationsmodus wird automatisch verlassen, wenn für mehr als 30 Sekunden keine Betätigung des Tasters ausführt wird. Dann erlischt die Set-LED und die gelben LEDs zeigen wieder ihre normale Funktionalität an.

HINWEIS:

Die Funktion fünf und sechs werden nur angezeigt, wenn die entsprechende Konfiguration hinterlegt ist.

3.4.4. Konfigurations-Taster bei Industrie Switchen Typ 100x und 16XX

Bei Industrie-Switchen vom Typ iGigaSwitch 100x und iGigaSwitch 16XX befindet sich der Konfigurations-Taster unten links auf der Frontplatte und ist mit dem Text **Set** gekennzeichnet. Die Betätigung des Konfigurations-Tasters kann durch einen dünnen Stift, oder z.B. eine aufgebogene Büroklammer erfolgen:

**HINWEIS:**

Falls Funktionen des Konfigurations-Tasters per Management deaktiviert wurden, ist entsprechend Kapitel [3.5 Management Konfigurationsschalter deaktivieren](#) vorzugehen.

Durch Drücken und Festhalten des Konfigurations-Tasters (min. 3 Sekunden) schaltet der Switch in den Konfigurationsmodus, der durch das Erlöschen der Mgmt-LED angezeigt wird. Sobald die Mgmt-LED dauerhaft aus ist, muss der Taster wieder losgelassen werden. Ein schnelles blaues blinken der Mgmt -LED zeigt nun an, dass die Funktion Nummer 1 ausgewählt ist.

Durch kurze Betätigungen des Tasters (min. 0,1 Sekunde) kann nun die gewünschte Funktion ausgewählt werden, die jeweils über die entsprechende Farbe der LED angezeigt wird:

Funktion	Farbe	Funktion	siehe Kapitel
1	Blau	Booten mit Flash Konfiguration	3.6.1. Booten mit Flash Konfiguration (Normalbetrieb)
2	Rot	Booten mit fester IP-Adresse	3.6.2. Booten mit fester IP-Adresse
3	Weiß	Booten mit Factory-Default Einstellungen	3.6.3. Booten mit Factory-Default Einstellungen
4	Cyan	Booten mit Customer-Default Einstellungen	3.6.5 Booten mit Customer-Default Einstellungen
5	Magenta	Booten ohne Customer-Reboot Einstellungen	3.6.6 Booten ohne Customer-Reboot Einstellungen

Um die gewählte Funktion auszuführen, muss der Taster anschließend für min. 3 Sekunden gedrückt und festgehalten werden. Als Quittung, dass das Management den Befehl akzeptiert hat, geht die LED aus, blinkt nochmals kurz und erlischt dann. Nun kann der Taster wieder losgelassen werden und der Switch bootet um den Befehl auszuführen.

HINWEIS:

Der Konfigurationsmodus wird automatisch verlassen, wenn für mehr als 30 Sekunden keine Betätigung des Tasters ausführt wird.

HINWEIS:

Die Funktion vier und fünf werden nur angezeigt, wenn die entsprechende Konfiguration hinterlegt ist.

3.5. Management Konfigurationsschalter deaktivieren

Booten mit fester IP-Adresse und **Booten mit Factory-Default Einstellungen** können per Management separat deaktiviert werden, um ein zufälliges oder böswilliges manipulieren durch den Benutzer auszuschließen.

Für jede Funktion sind dabei folgende Einstellungen möglich:

- Enabled Werkseinstellung, der betreffende Schalter ist aktiviert
- Disabled der betreffende Schalter ist deaktiviert und ohne Funktion

Nach Deaktivierung der Funktion **Booten mit Factory-Default Einstellungen** ist ein Rücksetzen des Switches auf Werkseinstellungen nur noch per Management Zugriff möglich (sofern der Name und das Passwort für den Admin Account bekannt sind). Ist kein Zugriff per Management möglich, weil z.B. Name oder Passwort unbekannt sind bzw. die VLAN's falsch konfiguriert wurden, so kann der Switch dennoch über einen speziellen Reset-Adapter zurückgesetzt werden. Dieser kann über Nexans unter der Part-Nr. 88301208 bezogen werden.

HINWEIS:

Ein aufgesteckter Reset-Adapter wird ausschließlich beim Booten des Switches erkannt. Ein abziehen oder aufstecken im laufenden Betrieb hat daher keine unmittelbare Auswirkung.

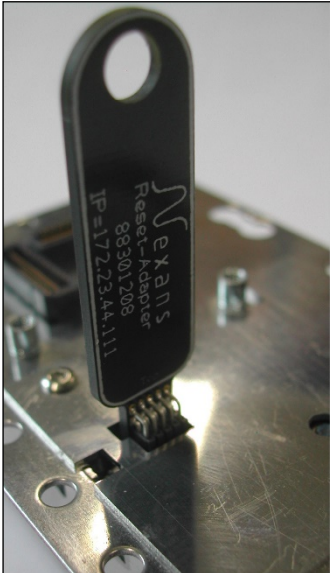
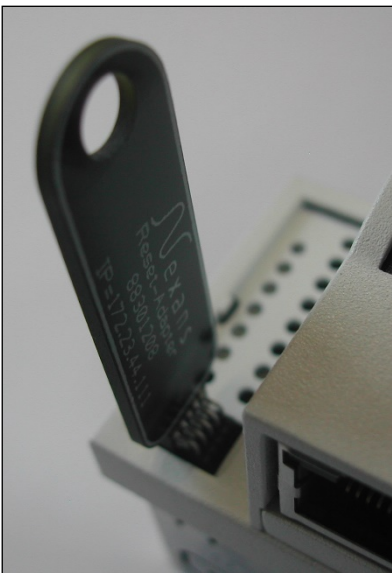
HINWEIS:

Bei Desk-Switchen vom Typ **GigaSwitch 54X** ist das Management Modul von außen nicht zugänglich. Ein zurücksetzen per Reset-Adapter ist daher nur werksseitig durch öffnen des Gehäuses möglich.

HINWEIS:

Bei Desk-Switchen vom Typ **GigaSwitch 64X** ist das Management Modul von außen nicht zugänglich. Das Management Modul befindet sich hinter einer Abdeckung auf der Unterseite des Switches.

Bei deaktivierten Konfigurationsschaltern ist die Vorgehensweise für das Rücksetzen auf Werkseinstellungen wie folgt:

1	Reset-Adapter aufstecken Der Reset-Adapter ist entsprechend den folgenden Bildern auf das Management Modul bzw. auf den GigaSwitch V3 aufzustecken. WICHTIG: Keinesfalls Gewalt anwenden sondern ggf. die richtige Lage und Position anhand des folgenden Bildes überprüfen.    Mgmt module HW0-HW3 GigaSwitch V3 / V5 GigaSwitch Desk V3 / V5
2	Switch auf eine der folgenden Arten neu booten • den Netzstecker kurz ziehen und wieder aufstecken • alternativ bei Kabelkanal-Switchen - Beim GigaSwitch V3 den Reset- und Konfigurations -Taster gleichzeitig drücken - RJ45-Aufsatz <u>OHNE</u> Schalter: RJ45-Aufsatz abziehen und wieder aufstecken - RJ45-Aufsatz <u>MIT</u> Schalter: Schalter von der Stellung 'ON' kurz in Stellung 'Reset/Standby' schieben

3	Prüfen ob Switch vollständig und korrekt gebootet hat Siehe Hinweise zur Funktion der Status-LED im Kapitel <u>3.3 Management Status-LED</u>
4	Reset-Adapter abziehen
5	Switch auf eine der folgenden Arten neu booten • den Netzstecker kurz ziehen und wieder aufstecken • alternativ bei Kabelkanal-Switchen - RJ45-Aufsatz <u>OHNE</u> Schalter: RJ45-Aufsatz abziehen und wieder aufstecken - RJ45-Aufsatz <u>MIT</u> Schalter: Schalter von der Stellung 'ON' kurz in Stellung 'Reset/Standby' schieben

3.6. Management Betriebs-Modi

Der Betriebsmodi des Managements ist per Factory-Default auf **Booten mit Flash Konfiguration** eingestellt und kann, falls erforderlich, über die im vorherigen Kapitel beschriebenen Konfigurationsschalter verändert werden.

3.6.1. Booten mit Flash Konfiguration (Normalbetrieb)

Bei dieser Funktion bootet der Switch im normalen Betriebsmodus. Dabei werden alle im Flash gespeicherten Konfigurationseinstellungen wirksam. Ist eine Customer Reboot Konfiguration vorhanden, so wird die aktuelle Konfiguration mit den Parametern der Reboot Konfiguration überschrieben.

Dies ist der Auslieferungszustand. Er sollte nur in Ausnahmefällen verändert werden, z.B. zur Inbetriebnahme oder zum rücksetzen auf Factory-Default Einstellungen.

3.6.2. Booten mit fester IP-Adresse

Durch diese Funktion werden die folgenden temporären IP-Einstellungen aktiviert:

IP-Adresse	172.23.44.111
Netzwerkmaske	255.255.255.0
MAC-Adresse	00:C0:29:01:FF:FF

Über die obige temporäre IP-Adresse kann dann auf den Switch zugegriffen werden um die gewünschten Switchparameter (z.B. die IP-Adresse) zu konfigurieren.

HINWEIS:

Zur Konfiguration der IP-Adresse sollte vorzugsweise der Nexans Basic Configurator verwendet werden (siehe Kapitel 5.1.Einstellung der IP-Adresse mittels Nexans Basic Configurator).

Der hier beschriebene Betriebsmodus, mit fester IP Adresse, ist nur dann erforderlich, wenn:

der Nexans Basic Configurator nicht verfügbar ist

oder

der Admin Name und das Passwort verändert wurden

oder

der Switchport TP1 und das Management auf verschiedene VLAN's eingestellt sind

Zusätzlich zu den IP-Parametern werden die folgenden temporären Switcheinstellungen vorgenommen:

alle Ports im selben VLAN
 Trunking für alle Ports disabled
 Admin-State für alle Ports enabled
 Link-Setup für alle Ports auf Autonegotiation / Auto-Crossover
 Portsecurity für alle Ports disabled
 Rapid Spanning Tree global disabled

Durch die obigen Einstellungen ist sichergestellt, dass der Switch über einen beliebigen Port mittels der festen IP 172.23.44.111 ansprechbar ist.

Es können nun die IP-, Link-, VLAN-, Trunking- und Portsecurity-Einstellungen vorgenommen werden, ohne dass diese Einstellungen sofort wirksam werden. Erst nach einem {Boot mit Flash Konfiguration} wird die gespeicherte Konfigurationen aktiviert.

Ferner kann ein {Boot mit fester IP-Adresse} dazu verwendet werden um die Konfiguration des Switches zu kontrollieren (z.B. falls der Switch über die erwartete IP-Adresse nicht angesprochen werden kann weil evtl. VLAN's falsch eingestellt sind).

Um per PC auf das Management Modul zugreifen zu können, muss im PC ein Routing-Eintrag für die Adresse 172.23.44.111 hinzugefügt werden.

Beispiel:

Für einen PC mit der IP-Adresse 100.10.10.1 lautet das Kommando:

```
route add 172.23.44.111 100.10.10.1
```

Möchte man, dass dieser Routing-Eintrag auch nach einem Neustart des PC erhalten bleibt so kann die Option '-p' angehängt werden:

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

Alternativ kann der PC auch auf eine IP-Adresse im Bereich 172.23.44.x (außer 172.23.44.111) und die Netzwerkmaske 255.255.255.0 konfiguriert werden (in diesem Fall ist ein Routing-Eintrag nicht erforderlich). Eine bestimmte Gateway IP-Adresse ist nicht erforderlich und ohne Auswirkung.

HINWEIS:

Durch die feste MAC-Adresse ist es möglich, mehrere Switches nacheinander zu konfigurieren ohne den ARP-Cache des PC's löschen zu müssen.

WICHTIG:

Es darf jeweils nur ein Switch im Netzwerk mit fester IP-Adresse betrieben werden, da es sonst zu Adresskonflikten kommt.

3.6.3. Booten mit Factory-Default Einstellungen

Hierbei werden ALLE im Flash gespeicherten Einstellungen mit den Factory-Default Werten überschrieben und anschließend der normale Betriebsmodus aktiviert.

3.6.4. Booten mit Factory-Default Einstellungen und fester IP-Adresse

Hierbei werden ALLE im Flash gespeicherten Einstellungen mit den Factory-Default Werten überschrieben und anschließend die Funktion **Booten mit fester IP-Adresse** ausgeführt (siehe oben im Kapitel [3.6.2. Booten mit fester IP-Adresse](#)).

3.6.5. Booten mit Customer-Default Einstellungen

Durch diese Funktion wird der Switch mit der hinterlegten „Customer Konfiguration“ gebootet. Hierbei werden alle Parameter auf Factory-Default gesetzt und danach die Parameter der „Customer Konfiguration“ geladen.

3.6.6. Booten ohne Customer-Reboot Einstellungen

Bei vorhandener „Reboot Konfiguration“ wird bei dieser Option eine Reboot durchgeführt, ohne die aktuelle Konfiguration mit den Parametern der Reboot Konfiguration zu überschreiben.

4. Memory Card (MC)

Die optionale Verwendung einer Memory Card (MC) wird von Industrie- und Office Switchen unterstützt.

Die MC dient zur Speicherung der folgenden Switch-spezifischen Daten:

- MRP Lizenz (optional, nur für Industrie-Switches mit Redundanzprotokoll MRP)
- Switch-Konfiguration (ab Firmware-Version V4.11ao mit AES-256 Verschlüsselung)
- Firmware-Update (ab Firmware-Version V4.11df)

Entsprechende Karten können Sie über Nexans als Zubehör erwerben. Dabei stehen fünf Ausführungen zur Verfügung:

- | | |
|---|-------------------|
| • 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 |

HINWEIS:

Es können ausschließlich die oben aufgeführten MC Karten verwendet werden, da diese speziell für den erweiterten Temperaturbereich spezifiziert sind. Im Computerhandel erhältliche Karten, die meist nur einen eingeschränkten Temperaturbereich aufweisen, werden vom Switch nicht akzeptiert bzw. sind für einen Dauerbetrieb ungeeignet.

HINWEIS:

Der Begriff „integrated“ bei Nexans MC Karten bedeutet, dass die MC bereits ab Werk gesteckt ist.

4.1. Memory Card Schreibschutz bei HW5 Industrie-Switchen

Bei HW5 Industrie-Switchen kann die MC-Karte über den DIP-Schalter F2 an der Frontseite des Switches schreibgeschützt werden. Ist der DIP-Schalter beim Booten des Switches eingeschaltet (Schalterstellung „On“), wird der Schreibschutz aktiviert. D.h. die aktuelle Switch-Konfiguration und neue Firmware-Updates werden nicht auf der MC-Karte gespeichert. Der Memory Card Schreibschutz wird durch eine blue leuchtende MC LED angezeigt.

HINWEIS:

Das Umschalten des DIP-Schalters F2 während des laufenden Betriebs hat keine Auswirkung auf den Schreibschutz der MC-Karte.

HINWEIS:

Der Schreibschutz kann nicht über den Lock-Schalter an der Seite der MC-Karte ein- oder ausgeschaltet werden.

4.2. Memory Card MAC-Adresse

Bei allen Nexans MC Karten wird im Werk eine eindeutige MAC-Adresse in die MC gespeichert, die auch auf der Karte aufgedruckt ist.

Wird ein Switch mit einer solchen MC gebootet, so übernimmt der Switch statt der internen MAC-Adresse im Flash die MAC-Adresse der MC für die Kommunikation. Bei Austausch des Switches bleiben somit die MAC-Adresse des Switches und evtl. vorhandene DHCP-Server Einträge erhalten.

WICHTIGER HINWEIS:

Die MAC-Adresse der MC wird nur beim Booten des Switches gelesen. Das bedeutet, dass eine im laufenden Betrieb eingesteckte MC zwar erkannt wird, aber die MAC-Adresse erst nach dem nächsten Reboot angezeigt und wirksam wird.

4.3. Memory Card MRP-Lizenz

Switche, die das Redundanzprotokoll MRP unterstützen, benötigen bis einschließlich Firmwareversion V5.03go eine MRP-Lizenz. Um MRP zu aktivieren, muss eine entsprechende MC-Karte mit einer MRP-Lizenz im Switch vorhanden sein.

Ab Firmware Version V5.03gp kann MRP auch ohne entsprechende MC-Karte aktiviert werden, da das MRP-Patent im Mai 2019 ausgelaufen ist.

4.4. Memory Card Switch-Konfiguration

Die komplette Switch-Konfiguration wird redundant im Switch und auf der MC gespeichert.

Sobald die Karte gesteckt ist, werden die Konfiguration im internen Flash des Switches und die Konfiguration auf der MC konsistent gehalten. Falls ein Switch ausgetauscht werden muss, müssen Sie lediglich die MC des alten Switches ziehen und in den neuen Switch einstecken. Beim Power-Up wird dann die Konfiguration der MC gelesen und in den internen Flash des Switches übertragen.

Die lokalen Passwörter werden per Default mit einem proprietären Verschlüsselungsverfahren auf der MC abgelegt. Um diese Passwörter besser zu schützen, sollte der Password Encryption Mode auf „SHA256 Hash“ eingestellt werden. Ist die Access Policy „Allow secure protocols and strong passwords only“ gesetzt, ist der Password Encryption Mode fest auf „SHA256 Hash“ eingestellt.

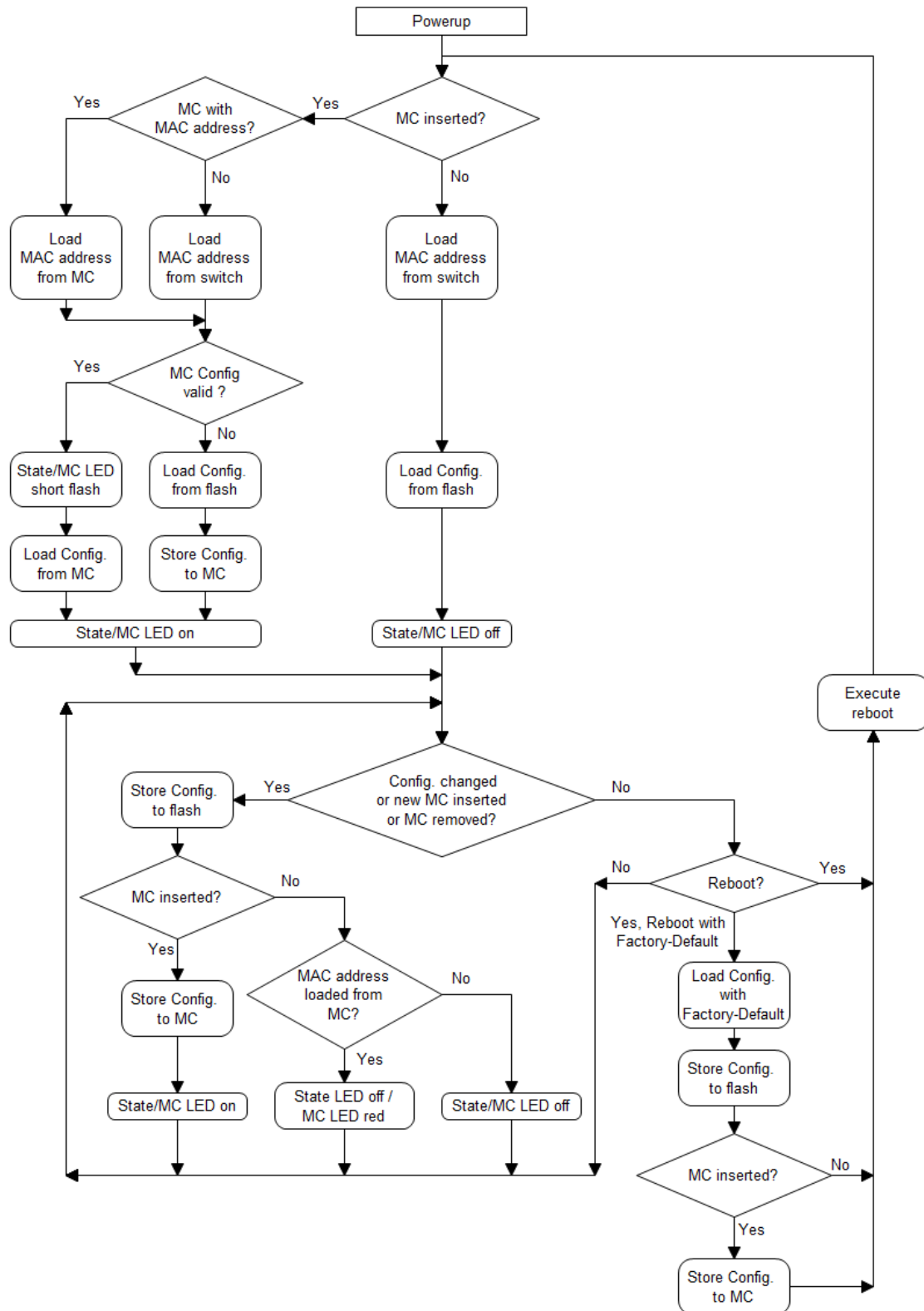
Bei dieser Einstellung werden die Passwörter der beiden lokalen Accounts ausschließlich als SHA256 Hash gespeichert. Sofern die Komplexität der Passwörter ausreichend hoch ist (mindestens 8 Zeichen, empfohlen wird 12 Zeichen), ist bei einer Kompromittierung der Memory Card und des Hash Wertes ein Rückschluss auf das Passwort praktisch unmöglich.

Ab Firmware-Version V4.11ac wird die komplette Switch-Konfiguration standardmäßig mit einer AES-256 Verschlüsselung auf die MC abgespeichert. Dies verhindert somit jegliches Auslesen der Switch-Konfiguration durch beliebige SD-Card Lesegeräte.

WICHTIGER HINWEIS:

Switche mit einer älteren Firmware-Version können die verschlüsselte Switch-Konfiguration auf der MC nicht lesen.

Das Laden und Speichern der Switch-Konfiguration (mit oder ohne MC) läuft wie folgt ab:

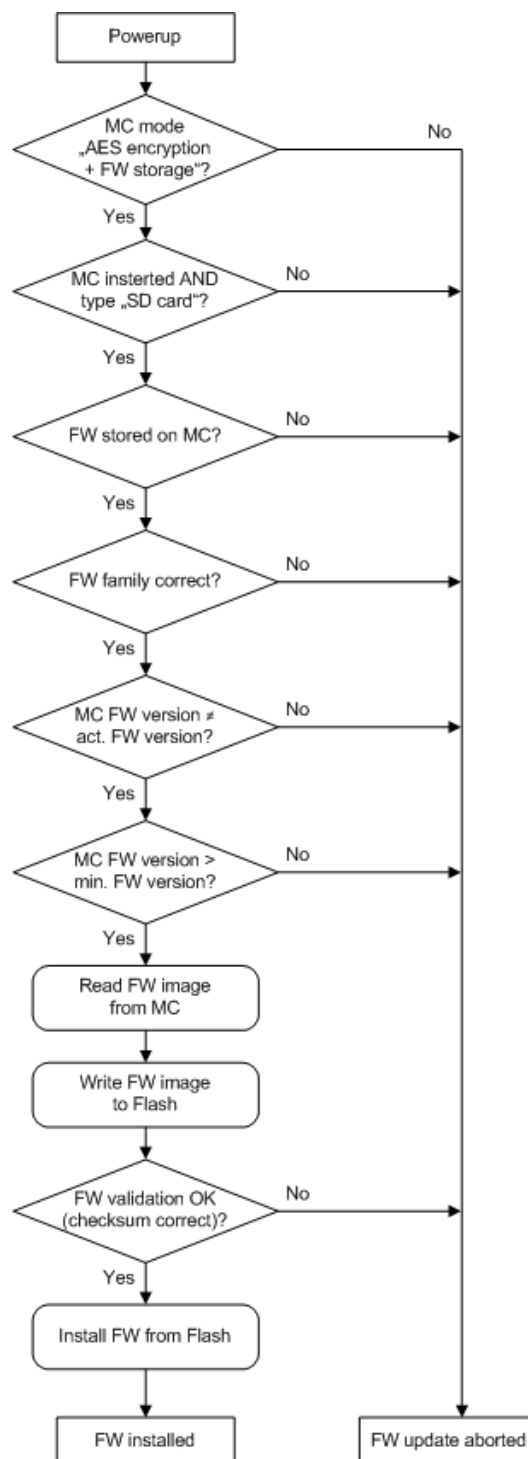


4.5. Memory Card Firmware-Update

Ab Firmware-Version V4.11df wird bei einem Firmware-Update die Firmware-Datei redundant auf der MC gespeichert (siehe Abschnitt 4.6 Memory Card Mode).

Wenn beim Firmware-Update eine MC gesteckt ist, wird die Firmware-Datei im internen Flash des Switches und auf der MC gespeichert.

Falls beim Reboot des Switches eine MC mit einer gespeicherten Firmware gesteckt ist, wird die Firmware – Version geprüft und mit der aktuellen Version verglichen. Weicht die Firmware -Version auf der MC von der aktuellen Version ab, wird die Installation der Firmware (FW) von der MC gestartet:



HINWEIS:

Die Firmware kann auf der MC-Karte über den Reset-Befehl „Reset Firmware on Memory Card“ gelöscht werden (siehe Kapitel [9.3 Reset-Befehle](#)).

4.6. Memory Card Mode

Mit dem Memory Card Mode können Sie die Funktion der Memory Card deaktivieren bzw. aktivieren.

Es gibt folgende Auswahlmöglichkeiten:

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

Enabled:

Dies ist der Factory Default Wert. Die Funktion der Memory Card ist aktiv.

Enabled with AES-256 encryption:

Die Funktion der Memory Card ist aktiv. Die Switch-Konfiguration wird AES-256 verschlüsselt, bevor sie auf der MC gespeichert wird. Eine verschlüsselte Konfiguration auf der MC kann gelesen werden, auch wenn dieser Memory Card Mode nicht gesetzt ist.

Enabled with AES-256 encryption and Firmware storage:

Die Funktion der Memory Card ist aktiv. Zusätzlich zum Speichern der Konfiguration wird bei einem Firmware-Update die Firmware-Datei im Flash und auf der MC gespeichert.

Disabled:

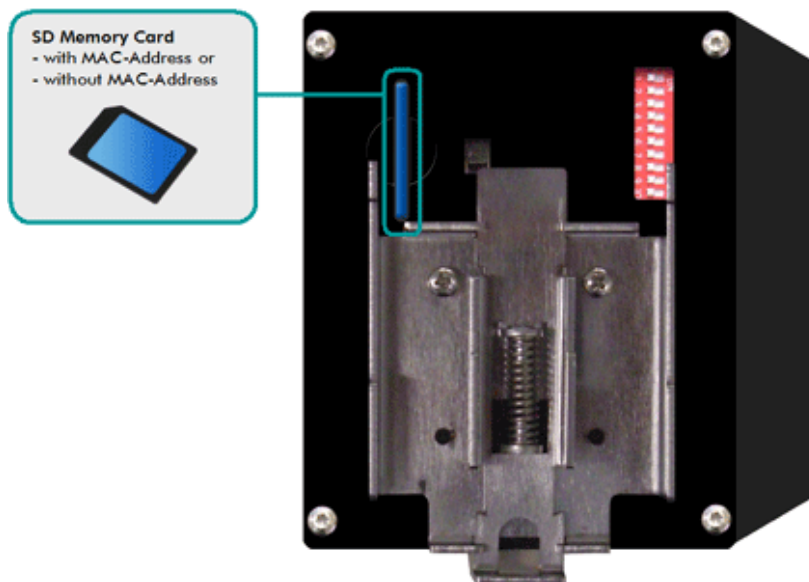
Ist der Memory Card Mode auf Disabled eingestellt, so wird die Funktion der Memory Card deaktiviert.

Permanently Disabled:

Durch Auswahl dieses Modus wird die Funktion der Memory Card unwiderruflich deaktiviert. Ein erneutes Einschalten ist nicht möglich. Das Zurücksetzen des Switches auf Factory Default Einstellungen hat ebenfalls keinen Einfluss auf diesen Modus. Um die Funktion der Memory Card wieder nutzen zu können, muss der Switch an Nexans ANS zurückgeschickt werden.

Nehmen Sie hierzu bitte Kontakt mit unserem Support unter <http://www.nexans-ans.de/support> auf.

4.7. Memory Card bei Industrie Switchen vom Typ iSwitch 74x / 104X

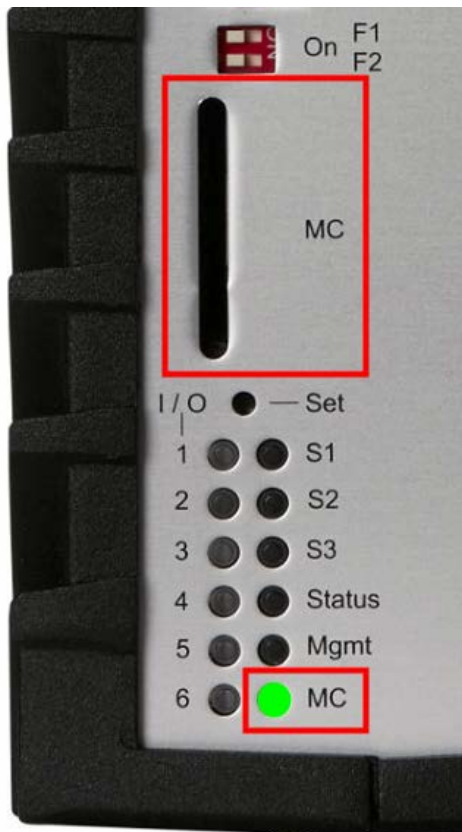


Ob eine gültige MC gesteckt ist, wird über die frontseitige grüne Status-LED angezeigt. Ferner ist der Status über die Info Seite im WEB, Telnet und NEXMAN abrufbar.

Falls der Switch mit einer gesteckten MC Karte gebootet wird und diese eine gültige Switch-Konfiguration enthält, blinkt während des Bootvorgangs die Status-LED kurz auf. Nachdem die Konfiguration der MC Karte vollständig geladen wurde, leuchtet die Status-LED anschließend permanent auf.

Falls darüber hinaus die MC-Karte während des Betriebs ausgesteckt wird, erlischt die Status-LED.

4.8. Memory Card bei Industrie Switchen vom Typ iSwitch 100x / 16XX



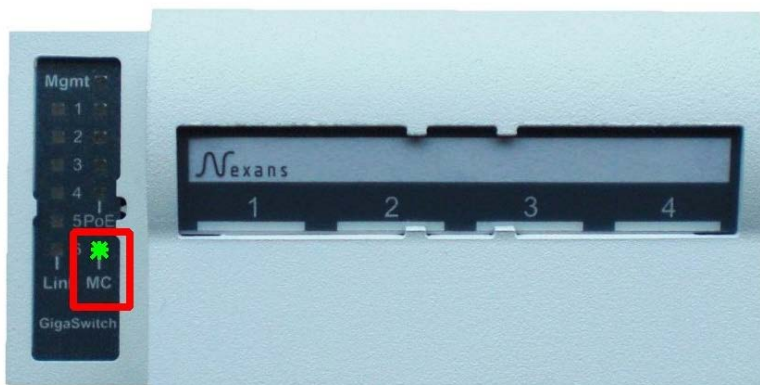
Ob eine gültige MC gesteckt ist, wird über die frontseitige Multi-Colour LED mit der Bezeichnung 'MC' angezeigt. Ferner ist der Status über die Info Seite im WEB, Telnet, SSH und NEXMAN abrufbar.

Falls der Switch mit einer gesteckten MC Karte gebootet wird und diese eine gültige Switch-Konfiguration enthält, leuchtet die MC-LED während des Bootvorgangs für einige Sekunden blau auf. Nachdem die Konfiguration der MC Karte vollständig geladen wurde, leuchtet die MC-LED anschließend permanent grün.

Falls die MC-Karte während des Betriebs ausgesteckt wird und beim Powerup die MAC-Adresse von der MC-Karte geladen wurde, leuchtet die MC-LED rot. Ansonsten erlischt die MC-LED.

4.9. Memory Card bei Kabelkanal-Switchen vom Typ 'GigaSwitch V3 / V5'

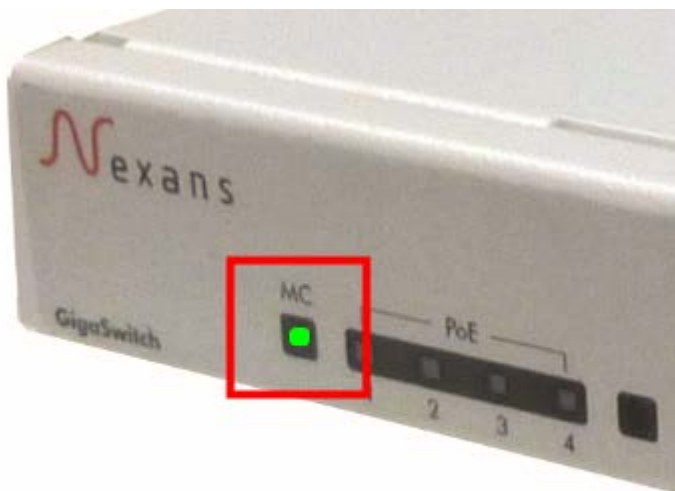
GigaSwitch V3:



GigaSwitch V5:



GigaSwitch V3 / V5 Desk:



Ob eine gültige MC gesteckt ist, wird über die frontseitige Multi-Colour LED mit der Bezeichnung 'MC' angezeigt. Ferner ist der Status über die Info Seite im WEB, Telnet, SSH und NEXMAN abrufbar.

Falls der Switch mit einer gesteckten MC Karte gebootet wird und diese eine gültige Switch-Konfiguration enthält, leuchtet die MC-LED während des Bootvorgangs für einige Sekunden blau auf. Nachdem die Konfiguration der MC Karte vollständig geladen wurde, leuchtet die MC-LED anschließend permanent grün.

Falls die MC-Karte während des Betriebs ausgesteckt wird und beim Powerup die MAC-Adresse von der MC-Karte geladen wurde, leuchtet die MC-LED rot. Ansonsten erlischt die MC-LED.

5. Einstellung der IP-Adresse

Die Konfiguration der IP-Adresse kann auf vier Arten erfolgen:

per Nexans Basic Configurator
per V.24 Console Schnittstelle
per DHCP
per Konfigurationsschalter

HINWEIS:

Per Factory-Default ist der Switch auf DHCP konfiguriert und kann daher seine Grundkonfiguration direkt über einen DHCP Server empfangen (siehe Kapitel [5.3. Einstellung der IP-Adresse per DHCP](#), [5.4. Einstellung des Switch Namen per DHCP](#) und [7.2.5 Switch-Konfiguration automatisch per DHCP/BootP und TFTP laden](#)).

5.1. Einstellung der IP-Adresse mittels Nexans Basic Configurator

WICHTIG: Für detaillierte Informationen zur Konfiguration mittels Nexans Basic Configurator bzw. Nexans Switch Manager lesen Sie bitte das jeweilige Handbuch.

Der Nexans Basic Configurator ist Bestandteil des Nexans Switch Managers (NEXMAN). Er ermöglicht die Grundkonfiguration des Switches und umfasst folgende Parameter:

Switchnamen (Name, Location, Contact)
IP Parameter (DHCP, IP Address, Netmask, Gateway)
Trunk Uplink Parameter (Trunk Port, Mgmt VLAN-ID)

Der Basic Configurator unterstützt zwei verschiedene Betriebsmodi:

Local Mode:

Der (Local Mode) dient zur lokalen Vor-Ort Konfiguration der Switchparameter. Voraussetzung ist dabei, dass das Netzkabel vom PC direkt mit dem ersten Twisted Pair Port (TP1) des Switches verbunden ist.

MAC Address Mode:

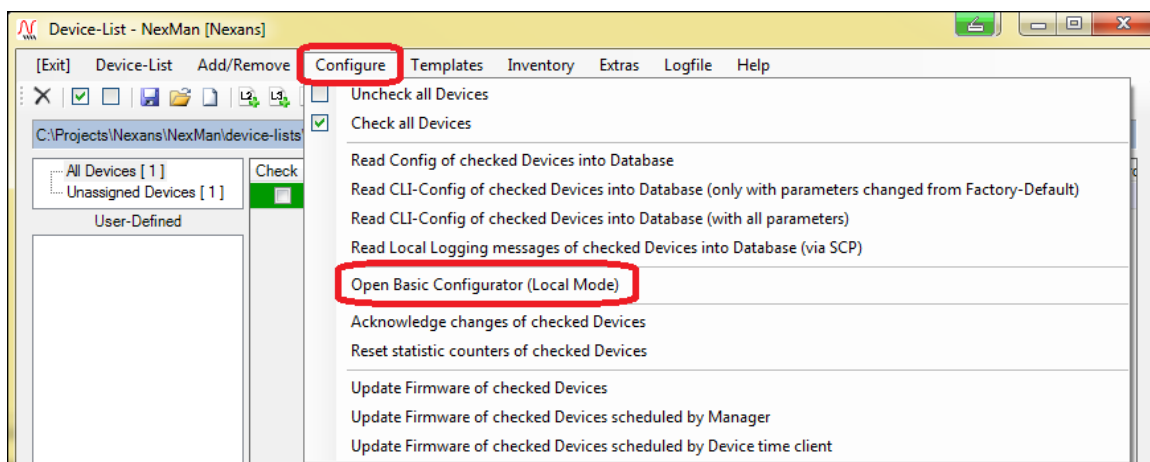
Der (MAC Address Mode) dient zur zentralen Konfiguration der Switchparameter innerhalb der NEXMAN Funktion 'Autodiscover Devices on local segments (Layer-2)' und kann deshalb nur aus dem NEXMAN heraus aufgerufen werden.

Nach der Grundeinstellung des Switches per Basic Configurator kann die weitere Konfiguration z.B. über die Device-List des Nexans Switch Manager (NEXMAN) erfolgen.

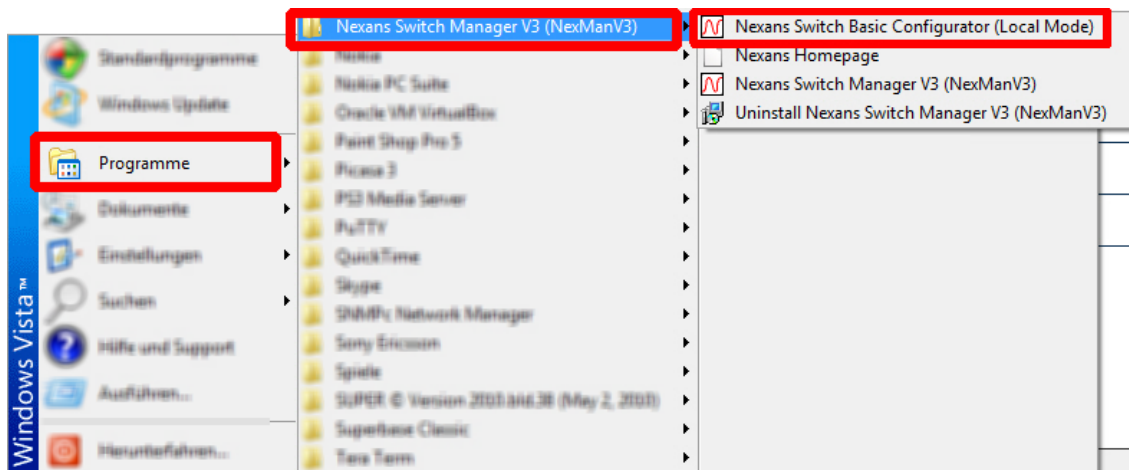
5.1.1. Start des Basic Configurator im (Local Mode)

Der Start im (Local Mode) kann auf zwei Arten erfolgen:

- Innerhalb des NEXMAN über das Menü **Configure > Open Basic Configurator (Local Mode)**:



- Über das Windows Startmenü:

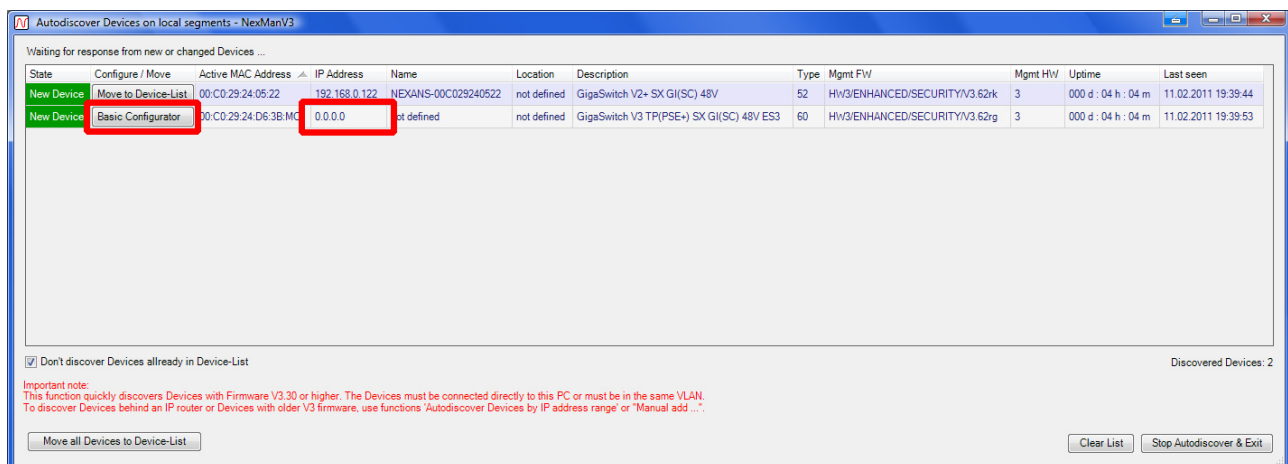


5.1.2. Start des Basic Configurator (MAC Address Mode)

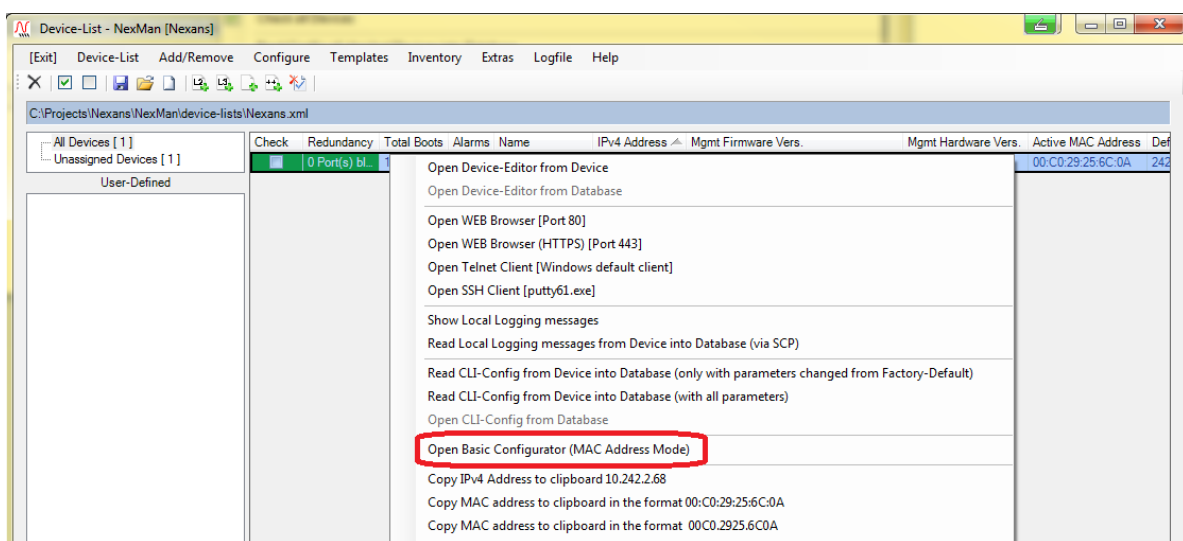
Der Start im (MAC Address Mode) kann auf zwei Arten erfolgen:

Innerhalb des NEXMAN über das Menü

Add/Remove > Autodiscover Devices on local segments (Layer-2):



Innerhalb des NEXMAN über per Rechts-Klick auf die entsprechende Zeile des Switches und Auswahl des Menüpunktes **Open Basic Configurator from Device (MAC Address Mode):**

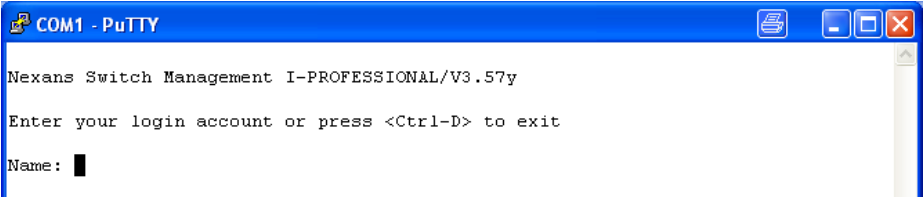
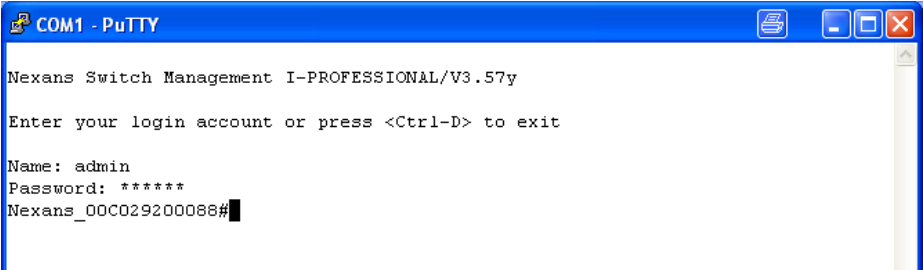
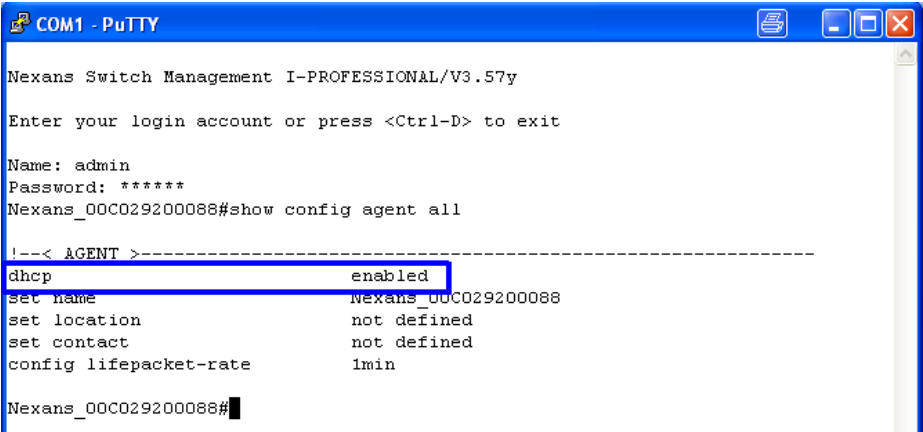


5.2. Einstellung der IP-Adresse mittels V.24 Console

Die Konfiguration mittels V.24 Console Interface wird von allen Industrie-Switchen, vom 'GigaSwitch V3' und von Desk-Switchen vom Typ 'GigaSwitch' unterstützt.

HINWEIS:

Für die korrekte Einstellung der V.24 Übertragungsparameter und die Belegung der RJ11-Buchse siehe Kapitel [6.3. Switch Konfiguration mittels V.24 Console](#).

1	Prüfen ob die Management Status-LED auf der Frontplatte des Switches richtig leuchtet Hinweise zur Funktion der Status-LED siehe Kapitel 3.3 Management Status-LED .
2	RJ11 Buchse des Switches über Adapterkabel mit dem Konfigurations-PC verbinden WICHTIG: Die V.24 Übertragungsparameter des PC's müssen korrekt eingestellt sein (siehe oben).
3	Durch drücken der <Enter> Taste den Login Modus aktivieren 
4	Benutzername und Kennwort eingeben Die Factory-Default Einstellung für den Benutzernamen ist 'admin' und für das Kennwort 'nexans'. 
5	Aktuelle IP-Einstellungen anzeigen Kommando 'show config agent all' eingeben: 

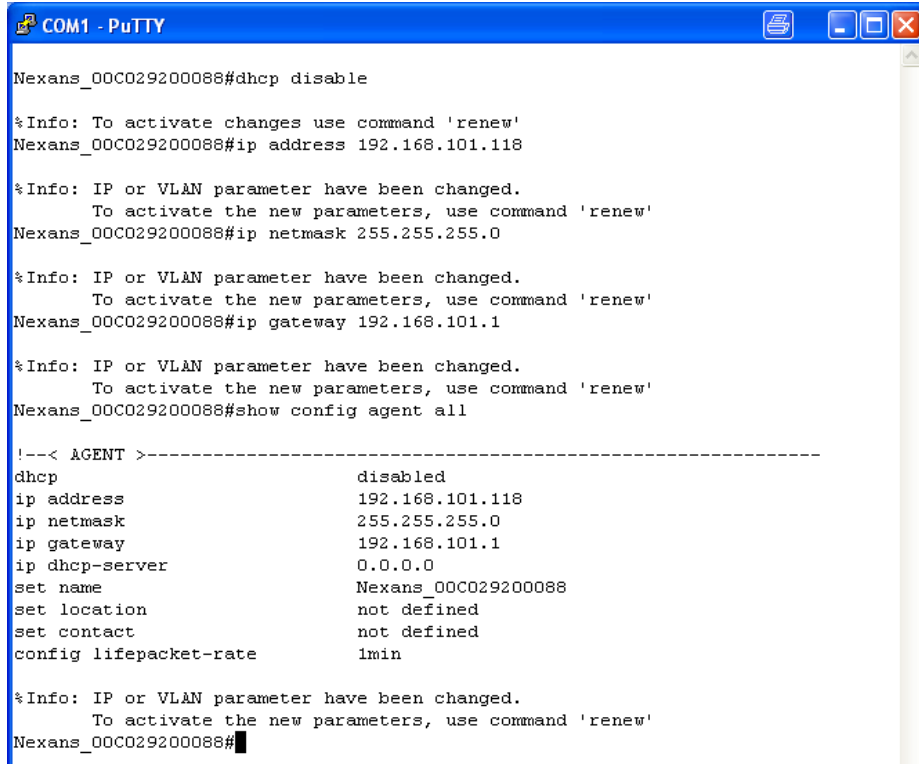
6 IP-Parameter eingeben

Folgende Console Kommandos stehen zur Verfügung:

DHCP ausschalten: dhcp disable
IP-Adresse: ip address a.b.c.d
Netzmaske: ip netmask a.b.c.d
Gateway: ip gateway a.b.c.d

Als erstes Kommando muss zunächst DHCP ausgeschaltet werden. Danach können die anderen IP-Parameter geändert werden.

Nachfolgend ein Beispiel:



```
COM1 - PuTTY
Nexans_00C029200088#dhcp disable

%Info: To activate changes use command 'renew'
Nexans_00C029200088#ip address 192.168.101.118

%Info: IP or VLAN parameter have been changed.
      To activate the new parameters, use command 'renew'
Nexans_00C029200088#ip netmask 255.255.255.0

%Info: IP or VLAN parameter have been changed.
      To activate the new parameters, use command 'renew'
Nexans_00C029200088#ip gateway 192.168.101.1

%Info: IP or VLAN parameter have been changed.
      To activate the new parameters, use command 'renew'
Nexans_00C029200088#show config agent all

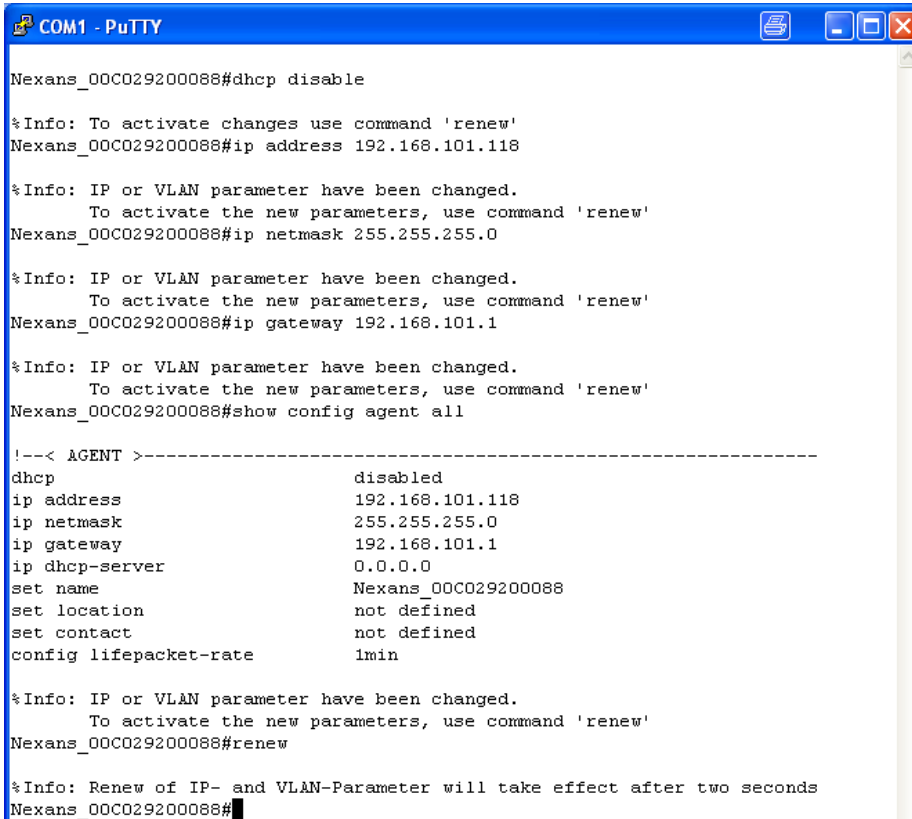
!--< AGENT >-----
dhcp                disabled
ip address          192.168.101.118
ip netmask          255.255.255.0
ip gateway          192.168.101.1
ip dhcp-server      0.0.0.0
set name            Nexans_00C029200088
set location        not defined
set contact         not defined
config lifepacket-rate 1min

%Info: IP or VLAN parameter have been changed.
      To activate the new parameters, use command 'renew'
Nexans_00C029200088#
```

7 Neue IP Parameter aktivieren

Konfigurationsänderungen an den IP- und VLAN-Parametern per V.24, Telnet, Web oder SNMP, werden nicht sofort wirksam, sondern erst nach Ausführen des Kommandos {Renew IP- and VLAN-Parameter}.

Das entsprechende Console Kommando hierfür lautet 'renew'



```
COM1 - PuTTY
Nexans_00C029200088#dhcp disable
%Info: To activate changes use command 'renew'
Nexans_00C029200088#ip address 192.168.101.118
%Info: IP or VLAN parameter have been changed.
      To activate the new parameters, use command 'renew'
Nexans_00C029200088#ip netmask 255.255.255.0
%Info: IP or VLAN parameter have been changed.
      To activate the new parameters, use command 'renew'
Nexans_00C029200088#ip gateway 192.168.101.1
%Info: IP or VLAN parameter have been changed.
      To activate the new parameters, use command 'renew'
Nexans_00C029200088#show config agent all

!--< AGENT >-----
dhcp                disabled
ip address          192.168.101.118
ip netmask          255.255.255.0
ip gateway          192.168.101.1
ip dhcp-server      0.0.0.0
set name            Nexans_00C029200088
set location        not defined
set contact         not defined
config lifepacket-rate 1min

%Info: IP or VLAN parameter have been changed.
      To activate the new parameters, use command 'renew'
Nexans_00C029200088#renew
%Info: Renew of IP- and VLAN-Parameter will take effect after two seconds
Nexans_00C029200088#
```

Nach Ausführen dieses Kommandos ist das Management-Modul sofort über die neuen IP-Parameter ansprechbar. Ein Reboot ist dabei nicht erforderlich.

5.3. Einstellung der IP-Adresse per DHCP

Für die Konfiguration per DHCP wird ein DHCP-Server benötigt. Das DHCP - Abkürzung für 'Dynamic Host Configuration Protocol', weist dem Switch aus einem festgelegten Bereich von IP-Adressen automatisch IP-Adressen zu und spart so viel Konfigurationsarbeit bei größeren Netzen. Neben einer IP-Adresse erhält der Switch auch zusätzliche Informationen, etwa die Adresse des Gateways und die Netzwerkmaske.

Soll sichergestellt werden, dass der Nexans Switch eine festgelegte IP-Adresse erhält, so muss dem DHCP-Server die MAC-Adresse des Switches bekannt gemacht werden und zu dieser MAC-Adresse eine feste IP-Adresse eingetragen werden.

Wegen der Vielzahl von DHCP-Servern kann hier nicht auf die Vorgehensweise zur Konfiguration des Servers eingegangen werden. Diesbezüglich sollte der Netzwerkadministrator kontaktiert werden.

Die für den DHCP-Server benötigte MAC-Adresse des Switches befindet sich auf dem Typenschild des Systems oder (bei Kabelkanalmodulen) unterhalb des RJ45-Aufsatzes (Aufsatz dazu abziehen):

00 C0 29 __ __ __ (12 Zeichen lang)

Unmittelbar nachdem die Status-LED auf dem Management Modul permanent leuchtet, sendet der Switch einen DHCP-Request. Erhält er eine gültige Antwort von einem DHCP-Server, so werden die IP-Parameter übernommen und das Management-Modul ist sofort über die zugewiesene IP-Adresse ansprechbar. Erhält der Switch keine Antwort, so wird der DHCP-Request in immer größeren Zeitintervallen wiederholt (der maximale Abstand beträgt ca. 30 Sekunden).

Als einfacher Verbindungstest kann z.B. ein Ping-Befehl ausgeführt werden. Nachdem das Modul nun über die zugewiesene IP-Adresse ansprechbar ist, kann, falls gewünscht, die DHCP-Funktion abgeschaltet werden und ggf. weitere Änderungen an den IP-Parametern per WEB, Telnet, SNMP oder NEXMAN vorgenommen werden.

DHCP ist die Werkseinstellung des Management Moduls. Alle IP Parameter des letzten erfolgreichen DHCP-Acknowledge werden im Flash gespeichert (incl. der DHCP Server IP-Adresse). Nach einem Reboot oder Power-Up wird zunächst versucht die IP-Parameter vom gespeicherten DHCP Server per DHCP-Request zu erhalten. Nur wenn dies nach drei Versuchen fehlschlägt bzw. nach Factory-Default Reset wird ein DHCP-Discover ausgeführt.

Abhängig von der Lease-Time im DHCP-Acknowledge, sendet der Nexans Switch einen neuen DHCP-Request um die IP-Adresse beim DHCP-Server zu bestätigen. Dabei wird der erste DHCP-Request nach der halben Lease-Time versendet und es wird zunächst versucht, die IP-Parameter vom gespeicherten DHCP Server zu erhalten. Nur wenn dies nach drei Versuchen fehlschlägt wird ein DHCP-Discover ausgeführt, auf den alle DHCP-Server antworten dürfen. Der DHCP-Discover wird dann in 30 Sekunden Intervallen solange wiederholt, bis ein DHCP-Server antwortet. Nach Ablauf der kompletten Lease-Time wird dann die zuvor erhaltene IP-Adresse im Nexans-Switch gelöscht. Nach jedem Empfang eines DHCP-Acknowledge, wird die Lease-Time im Switch neu festgelegt, d.h., dass eine Änderung der Lease-Time auf dem DHCP-Server jeweils beim nächsten DHCP-Request des Switches übernommen wird.

Es wird empfohlen, die Lease-Time auf einen Wert von 10 Tagen oder höher zu setzen. Dies garantiert die Erreichbarkeit der Switches im Falle eines längeren Ausfalls des DHCP-Servers (bei einer Lease-Time von 10 Tagen dürfte der DHCP-Server max. 5 Tage ausfallen).

Folgende Optionen werden im DHCP Discover bzw. DHCP Request vom Switch gesendet:

Option	Option Bezeichnung	Bemerkung
53	DHCP Message Type	Enthält entweder den Typ "Discover" oder "Request"
60	Vendor Class Identifier	Enthält den Hersteller und Gerätetyp des Switches im folgenden Format: 266:XXX 266 ist dabei die Nexans Private Enterprise Nummer gemäß IANA (siehe http://www.iana.org/assignments/enterprise-numbers) XXX ist der Switchtyp gemäß Kapitel <u>2.1 Unterstützte Switchtypen</u>
61	Client Identifier	Die MAC Adresse des Switches

50	Requested IP Address	Wird ausschließlich im DHCP Request gesendet und enthält die beantragte IP Adresse. Diese IP Adresse wurde zuvor vom DHCP Server per DHCP Offer bzw. DHCP Acknowledge übermittelt.
54	DHCP Server Identifier	Wird ausschließlich im DHCP Request gesendet und enthält die IP-Adresse des gewünschten DHCP Servers. Diese IP Adresse wurde vom letzten gültigen DHCP Server übernommen.
12	Host Name	Der benutzerdefinierte Name des Switches. HINWEIS: Falls der DHCP Server diese Option zurücksendet wird der enthaltene Host Name als Switchname übernommen.
55	Parameter Request List	Eine Liste der vom DHCP Server angeforderten Informationen. Diese enthält folgende Werte: 1 Subnet Mask 3 Router IP 12 Host Name 66 TFTP Server Name 67 Bootfile Name

Folgende Optionen im DHCP Acknowledge des DHCP Servers werden vom Switch ausgewertet:

Option	Option Bezeichnung	Bemerkung
53	DHCP Message Type	Muss entweder den Typ "Offer" oder "Acknowledge" enthalten
12	Host Name	Der übermittelte Host Name wird als Switchname übernommen.
66 67	TFTP Server Name Bootfile Name	Falls in der Option 66 eine gültige IP Adresse und in der Option 67 ein Dateiname übermittelt wurde, so wird der Switch die angegebene Datei über die IP Adresse per TFTP laden und als CLI-Skript ausführen. Für eine detaillierte Erläuterung der Funktion siehe Kapitel <u>7.2.5 Switch-Konfiguration automatisch per DHCP/BootP und TFTP laden</u>

Sollte die DHCP-Funktion abgeschaltet sein, so kann diese über die Konfigurationsschalter wieder auf Werkseinstellung zurückgesetzt werden (siehe Kapitel [8. Rücksetzen auf Werkseinstellungen](#)).

5.4. Einstellung des Switch Namen per DHCP

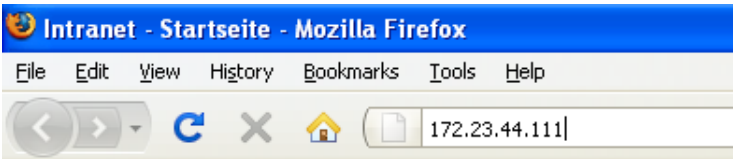
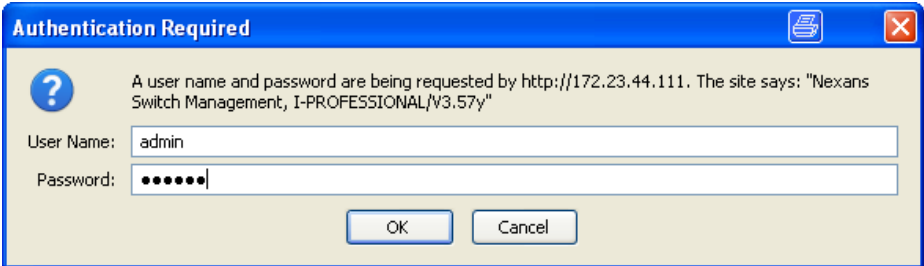
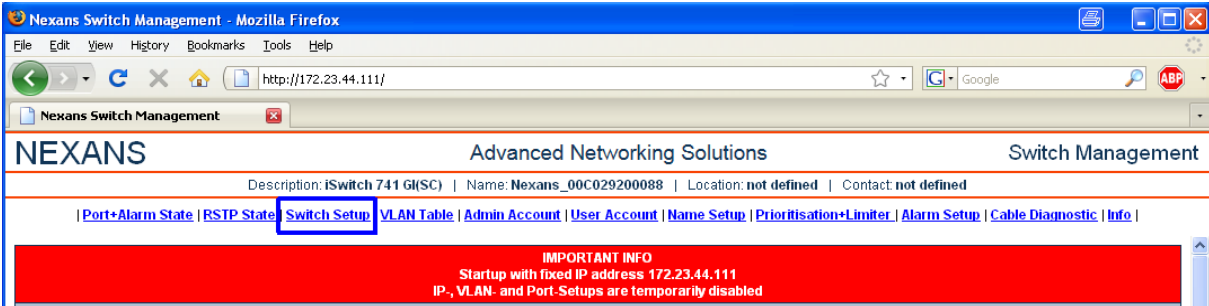
Der Name des Switches kann optional über die DHCP Option 12 'Host Name' zugewiesen werden. Die Länge des Namens darf dabei 50 Zeichen nicht überschreiten, ansonsten wird dieser ignoriert. Fehlt diese Option, wird der Name des Switches unverändert beibehalten.

5.5. Einstellung der IP-Adresse per Konfigurationsschalter

Die Einstellung der IP-Adresse mit Hilfe des Konfigurationsschalters und der Funktion {Booten mit fester IP-Adresse} ist nur dann erforderlich wenn:

- der Nexans Basic Configurator nicht verfügbar ist
- oder
- Admin Name und Passwort verändert wurden
- oder
- der Switchport TP1 und das Management auf verschiedene VLAN's eingestellt sind

5.5.1. Einstellung der IP-Adresse per Konfigurationsschalter und Web Browser

1	Booten mit fester IP-Adresse Switch per Konfigurationsschalter mit fester IP-Adresse booten. Detaillierte Vorgehensweise siehe Kapitel 3.4. Management Konfigurations-Schalter bzw. -Taster
2	Prüfen ob die Status-LED auf dem Management Modul permanent leuchtet Hinweise zur Funktion der Status-LED siehe Kapitel 3.3 Management Status-LED .
3	Switch über Netzwerk mit dem Konfigurations-PC verbinden Die Verbindung zum Konfigurations-PC erfolgt entweder über eine direkte Twisted-Pair-Verbindung zwischen Switch und PC, oder über den Uplink-Port und das bestehende Hausnetz. WICHTIG: Die IP Einstellungen des PC's müssen korrekt eingestellt sein. Hinweise hierzu siehe Kapitel 3.6.2. Booten mit fester IP-Adresse
4	Web-Browser starten und die IP-Adresse 172.23.44.111 eingeben 
5	Benutzername und Kennwort für den Zugriff auf das Management Moduls eingeben  Die Factory-Default Einstellungen für Name und Passwort lauten: Name=admin, Passwort=nexans
6	Die Web-Seite 'Switch Setup' auswählen 

7 IP-Parameter eingeben

WICHTIG: Der Haken für DHCP muss entfernt werden damit die IP-Parameter als feste Vorgabe übernommen werden.

Als letztes müssen alle Einstellungen durch anklicken des 'Set' Buttons abgespeichert werden.

IP Setup	
DHCP enabled	☐ [-1]
IP Address	192.168.101.118 [-1]
Netmask	255.255.255.0 [-1]
Gateway	192.168.101.1 [-1]
Global Setup	
Refreshrate for Port and PoE State pages	5 sec
Reset command	none
VLAN Table Mode	Static [-1]
Renew Command	
Renew IP and VLAN parameter	☐
Set successful	
[-1] To activate changes for this parameters, use the above Renew Command [Renew IP and VLAN parameter]	
Set	

8 Booten mit Flash Konfiguration

Switch per Konfigurationsschalter mit Flash Konfiguration booten.

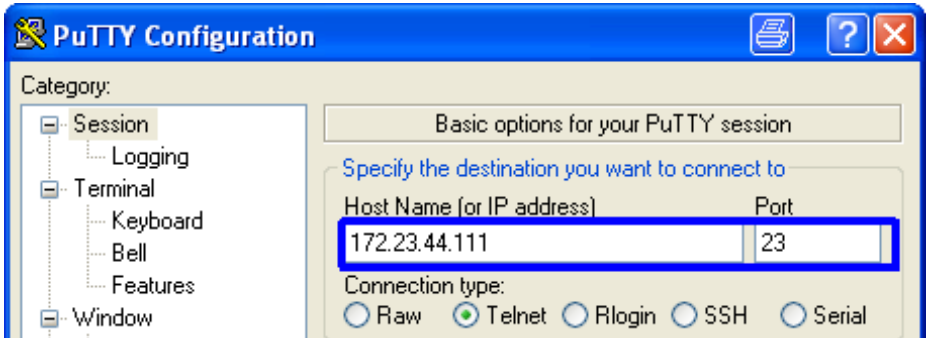
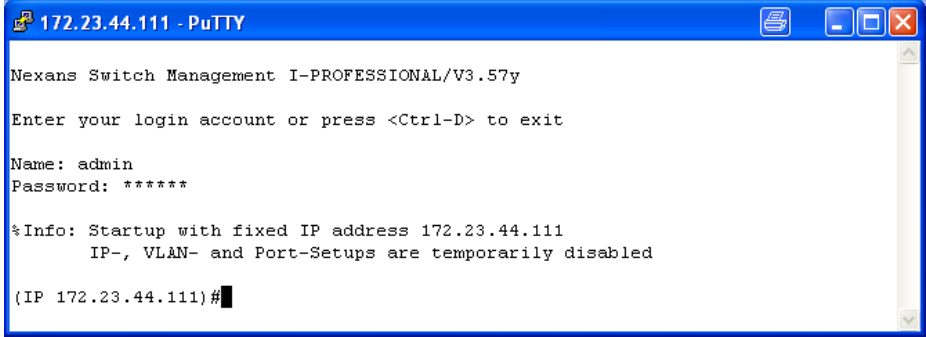
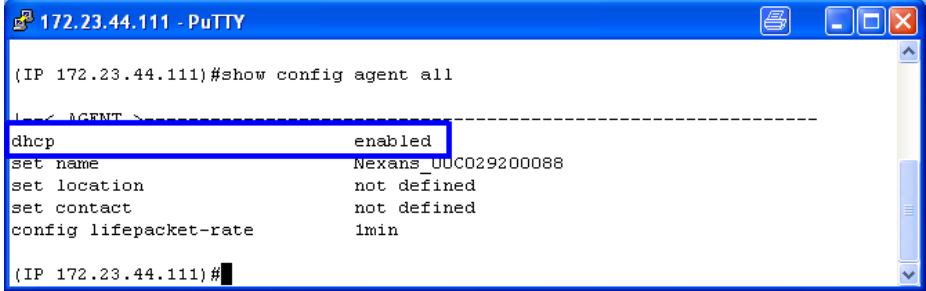
Detaillierte Vorgehensweise siehe Kapitel 3.4. Management Konfigurations-Schalter bzw. -Taster

9 Prüfen ob die Status-LED auf dem Management Modul permanent leuchtet

Jetzt ist der Switch erfolgreich mit den neuen IP-Parametern initialisiert worden und kann im endgültigen Subnetz unter der neuen IP-Adresse angesprochen werden.

Erst hier sollten die weiteren Einstellungen wie 'Name Setup', 'Port Setup', 'VLAN Setup' usw. durchgeführt werden.

5.5.2. Einstellung der IP-Adresse per Konfigurationsschalter und TELNET Console

1	Booten mit fester IP-Adresse Switch per Konfigurationsschalter mit fester IP-Adresse booten. Detaillierte Vorgehensweise siehe Kapitel 3.4. Management Konfigurations-Schalter bzw. -Taster
2	Prüfen ob die Status-LED auf dem Management Modul permanent leuchtet Hinweise zur Funktion der Status-LED siehe Kapitel 3.3 Management Status-LED .
3	Switch über Netzwerk mit dem Konfigurations-PC verbinden Die Verbindung zum Konfigurations-PC erfolgt entweder über eine direkte Twisted-Pair-Verbindung zwischen Switch und PC, oder über den Uplink-Port und das bestehende Hausnetz. WICHTIG: Die IP Einstellungen des PC's müssen korrekt eingestellt sein. Hinweise hierzu siehe Kapitel 3.6.2. Booten mit fester IP-Adresse .
4	Telnet mit IP-Adresse 172.23.44.111 starten 
5	Benutzername und Kennwort für den Zugriff auf das Management Modul eingeben  Als Benutzernamen 'admin' und als Kennwort 'nexans' eingeben. Zur Kennzeichnung, dass der Switch auf die feste IP-Adresse eingestellt ist, wird als Prompt die IP-Adresse angezeigt und ein entsprechender Infotext ausgegeben.
6	Aktuelle IP-Einstellungen anzeigen Console Kommando 'show config agent all' eingeben: 

7 IP-Parameter eingeben

Folgende Console Kommandos stehen zur Verfügung:

DHCP ausschalten: `dhcp disable`
 IP-Adresse: `ip address a.b.c.d`
 Netzmaske: `ip netmask a.b.c.d`
 Gateway: `ip gateway a.b.c.d`

Als erstes Kommando muss DHCP ausgeschaltet werden. Danach können die anderen IP-Parameter geändert werden.

Nachfolgend ein Beispiel:

```
(IP 172.23.44.111)#dhcp disable
%Info: Reboot switch with FLASH configuration to take changes in effect
(IP 172.23.44.111)#ip address 192.168.101.118
%Info: Reboot switch with FLASH configuration to take changes in effect
(IP 172.23.44.111)#ip netmask 255.255.255.0
%Info: Reboot switch with FLASH configuration to take changes in effect
(IP 172.23.44.111)#ip gateway 192.168.101.1
%Info: Reboot switch with FLASH configuration to take changes in effect
(IP 172.23.44.111)#show config agent all
!--< AGENT >-----
dhcp                disabled
ip address           192.168.101.118
ip netmask           255.255.255.0
ip gateway           192.168.101.1
ip dhcp-server       0.0.0.0
set name              Nexans_00C029200088
set location          not defined
set contact           not defined
config lifepacket-rate 1min
(IP 172.23.44.111)#
```

8 Booten mit Flash Konfiguration

Switch per Konfigurationsschalter mit Flash Konfiguration booten.

Detaillierte Vorgehensweise siehe Kapitel 3.4. Management Konfigurations-Schalter bzw. -Taster

9 Prüfen ob die Status-LED auf dem Management Modul permanent leuchtet

Jetzt ist der Switch erfolgreich mit den neuen IP-Parametern initialisiert worden und kann im endgültigen Subnetz unter der neuen IP-Adresse angesprochen werden.

Erst hier sollten die weiteren Einstellungen wie 'Name Setup', 'Port Setup', 'VLAN Setup' usw. durchgeführt werden.

6. Switch Konfiguration

6.1. Switch Konfiguration mittels Nexans Switch Manager (NEXMAN)

Der NEXMAN ist eine Windows Applikation, die auf Systemen mit Windows 7 oder höher lauffähig ist.

Eine Evaluation-Version des NEXMAN befindet sich auf unserer Support-Homepage:

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

Nach einer kurzen Registrierung kann der Manager heruntergeladen werden. Durch Aufnahme Ihrer Email-Adresse in den Newsletter für Softwareupdates, werden Ihnen Informationen über aktuelle Updates des Managers automatisch zugestellt.

6.1.1. Firmwarevoraussetzungen

Die Konfiguration mittels NEXMAN (Nexans Switch Manager) ist bei allen Firmwarefamilien möglich. Als Release Stand wird mindestens V3.01 vorausgesetzt.

HINWEIS:

Sollte auf dem Switch eine Firmware-Version V1.xx oder V2.xx installiert sein, so muss zunächst ein Update auf Firmware V3.xx oder höher durchgeführt werden. Dieses Update muss in jedem Fall mit dem NEXMAN durchgeführt werden.

6.1.2. Login

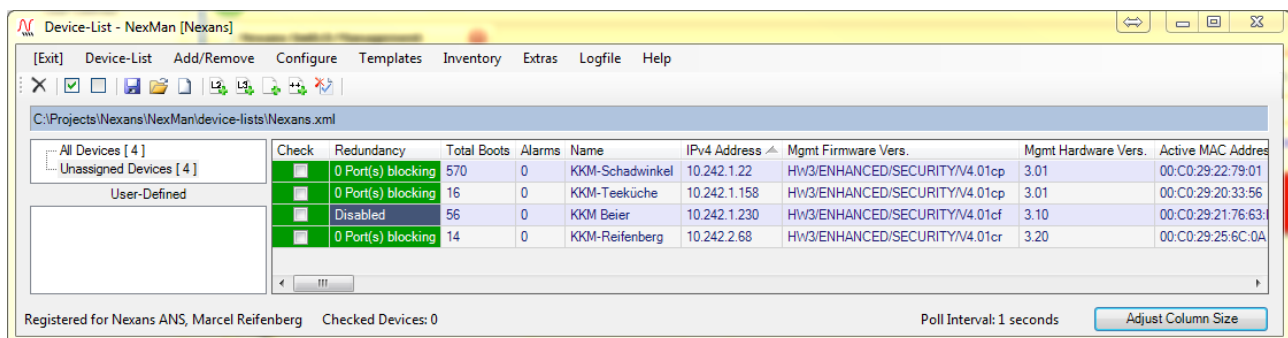
Für Authentifizierung des NEXMAN gegenüber dem Switch sind verschiedene Modi im Switch einstellbar. Per Factory-Default Einstellung wird SCP (Secure Copy) für das Schreiben und Lesen der Konfiguration. Die Factory-Default Einstellungen für Name und Passwort lauten: Name=admin, Passwort=nexans

Für eine detaillierte Erklärung der einzelnen Modi siehe Kapitel 10.10. Manager Authentication Mode

6.1.3. Konfiguration

Mit dem NEXMAN kann die Konfiguration des Switches heruntergeladen und archiviert werden. Ferner kann die Konfiguration geändert und auf einen einzelnen Switch oder auch auf eine ganze Liste von Switchen zurückgeladen werden.

Für detaillierte Informationen zur Konfiguration und zum Update mittels NEXMAN lesen Sie bitte das Handbuch zum NEXMAN.



6.2. Switch Konfiguration mittels Web-Browser (HTTP / HTTPS)

6.2.1. Authentifizierung / Login

WICHTIGER HINWEIS:

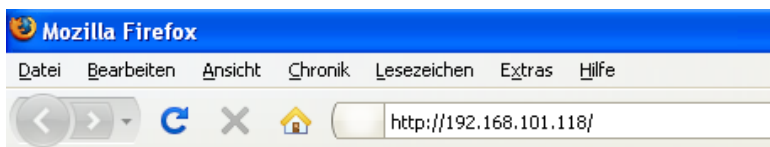
Das Web Interface kann für HTTP bzw. HTTPS separat abgeschaltet werden. In diesem Fall ist ein Zugriff per HTTP bzw. HTTPS nicht möglich.

Der HTTP Zugriff auf das Web-Modul ist mit jedem üblichen Web-Browser möglich. Voraussetzung ist, dass das Modul bereits mit einer IP-Adresse konfiguriert ist und die Netzwerkmaske und das Gateway beim Switch und PC korrekt eingestellt sind. Als einfacher Verbindungstest kann z.B. ein Ping-Befehl ausgeführt werden.

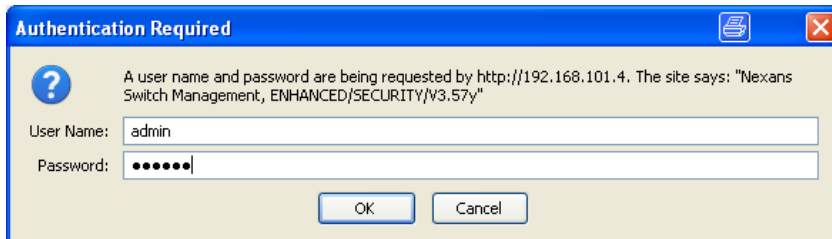
Beim Einsatz von HTTPS sind folgende Punkte zu beachten:

- Benötigt die Management Hardwareversion HW3 oder höher
- Auf den Switches ist ein von der Nexans Advanced Networking Solutions CA (Nexans-ANS CA) signiertes Zertifikat installiert (RSA, 1024 Bit Key, SHA-256).
- Das zur Signierung verwendete Nexans CA Zertifikat befindet sich zum Download auf unsere Support Homepage: <http://www.nexans-ans.de/support/>.
- Das Nexans-ANS CA Zertifikat kann in den verwendeten WEB-Browser als Stammzertifikat importiert werden um die Sicherheitswarnungen beim ersten Aufruf jedes Switches zu umgehen. Dabei ist jedoch zu beachten, dass der Aufruf des Switches nicht über die IP Adresse erfolgen darf (dies ist eine grundsätzliche Beschränkung des HTTPS Zertifikatkonzeptes), sondern über einen symbolischen Namen. Dieser Name muss dann entweder durch einen DNS-Server oder durch die hosts Datei in die entsprechende IP Adresse aufgelöst werden. Auf allen Nexans Switches ist ein identisches Zertifikat installiert, dass für den symbolischen Namen *.switch.nexans signiert wurde. Der * darf dabei durch einen beliebigen Switchnamen (der allerdings keinen '.' enthalten darf) ersetzt werden damit der Browser das Switch-Zertifikat als gültig ansieht.

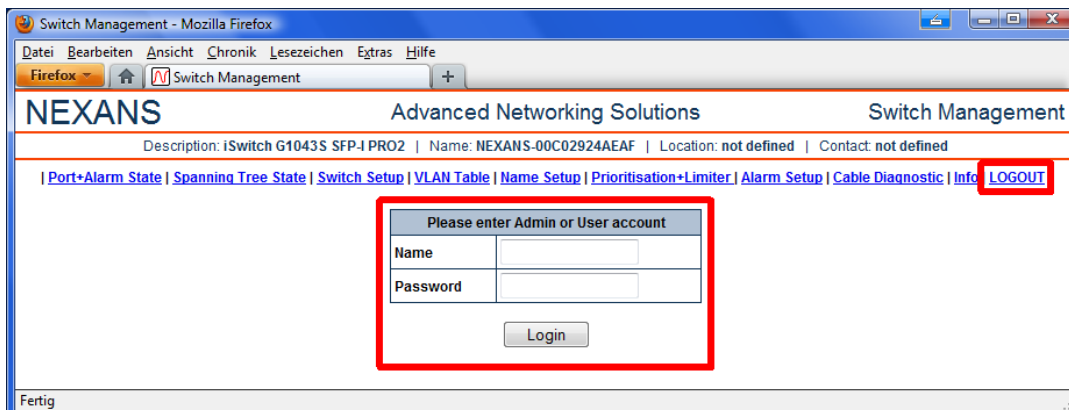
Nach Start des Web-Browsers muss in der Adresszeile des Web-Browsers die IP-Adresse bzw. der symbolische Name des Switches eingegeben werden:



Der Zugriff auf das Management Modul ist durch ein Passwort geschützt:



Ab Management Hardware Version HW3 erfolgt die Eingabe von Name und Passwort im Browser-Fenster:



Die Factory-Default Einstellungen für Name und Passwort lauten: Name=admin, Passwort=nexans

6.2.2. Konfiguration

Nach erfolgreichem Login kann nun über die Menü-Leiste auf die verschiedenen Funktionen des Switches zugegriffen werden:

Nexans Switch Management - Mozilla Firefox

http://192.168.101.118/

NEXANS Advanced Networking Solutions Switch Management

Description: iSwitch 741 G(SC) | Name: Nexans_00C029200088 | Location: not defined | Contact: not defined

[Port*Alarm State](#) | [RSTP State](#) | [Switch Setup](#) | [VLAN Table](#) | [Admin Account](#) | [User Account](#) | [Name Setup](#) | [Prioritisation*Limiter](#) | [Alarm Setup](#) | [Cable Diagnostic](#) | [Info](#)

Industrial Output / Input State

Alarm Output M1		No Alarm (Alarm contact closed)											
Alarm Output M2		No Alarm (Alarm contact closed)											
Port State													
Port No.	Port Descr.	Port Name	Link Type Port Type	Current Link State	Speed Duplex Setup	Autocross. Autopol. Setup	Error Counter	Security Mode [MAC Addr.](MAC State)	Security State [Failure MAC Address]	Active Default VLAN-ID	Active Voice VLAN-ID	Active Trunking Mode	Flow Control State
0	MGMT	-	Internal Management	-	-	-	-	-	-	1	-	-	-
1	TP-1	<none>	User TP 10/100 MBit	no link	Autoneg	ENABLED	0 All Counters	Disabled	Disabled	1	disabled	disabled	no link
2	TP-2	<none>	User TP 10/100 MBit	no link	Autoneg	ENABLED	0 All Counters	Disabled	Disabled	1	disabled	disabled	no link
3	TP-3	<none>	User TP 10/100 MBit	100fdx	Autoneg	ENABLED	0 All Counters	Disabled [More than 3 MAC's]	Disabled	1	disabled	disabled	ACTIVE
4	TP-4	<none>	User TP 10/100 MBit	no link	Autoneg	ENABLED	0 All Counters	Disabled	Disabled	1	disabled	disabled	no link
5	TP-5	<none>	User TP 10/100 MBit	no link	Autoneg	ENABLED	0 All Counters	Disabled	Disabled	1	disabled	disabled	no link
6	FO-6	<none>	Uplink/Downlink Fiber 100 MBit	no link	100fdx	-	0 All Counters	Disabled	Disabled	1	disabled	disabled	no link
7	TP-7	<none>	User TP 10/100 MBit	no link	Autoneg	ENABLED	0 All Counters	Disabled	Disabled	1	disabled	disabled	no link

Fertig

6.3. Switch Konfiguration mittels V.24 Console

Die Konfiguration mittels V.24 Console Interface wird von allen Industrie-Switchen, von Desk-Switchen vom Typ 'GigaSwitch' und von Kabelkanalmodulen vom Typ 'GigaSwitch V3' unterstützt.

Die V.24-Übertragungsparameter sind im Terminalprogramm des PC's wie folgt einzustellen:

- 9600 Bd
- 8 Datenbits
- 1 Stoppbit
- keine Parität
- Flusssteuerung Xon/Xoff oder Keine

6.3.1. Anschluss bei Switches mit RJ11-Buchse

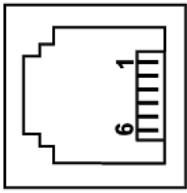
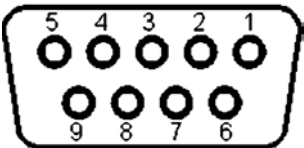
Als V.24 Anschluss ist auf der Frontseite der Switches eine RJ11-Buchse angebracht, die über ein spezielles RJ11/DSUB9-Adapterkabel mit der seriellen Schnittstelle des PC's verbunden werden muss:



Ein entsprechend konfektioniertes Adapterkabel kann als Zubehörartikel über Nexans bezogen werden (Nexans Artikel-Nr.: 88300688):



Die Belegung der RJ11-Buchse am Switch und der D-Sub-Buchse am Adapterkabel ist wie folgt:

RJ11-Buchse am Switch	9pol. D-Sub-Buchse am Adapterkabel	
		
Pin	Pin	Signalname
1	7	RTS
2	-	-
3	3	TxD
4	5	GND
5	2	RxD
6	8	CTS)
	1 4 6 HINWEIS: Diese drei Pins sind in der Buchse gebrückt.	DCD DTR DSR

6.3.2. Anschluss beim Industrie-Switch mit RJ45-Buchse

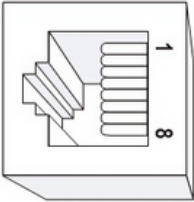
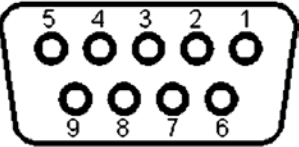
Als V.24 Anschluss ist auf der Frontseite der Industrieswitches eine RJ45-Buchse angebracht, die über ein spezielles RJ45/DSUB9-Adapterkabel mit der seriellen Schnittstelle des PC's verbunden werden muss:



Ein entsprechend konfektioniertes Adapterkabel kann als Zubehörartikel über Nexans bezogen werden (Nexans Artikel-Nr.: 88646169). HINWEIS: Dieses Kabel ist kompatibel mit Standard Cisco Consolen Kabeln (z.B. Cisco Artikel-Nr.: 72-3383-01):



Die Belegung der 8pol. RJ45-Buchse am Switch und der 9pol. D-Sub-Buchse am Adapterkabel ist wie folgt:

8 pol. RJ45-Buchse am Switch 	9pol. D-Sub-Buchse am Adapterkabel 	
Pin	Pin	Signalname
1	8	CTS
2 Dieser Pin ist im Switch mit Pin 7 gebrückt	6	DSR
3	2	RxD
4	5	GND
5		
6	3	TxD
7 Dieser Pin ist im Switch mit Pin 2 gebrückt	4	DTR
8	7	RTS

6.3.3. Anschluss beim GigaSwitch V3 und GigaSwitch 5xx Desk

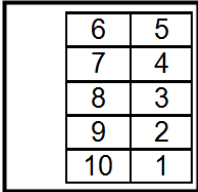
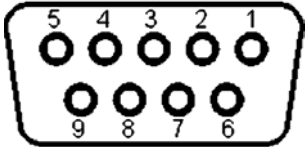
Der V.24 Anschluss beim GigaSwitch V3 Kabelkanal-Switch befindet sich unter dem LED-Einleger und beim GigaSwitch 5xx Desk auf der Bodenseite des Switches unterhalb der Abdeckung für die MC-Karte:



Die 10 polige Mini-Buchse muss dabei über ein spezielles aktives DSUB9-Adapterkabel mit der seriellen Schnittstelle des PC's verbunden werden. Ein entsprechendes Adapterkabel kann als Zubehörartikel über Nexans bezogen werden (Nexans Artikel-Nr.: 88300695):



Die Belegung der 10pol. Mini-Buchse und der 9pol. D-Sub-Buchse am Adapterkabel ist wie folgt:

10pol. Mini-Buchse	9pol. D-Sub-Buchse am Adapterkabel	
		
Pin	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 Diese drei Pins sind in der Buchse gebrückt.	DCD DTR DSR
	7 8 Diese beiden Pins sind in der Buchse gebrückt.	RTS CTS

6.3.4. Firmwarevoraussetzungen

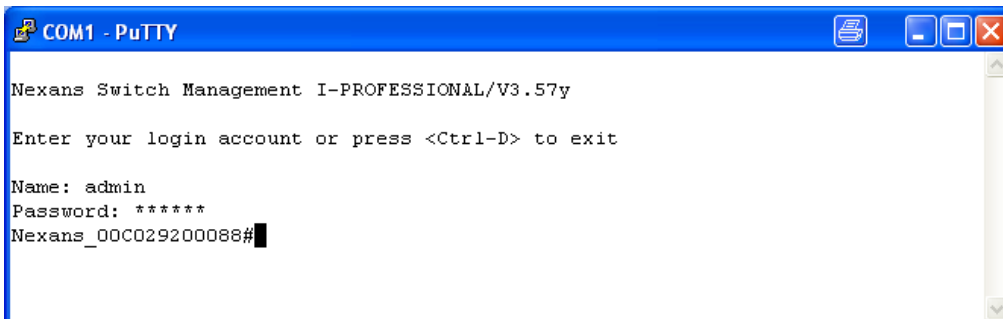
Als Firmware-Versionen wird die Release 3.10 oder höher vorausgesetzt.

6.3.5. Authentifizierung / Login

Der Switch kann über jede Standard V.24 Terminal-Applikation angesprochen werden.

Um Konflikte bei der Konfiguration zu vermeiden, darf jeweils nur eine Console Verbindung (Telnet bzw. V.24) offen sein, d.h., alle weiteren gleichzeitigen Verbindungsversuche werden vom Switch abgelehnt. Um ein blockieren der Console verhindern, wird die aktive Console Verbindung automatisch beendet, falls 15 Minuten keine Eingabe erfolgt.

Nach dem Start des Terminal-Programms mit zunächst durch drücken der <Enter> Taste der Login Modus aktiviert werden. Anschließend müssen der korrekte Login-Name und das zugehörige Passwort eingegeben werden:



Die Factory-Default Einstellungen für Name und Passwort lauten: Name=admin, Passwort=nexans
Für eine detaillierte Erklärung der V.24 Console Authentifizierung siehe Kapitel [10.14. V.24 Console Authentication Mode](#) bzw. [10.56.RADIUS Console Authentication Modes](#).

6.3.6. Konfiguration

Nach erfolgreichem Login meldet sich der Switch mit seinem Eingabe-Prompt. Abhängig vom Access-Level wird als Prompt '#' (Admin-Level) oder '>' (User-Level) ausgegeben.

Der im Bild oben vor dem Prompt angezeigte Name 'Nexans-00C029200088' ist der Name des Switches und ist per Factory Default auf 'Nexans-xxxxxxxxxx' eingestellt, wobei xxxxxxxxxxxx durch die MAC-Adresse ersetzt wird.

Durch das Console Kommando 'set n:ame [<string 1...50 chars>]' kann dieser geändert werden. Er ist außerdem identisch mit der SNMP-Variablen 'sysName' in der MIB-II system-group und kann auch per SNMP verändert werden.

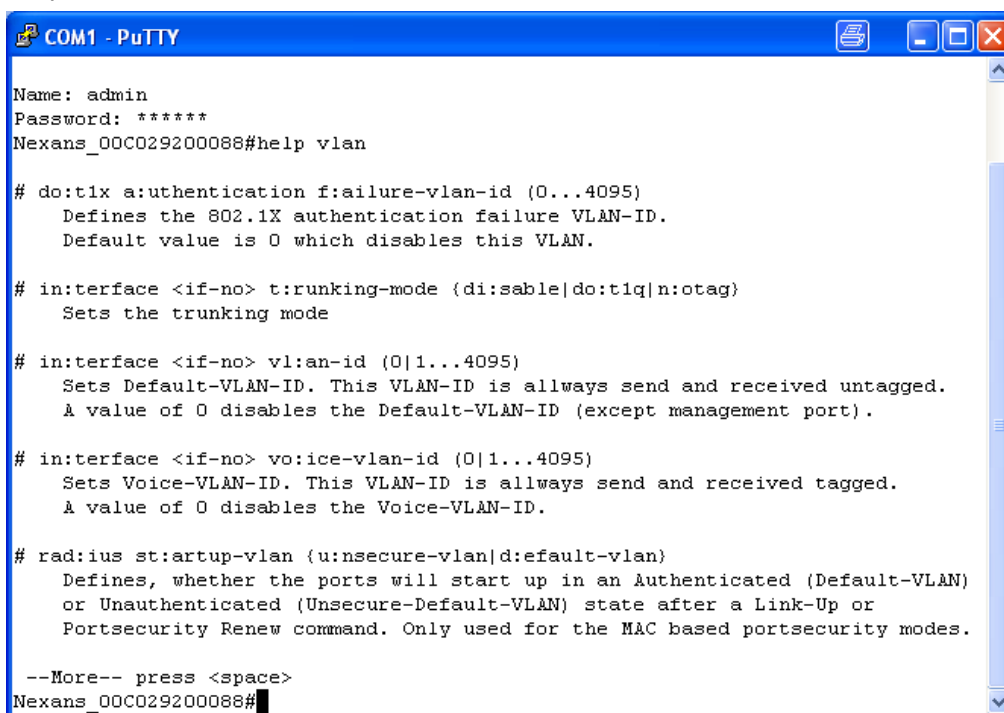
Der Switch unterstützt einen History-Buffer, der die letzten zehn eingegeben Kommandos speichert. Mit den Tasten '↑' bzw. '↓' kann durch den Buffer gescrollt werden.

Mit dem Console Kommando 'help' oder '?' kann eine Übersicht aller gültigen Console Kommandos angezeigt werden. Für die Suche nach einem bestimmten Kommando können bis zu zwei Stichworte angegeben werden.

Die Syntax lautet wie folgt:

h:elp [<search-string>] [<search-string>]

Beispiel:



```
COM1 - PuTTY

Name: admin
Password: *****
Nexans_00C029200088#help vlan

# do:tlx a:uthentication f:ailure-vlan-id (0...4095)
  Defines the 802.1X authentication failure VLAN-ID.
  Default value is 0 which disables this VLAN.

# in:terface <if-no> t:runking-mode (di:sable|do:tlq|n:otag)
  Sets the trunking mode

# in:terface <if-no> vl:an-id (0|1...4095)
  Sets Default-VLAN-ID. This VLAN-ID is allways send and received untagged.
  A value of 0 disables the Default-VLAN-ID (except management port).

# in:terface <if-no> vo:ice-vlan-id (0|1...4095)
  Sets Voice-VLAN-ID. This VLAN-ID is allways send and received tagged.
  A value of 0 disables the Voice-VLAN-ID.

# rad:ius st:artup-vlan (u:nsecure-vlan|d:efault-vlan)
  Defines, whether the ports will start up in an Authenticated (Default-VLAN)
  or Unauthenticated (Unsecure-Default-VLAN) state after a Link-Up or
  Portsecurity Renew command. Only used for the MAC based portsecurity modes.

--More-- press <space>
Nexans_00C029200088#
```

Für eine Übersicht aller Switchparameter mit den jeweils zugehörigen Console Kommandos siehe Kapitel 9. Liste der Status- und Konfigurationsparameter.

6.4. Switch Konfiguration mittels Telnet bzw. SSH Console

6.4.1. Authentifizierung / Login

Der Switch kann über jede Standard Telnet- bzw. SSHv2-Client angesprochen werden. Voraussetzung ist, dass das Modul bereits mit einer IP-Adresse konfiguriert ist und die Netzwerkmaske und das Gateway beim Switch und PC korrekt eingestellt sind. Als einfacher Verbindungstest kann z.B. ein Ping-Request ausgeführt werden.

HINWEIS: Alle Parameter des Switches können ausnahmslos per Console konfiguriert werden.

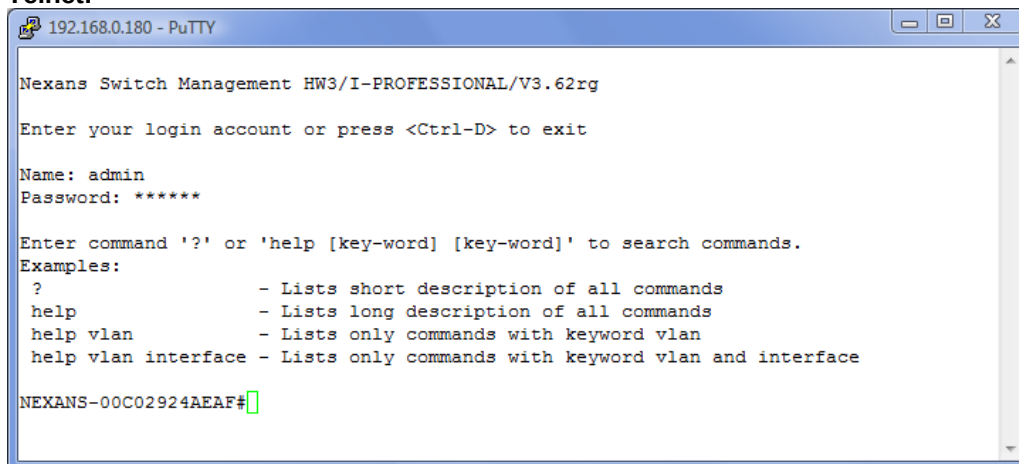
Beim Einsatz von SSH sind folgende Punkte zu beachten:

- benötigt die Management Hardwareversion HW3 oder höher
- ausschließliche Unterstützung von SSH Version 2
- im Auslieferungszustand ist bereits ein individuell generiertes 1024 Bit RSA-Key-Paar vorinstalliert
- es werden ausschließlich 1024 Bit RSA-Keys unterstützt
- ein neues RSA-Key-Paar kann per CLI Reboot-Kommando "reload new-rsa-key" generiert werden
- nach Rücksetzen auf Factory Default Einstellungen wird ein neues RSA-Key-Paar automatisch generiert
- für die Data-Encryption werden Algorithmen mit bis zu 256Bit (AES-256) unterstützt
- der Public Teil des Key-Paares kann z.Z. nicht angezeigt werden
- das öffnen mehrerer SSH, Telnet bzw. V.24 Console Sessions ist aus Sicherheitsgründen nicht möglich

Um Konflikte bei der Konfiguration zu vermeiden, darf jeweils nur eine Console Verbindung (Telnet, SSH bzw. V.24) offen sein, d.h., alle weiteren gleichzeitigen Verbindungsversuche werden vom Switch abgelehnt. Um ein blockieren der Console verhindern, wird die aktive Console Verbindung automatisch beendet, falls 15 Minuten keine Eingabe erfolgt.

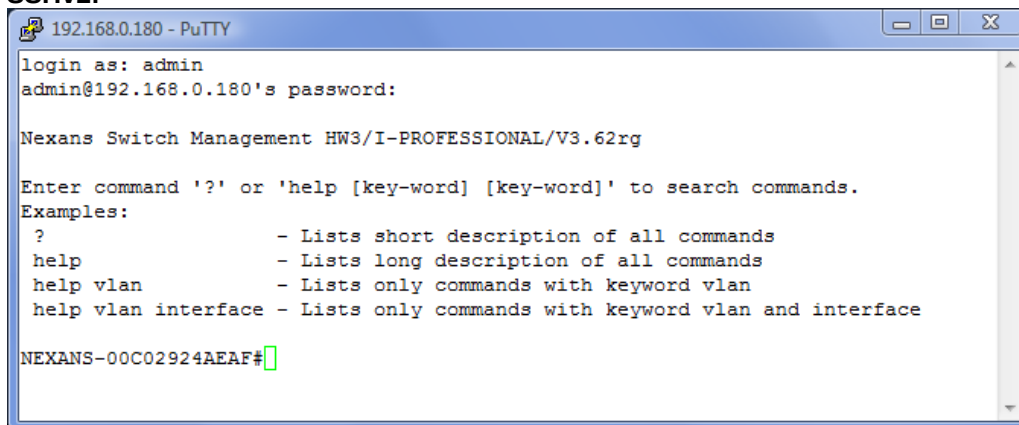
Nach dem Start des Telnet- bzw. SSHv2 Clients mit der IP-Adresse des Management Moduls, muss zunächst der korrekte Login-Name und das zugehörige Passwort eingegeben werden:

Telnet:



```
192.168.0.180 - PuTTY
Nexans Switch Management HW3/I-PROFESSIONAL/V3.62rg
Enter your login account or press <Ctrl-D> to exit
Name: admin
Password: *****
Enter command '?' or 'help [key-word] [key-word]' to search commands.
Examples:
?                - Lists short description of all commands
help             - Lists long description of all commands
help vlan       - Lists only commands with keyword vlan
help vlan interface - Lists only commands with keyword vlan and interface
NEXANS-00C02924AEAF#
```

SSHv2:



```
192.168.0.180 - PuTTY
login as: admin
admin@192.168.0.180's password:
Nexans Switch Management HW3/I-PROFESSIONAL/V3.62rg
Enter command '?' or 'help [key-word] [key-word]' to search commands.
Examples:
?                - Lists short description of all commands
help             - Lists long description of all commands
help vlan       - Lists only commands with keyword vlan
help vlan interface - Lists only commands with keyword vlan and interface
NEXANS-00C02924AEAF#
```

Die Factory-Default Einstellungen für Name und Passwort lauten: Name=admin, Passwort=nexans

Für eine detaillierte Erklärung der Telnet/SSH Authentifizierung siehe Kapitel [10.48 Telnet Console Authentication Mode](#), [10.49 SSHv2 Console Authentication Mode](#), [10.56. RADIUS Console Authentication Modes](#) bzw. [10.64 TACACS+ Console Authentication Modes](#).

6.4.2. Konfiguration

Nach erfolgreichem Login meldet sich der Switch mit einigen Hinweisen zur Hilfefunktion und anschließend mit seinem Eingabe-Prompt. Abhängig vom Access-Level wird als Prompt '#' (Admin-Level) oder '>' (User-Level) ausgegeben.

Der im Bild oben vor dem Prompt angezeigte Name 'Nexans-00C029200088' ist der Name des Switches und ist per Factory Default auf 'Nexans-xxxxxxxxxx' eingestellt, wobei xxxxxxxxxxxx durch die MAC-Adresse ersetzt wird.

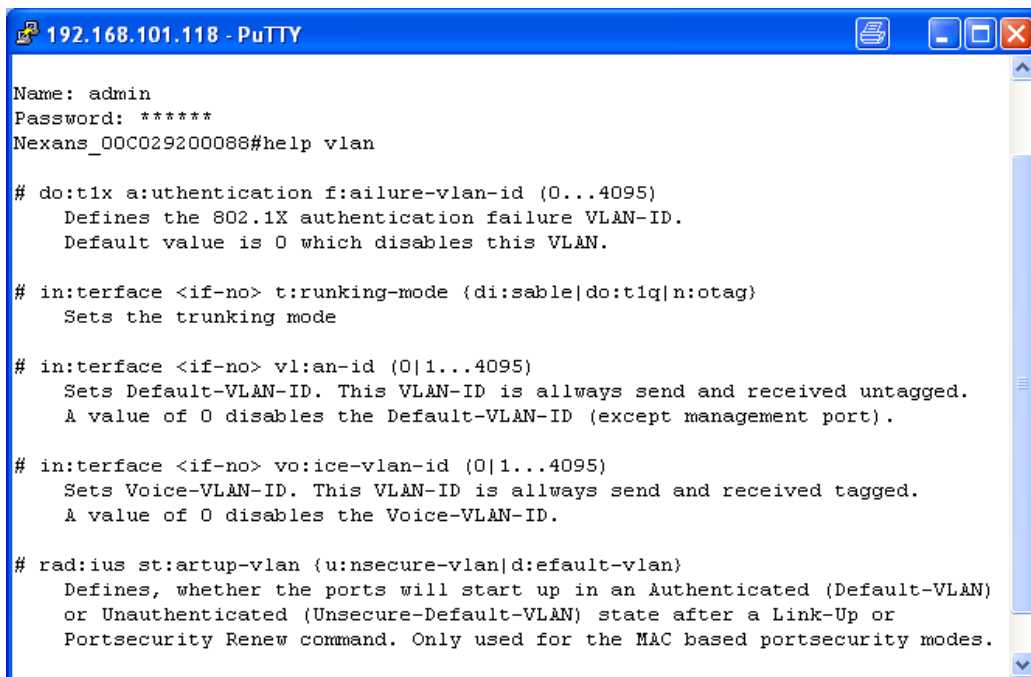
Durch das Console Kommando 'set n:ame [<string 1...50 chars>]' kann dieser geändert werden. Er ist außerdem identisch mit der SNMP-Variablen 'sysName' in der MIB-II system-group und kann auch per SNMP verändert werden.

Der Switch unterstützt einen History-Buffer, der die letzten zehn eingegeben Kommandos speichert. Mit den Tasten '↑' bzw. '↓' kann durch den Buffer gescrollt werden.

Mit dem Console Kommando 'help' oder '?' kann eine Übersicht aller gültigen Console Kommandos angezeigt werden. Für die Suche nach einem bestimmten Kommando können bis zu zwei Stichworte angegeben werden. Die Syntax lautet wie folgt:

h:elp [<search-string>] [<search-string>]

Beispiel:



```
192.168.101.118 - PuTTY
Name: admin
Password: *****
Nexans_00C029200088#help vlan

# do:tlx a:uthentication f:ailure-vlan-id (0...4095)
  Defines the 802.1X authentication failure VLAN-ID.
  Default value is 0 which disables this VLAN.

# in:terface <if-no> t:runking-mode {di:sable|do:tlq|n:otag}
  Sets the trunking mode

# in:terface <if-no> vl:an-id (0|1...4095)
  Sets Default-VLAN-ID. This VLAN-ID is always send and received untagged.
  A value of 0 disables the Default-VLAN-ID (except management port).

# in:terface <if-no> vo:ice-vlan-id (0|1...4095)
  Sets Voice-VLAN-ID. This VLAN-ID is always send and received tagged.
  A value of 0 disables the Voice-VLAN-ID.

# rad:ius st:artup-vlan {u:nsecure-vlan|d:efault-vlan}
  Defines, whether the ports will start up in an Authenticated (Default-VLAN)
  or Unauthenticated (Unsecure-Default-VLAN) state after a Link-Up or
  Portsecurity Renew command. Only used for the MAC based portsecurity modes.
```

Für eine Übersicht aller Switchparameter mit den jeweils zugehörigen Console Kommandos siehe Kapitel [9.Liste der Status- und Konfigurationsparameter](#).

6.5. Switch Konfiguration mittels SNMP

6.5.1. Authentifizierung / Communities

Der Zugriff mittels SNMP kann mit jedem Standard SNMP-Manager erfolgen.

Die SNMPv1/v2c Communities bzw. der SNMPv3 Username und das Passwort werden entsprechend ausgewertet und müssen beim SNMP-Manager korrekt eingestellt sein.

Für detaillierte Erläuterungen zu SNMP siehe Kapitel 10.53. SNMP Unterstützung.

6.5.2. Konfiguration

Die aktuell vom Switch unterstützen SNMP MIBs können dem Kapitel 10.53.7. SNMP MIB Übersicht entnommen werden.

Für eine Übersicht aller Switchparameter mit den jeweils zugehörigen SNMP Variablen siehe Kapitel 9. Liste der Status- und Konfigurationsparameter.

Die zur Management Integration erforderlichen Nexans Private-MIBs kann über das Supportportal www.nexans-ans.de/support heruntergeladen werden.

7. Firmware-Update und Switch-Konfiguration

7.1. Firmware-Update

Für ein Firmware-Update bzw. –Upgrade wird eine entsprechende Firmware-Datei mit der neuen Release benötigt. Die aktuelle Release kann über das Supportportal von 'Advanced Networking Solutions', Internet Homepage www.nexans-ans.de/support nach einer kurzen Registrierung heruntergeladen werden. Durch Aufnahme Ihrer Email-Adresse in den Newsletter für Softwareupdates werden Ihnen Informationen über aktuelle Updates der Firmware automatisch zugestellt.

HINWEIS:

Durch das Update bzw. Upgrade werden alle Konfigurationseinstellungen des Switches unverändert übernommen. Lediglich für neu hinzugekommene Einstellungen werden die Factory-Default Einstellungen eingesetzt.

7.1.1. Duale Firmware-Speicherung

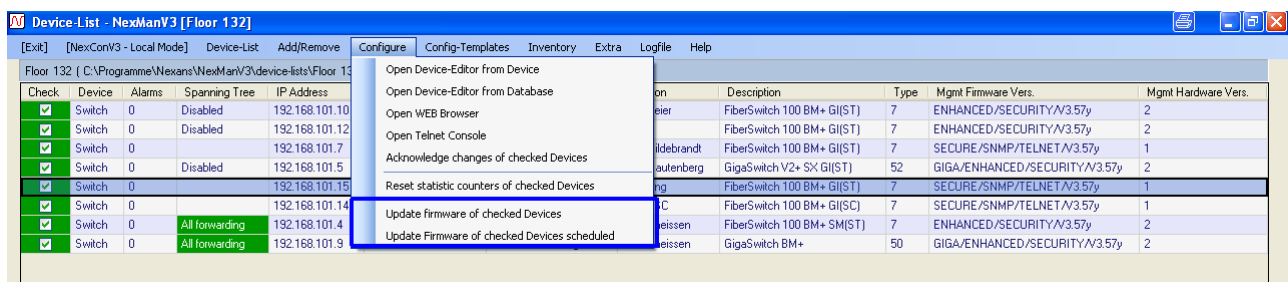
Auf HW5-Switchen werden zwei Firmware-Versionen parallel auf verschiedenen Boot-Partitionen gespeichert. Wenn ein Firmware-Update installiert wird, wird die aktuell ausgeführte Firmware als Backup gesichert und die installierte Firmware wird zur neuen ausgeführten Firmware. Falls die neu ausgeführte Firmware instabil oder beschädigt ist, wird die Backup-Firmware von der anderen Boot-Partition gestartet und die Backup-Firmware wird wieder zur ausgeführten Firmware.

Bei Bedarf können Sie die Backup-Firmware-Version in CLI und Manager manuell neu laden (siehe Kapitel *9.12 Management > Agent*).

7.1.2. Firmware-Update per Nexans Switch Manager (NEXMAN) ausführen

Mit dem NEXMAN kann ein automatisches Firmware-Update eines einzelnen Switches oder einer ganzen Liste von Switchen erfolgen. Der NEXMAN ist eine Windows Applikation, die auf Systemen mit W7 oder höher lauffähig ist.

Für detailliertere Informationen zum Update per NEXMAN lesen Sie bitte das entsprechende Handbuch des NEXMAN.



Die Hauptmerkmale des NEXMAN sind:

- Automatische Layer 2 und Layer 3 Suchfunktion nach aktiven Switchen
- Erweiterte Geräteliste mit individuellen Sortierparameter wie z.B. IP– oder MAC Adresse, Gerätenamen, etc.
- Freiwählbare Kategorien in Baumstruktur
- Farblich Kennzeichnung der Kategorie und des Switches bei eingehendem Alarm
- Komfortable Benutzer Verwaltung mit unterschiedlichen Zugriffsberechtigungen und benutzerspezifischer Geräteliste
- Online Ferndiagnose der SFP Parameter wie z.B. Rx/Tx Leistung, Wärme, etc
- Zeitgesteuertes Firmware Update von ausgewählten Switchen
- Master Konfiguration mit individuell wählbaren Parametern
- Erzeugen von beliebig vielen Master Konfigurationen für ein oder mehrere Switches
- Speichern der Gerätekonfiguration in einer Datenbank auf dem PC oder einem zentralen Server
- Speichern von alten Gerätekonfigurationen via History Funktion in der Datenbank
- Umfassende Import und Export Funktionen
- Umfassende Informationen im System Log für spätere Analyse

7.1.3. Firmware-Update per Telnet/SSH/V.24 Console ausführen

HINWEIS: Diese Funktion benötigt die Management Hardwareversion HW2 oder höher.

Das Laden einer neuen Firmware ist per TFTP-Kommando aus der Telnet-, SSH bzw. V.24-Console möglich.

Für diese Funktion wird allerdings ein externer TFTP-Server benötigt, der die Firmwaredatei zur Verfügung stellt. Der Switch selber fungiert dabei als TFTP-Client. Zum Ausführen des entsprechenden Kommandos muss man sich zuvor mit dem Admin Account auf der Console einloggen.

Die Befehlssyntax lautet dabei wie folgt:

```
tftp <ip-address> get <path> {<filename>.img|bin}
```

Parameter:

<ip-address>	IP Adresse des externen TFTP Servers
<path>	Pfad auf dem TFTP Server, z.B. '/' oder '/nexans-fw/iswitch/'
<filename>.IMG BIN	Name der Firmwaredatei, z.B. 'i-prof-hw2-355.img'

Die Zeichenlängen der Parameter <path> und <filename.xxx> dürfen jeweils 25 Zeichen nicht überschreiten. Dies ist eine Limitierung des Console Kommando Interpreters.

Vor dem Update mit der angegebenen Firmwaredatei, wird zunächst der Header der Datei gelesen und überprüft, ob das Image für den Switch geeignet ist. Fall nein, wird eine entsprechende Fehlermeldung an der Konsole ausgegeben und das weitere Update abgebrochen.

Wenn das Image passend für den Switchtyp und das Management Modul ist, wird die Konsole Session automatisch geschlossen und der Rest der Firmwaredatei per TFTP gelesen. Nachdem die Datei erfolgreich übertragen wurde, programmiert sich das Management Modul automatisch mit der neuen Firmware und führt nach ca. 5 Sekunden einen Reboot aus.

Ein Start des Updates per Console sieht dann wie folgt aus:

```

192.168.101.165 - PuTTY
Nexans Switch Management I-PROFESSIONAL/V3.57y
Enter your login account or press <Ctrl-D> to exit
Name: admin
Password: *****
Nexans_00C029200085#tftp 10.242.6.26 get \ i-prof-hw2-357u.img
%TFTP: Try receiving file \i-prof-hw2-357u.img from IP 10.242.6.26
%TFTP: Requesting file. Please wait ...
%Info: Firmwareupdate in progress...
%Info: Session automatically logged off ...
  
```

7.1.4. Firmware-Update automatisch per DHCP/BootP ausführen

HINWEIS: Diese Funktion benötigt die Management Hardwareversion HW2 oder höher.

Voraussetzung für das automatische Update der Firmware per DHCP/BootP ist das Laden einer Switch-Konfiguration als Kommando-Datei per DHCP/BootP. Bitte lesen Sie hierzu zunächst das Kapitel [7.2.5 Switch-Konfiguration automatisch per DHCP/BootP und TFTP laden](#).

In der per DHCP/BOOTP geladenen Kommando-Datei sollte als erstes Kommando der Update Befehl mit folgender Syntax stehen:

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

Parameter:

<version-number>	Versionsnummer ohne Punkt	z.B. '356' für Version 3.56
<path>	Relativer Pfad auf dem TFTP Server	z.B. '/' oder '/nexans-fw/iswitch/'
<filename>.img bin	Name der Firmwaredatei	z.B. 'i-prof-hw2-355.img'
<hw-version>	Optional: Management Hardwareversion	z.B. '2'

Die Zeichenlängen der Parameter <path> und <filename.xxx> dürfen jeweils 25 Zeichen nicht überschreiten. Dies ist eine Limitierung des Console Kommando Interpreters.

Beim Kommando **check-min-fw** wird das Update mit der angegebenen Firmwaredatei durchgeführt, wenn die auf dem Switch aktuell laufende Firmware-Version kleiner als die im Kommando angegebene <version-number> ist. Ist die installierte Version gleich oder höher als die angegebene, so wird das Kommando ignoriert.

Beim Kommando **check-this-fw** wird das Update mit der angegebenen Firmwaredatei durchgeführt, wenn die auf dem Switch aktuell laufende Firmware-Version kleiner oder größer als die im Kommando

angegebene <version-number> ist. Nur wenn die installierte Version identisch zur angegebenen Version ist, wird das Kommando ignoriert.

Der optionale Parameter [<hw-version>] bestimmt, für welche Hardwareversion des Management-Moduls die angegebene Firmware geladen werden soll. Stimmt die angegebene Version nicht mit der tatsächlichen Version des Management Moduls überein, so wird die Zeile ignoriert. Dies ist z.B. dann sinnvoll, wenn man dieselbe Kommando-Datei für Switches mit unterschiedlichen Management Hardwareversionen verwenden möchte und dieses jeweils unterschiedliche Firmware-Versionen benötigen. Für jede Hardwareversion wird dann eine Zeile mit der entsprechenden Firmware-Version in die Kommando-Datei aufgenommen.

WICHTIG: Die <version-number> muss im <filename> enthalten sein (z.B. <version-number> = 359 und <filename> = secu-hw2-359). Ansonsten wird die Zeile ignoriert.

Vor dem Update mit der angegebenen Firmwaredatei, wird zunächst der Header der Datei gelesen und überprüft, ob das Image für den Switch geeignet ist. Fall nein, wird das weitere Update abgebrochen und die restlichen Befehle in der geladenen Kommando-Datei ausgeführt.

Wenn das Image passend für den Switchtyp und das Management Modul ist, wird der Rest der Firmwaredatei per TFTP gelesen. Nachdem die Datei erfolgreich übertragen wurde, programmiert sich das Management Modul automatisch mit der neuen Firmware und führt nach ca. 5 Sekunden einen Reboot aus.

7.1.5. Firmware-Update per PC Console und SCP

HINWEIS: Diese Funktion benötigt die Management Hardwareversion HW3 oder höher.

Das Firmware-Image muss mittels Secure Copy (SCP) Protokoll zum Switch gesendet werden. Eine Verwendung von Secure FTP (SFTP) ist nicht möglich. Unter Windows kann hierzu z.B. das Programm „pscp.exe“ verwendet werden, das im Paket des SSH/Telnet Client „PuTTY“ enthalten ist (siehe <http://www.putty.org>). Bei Linux Betriebssystemen steht hierfür der Standardbefehl „scp“ zur Verfügung.

Für die Übertragung der Firmware mit sofortiger Ausführung des Updates gilt folgende Syntax:

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

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

Für die Übertragung der Firmware mit zeitgesteuertem Update via SNTP Server gilt folgende Syntax:

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

HINWEIS: Das zeitgesteuerte Update wird nur ausgeführt, wenn der Switch eine gültige Zeit vom Timeserver empfangen hat.

Nachdem das Firmware-Image erfolgreich übertragen wurde und das Update sofort bzw. zeitgesteuert ausgeführt wurde, wird automatisch nach ca. 5 Sekunden ein Reboot ausgeführt.

7.1.6. Firmware-Update per PC Console und TFTP

Ein manuelles Update der Firmware per PC Console ist nur möglich, wenn der 'Manager Authentication Mode' im Switch auf {none} eingestellt ist oder zuvor eine Authentifizierung per SNMP durchgeführt wurde (siehe Kapitel [7.5 TFTP Authentifizierung per SNMP](#)).

Voraussetzung für das Update ist, dass das Modul bereits mit einer IP-Adresse konfiguriert ist und die Netzwerkmaske und das Gateway beim Switch und PC korrekt eingestellt sind. Als einfacher Verbindungstest kann z.B. ein Ping-Request ausgeführt werden.

Das Firmware-Image muss nun mittels TFTP zum Management Modul gesendet werden. Hierzu kann z.B. das bei Windows NT/2000/XP mitgelieferte TFTP-Programm verwendet werden. Abhängig von der Dateierweiterung der Image-Datei ist die Befehlssyntax wie folgt:

- <name>.bin

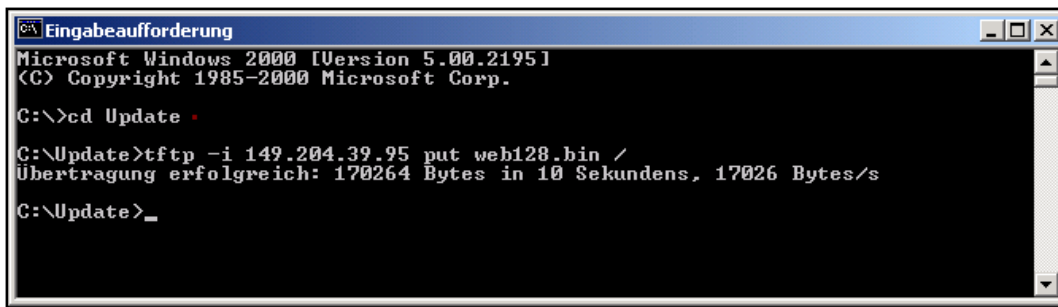
```
tftp -i <IP-Adresse> put <image.bin> /
```

- <name>.img

```
tftp -i <IP-Adresse> put <image.img> /img
```

Beispiel:

Für einen Switch mit der IP-Adresse 149.204.39.95 und der Update-Datei 'c:\update\web128.bin' sieht ein erfolgreiches Update wie folgt aus:



```
Eingabeaufforderung
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>cd Update

C:\Update>tftp -i 149.204.39.95 put web128.bin /
Übertragung erfolgreich: 170264 Bytes in 10 Sekunden, 17026 Bytes/s

C:\Update>_
```

Nachdem die Datei erfolgreich übertragen wurde, programmiert sich das Management Modul automatisch mit der neuen Firmware und führt nach ca. 5 Sekunden einen Reboot aus.

ACHTUNG:

Es wird empfohlen für das Update den *Nexans Switch Manager* (NEXMAN) zu verwenden, da dieser alle Funktionen automatisch ausführt und somit Fehler beim Update ausschließt.

7.2. Switch-Konfiguration verwalten

7.2.1. Dateiformate der Switch-Konfiguration

Grundsätzlich werden zwei verschiedene Dateiformate für die Verarbeitung der Switch-Konfiguration unterstützt:

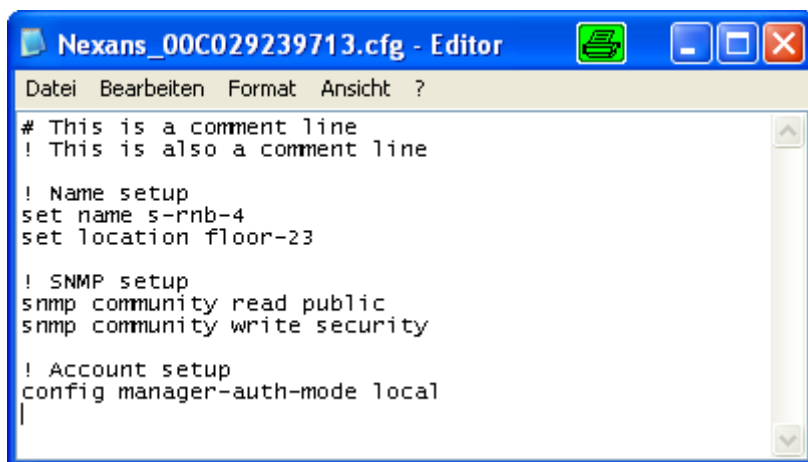
- **Binär-Format (.dat)**

Endet der Dateiname mit der Extension '.dat', so wird die Datei als Binärdatei interpretiert. Der Nexans Switch Manager (NEXMAN) verwendet ausschließlich dieses Dateiformat, da darüber eine sehr schnelles und effizientes Lesen und Schreiben der Switch-Konfiguration möglich ist.

- **Kommando-Format (.cfg)**

Eine Konfigurationsdatei im Kommando-Format beinhaltet eine Abfolge von Telnet/SSH/V.24 Kommandos und muss die Extension '.cfg' besitzen. Dabei sind die Dateiformate PC, UNIX und MAC zulässig.

Hier ein Beispiel für den Inhalt einer solchen Datei:



HINWEIS: Kommentarzeilen müssen mit '#' oder '!' beginnen.

7.2.2. Switch-Konfiguration per NEXMAN verwalten

Das Verwalten der Switch-Konfigurationen kann sehr komfortabel über den Nexans Switch Manager (NEXMAN) erfolgen. Über die Historyfunktion des NEXMAN können dabei auch ältere Konfigurationen in den Device-Editor geladen und in den Switch zurückgeschrieben werden. Die Konfigurationsdateien werden vom NEXMAN im sogenannten 'Database folder' abgelegt. Für jeden Switch wird dabei eine Datei mit dem Namen a_b_c_d.dat angelegt (a_b_c_d ist dabei die IP Adresse a.b.c.d des Switches). Innerhalb dieses Verzeichnisses wird ein weiteres Verzeichnis mit der Bezeichnung 'history' angelegt, das die archivierten Historykonfigurationen enthält.

Das Lesen und Schreiben der Konfiguration per NEXMAN erfolgt primär im Binär-Format. Der Switch arbeitet dabei als TFTP-oder SCP-Server und benötigt eine entsprechende Authentifizierung um das Update durchführen zu können.

Im Falle von TFTP wird die Authentifizierung über ein proprietäres Protokoll mittels UDP Port 50266 durchgeführt. Diese TFTP Authentifizierung ist allerdings im Auslieferungszustand deaktiviert und lässt daher jeden TFTP Transfer zu (siehe Kapitel [10.10. Manager Authentication Mode](#)).

Bei SCP ist die Authentifizierung integraler Bestandteil des Protokolls und erfordert daher keine zusätzliche Verwendung des UDP Ports 50266.

7.2.3. Switch-Konfiguration per Telnet/SSH/V.24 Console und TFTP sichern

HINWEIS: Diese Funktion benötigt die Management Hardwareversion HW2 oder höher.

Das Sichern der Switch-Konfiguration im Kommando-Format ist per TFTP-Kommando aus der Telnet-, SSH- bzw. V.24-Console möglich. Für diese Funktion wird ein externer TFTP-Server benötigt, der die Konfigurationsdatei entgegennimmt. Der Switch selber fungiert dabei als TFTP-Client. Zum Ausführen des entsprechenden Kommandos muss man sich zuvor mit dem Admin Account auf der Console einloggen.

Die Befehlssyntax lautet dabei wie folgt:

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

Parameter:

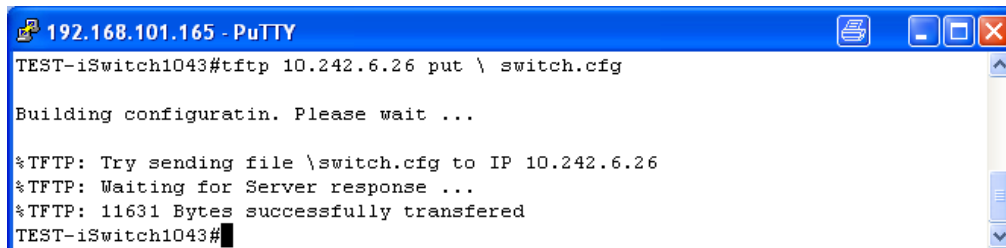
<ip-address>	IP Adresse des externen TFTP Servers
<path>	Relativer Pfad auf dem TFTP Server, z.B. '/' oder '/nexans-cfg/iswitch/'
<filename>.cfg	Name der Kommando-Datei mit Ext. ".cfg", z.B. 'Nexans-00c029245634.cfg'
!\$ip\$.cfg	Platzhalter für die IP- Adresse des Switches
!\$name\$.cfg	Platzhalter für den Name des Switches
all	Optionaler Parameter: siehe unten

Ohne Angabe des optionalen Parameters "all" werden nur solche Einstellungen gesichert, die vom Factory-Default abweichen. Mit Angabe des Parameters "all" werden alle Konfigurationseinstellungen gesichert, auch solche, die auf Factory-Default eingestellt sind.

Die Zeichenlängen der Parameter <path> und <filename.xxx> dürfen jeweils 25 Zeichen nicht überschreiten. Dies ist eine Limitierung des Console Kommando Interpreters.

Nach Absenden des Kommandos wird zunächst die Konfigurationsdatei im Speicher erstellt (identisch zum Kommando 'show running-config') und anschließend per TFTP versendet.

Ein erfolgreicher Sicherungsvorgang per Console sieht dann wie folgt aus:



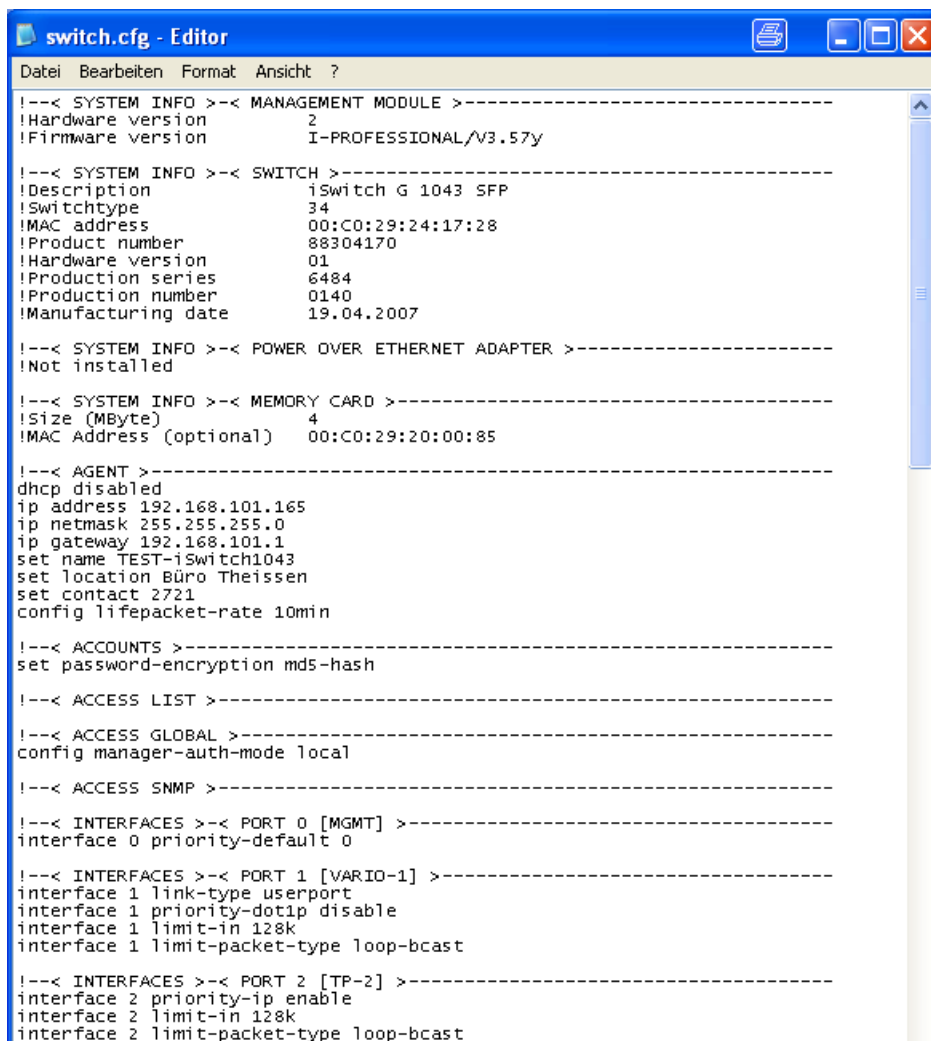
```

192.168.101.165 - PuTTY
TEST-iSwitch1043#tftp 10.242.6.26 put \ switch.cfg

Building configuratin. Please wait ...

%TFTP: Try sending file \switch.cfg to IP 10.242.6.26
%TFTP: Waiting for Server response ...
%TFTP: 11631 Bytes successfully transfered
TEST-iSwitch1043#
  
```

Hier ein Beispielauszug mit dem Inhalt einer solchen Datei:



```

switch.cfg - Editor
Datei Bearbeiten Format Ansicht ?

!---< SYSTEM INFO >--< MANAGEMENT MODULE >-----
!Hardware version      2
!Firmware version      I-PROFESSIONAL/V3.57y

!---< SYSTEM INFO >--< SWITCH >-----
!Description           iSwitch G 1043 SFP
!Switchtype            34
!MAC address           00:C0:29:24:17:28
!Product number        88304170
!Hardware version       01
!Production series      6484
!Production number      0140
!Manufacturing date     19.04.2007

!---< SYSTEM INFO >--< POWER OVER ETHERNET ADAPTER >-----
!Not installed

!---< SYSTEM INFO >--< MEMORY CARD >-----
!Size (MByte)          4
!MAC Address (optional) 00:C0:29:20:00:85

!---< AGENT >-----
dhcp disabled
ip address 192.168.101.165
ip netmask 255.255.255.0
ip gateway 192.168.101.1
set name TEST-iSwitch1043
set location Büro Theissen
set contact 2721
config lifepacket-rate 10min

!---< ACCOUNTS >-----
set password-encryption md5-hash

!---< ACCESS LIST >-----

!---< ACCESS GLOBAL >-----
config manager-auth-mode local

!---< ACCESS SNMP >-----

!---< INTERFACES >--< PORT 0 [MGMT] >-----
interface 0 priority-default 0

!---< INTERFACES >--< PORT 1 [VARIO-1] >-----
interface 1 link-type userport
interface 1 priority-dot1p disable
interface 1 limit-in 128k
interface 1 limit-packet-type loop-bcast

!---< INTERFACES >--< PORT 2 [TP-2] >-----
interface 2 priority-ip enable
interface 2 limit-in 128k
interface 2 limit-packet-type loop-bcast
  
```

7.2.4. Switch-Konfiguration per Telnet/SSH/V.24 Console und TFTP laden

HINWEIS:

Diese Funktion benötigt die Management Hardwareversion HW2 oder höher.

Das Laden der Switch-Konfiguration ist per TFTP-Kommando aus der Telnet-, SSH- bzw. V.24-Console möglich. Für diese Funktion wird ein externer TFTP-Server benötigt, der die Konfigurationsdateien zur Verfügung stellt. Der Switch selber fungiert dabei als TFTP-Client. Zum Ausführen des entsprechenden Kommandos muss man sich zuvor mit dem Admin Account auf der Console einloggen.

7.2.4.1. Konfiguration aus Kommando-Datei laden

Befehlssyntax:

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

Parameter:

<ip-address> IP Adresse des externen TFTP Servers
<path> Relativer Pfad auf dem TFTP Server, z.B. '/' oder '/nexans-cfg/iswitch/'
<filename>.cfg Name der Kommando-Datei mit Extension ".cfg", z.B. 'Nexans-00c029245634.cfg'

Die Zeichenlängen der Parameter <path> und <filename.xxx> dürfen jeweils 25 Zeichen nicht überschreiten. Dies ist eine Limitierung des Console Kommando Interpreters.

Nach dem Laden einer Datei mit der Extension 'cfg', wird zunächst die Konfiguration des Switches auf Factory-Default zurückgesetzt und anschließend der Inhalt zeilenweise als Abfolge von Console Kommandos interpretiert. Dabei sind die Dateiformate PC, UNIX und MAC zulässig.

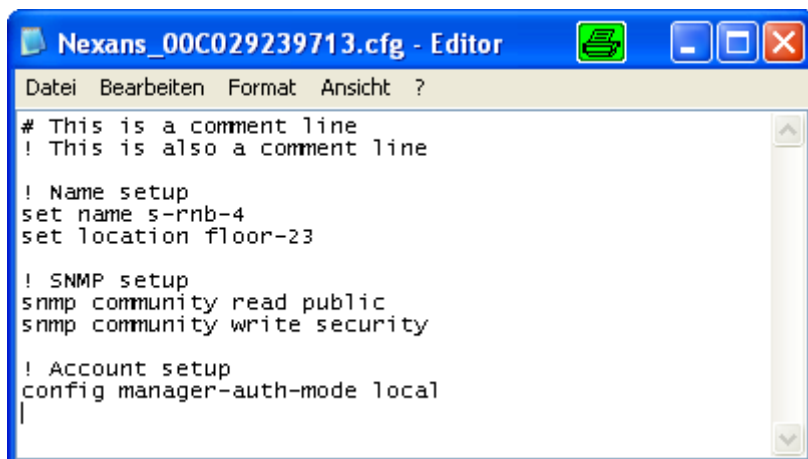
HINWEIS:

Folgende Parameter werden beim zurücksetzen des Switches auf Factory-Default beibehalten:

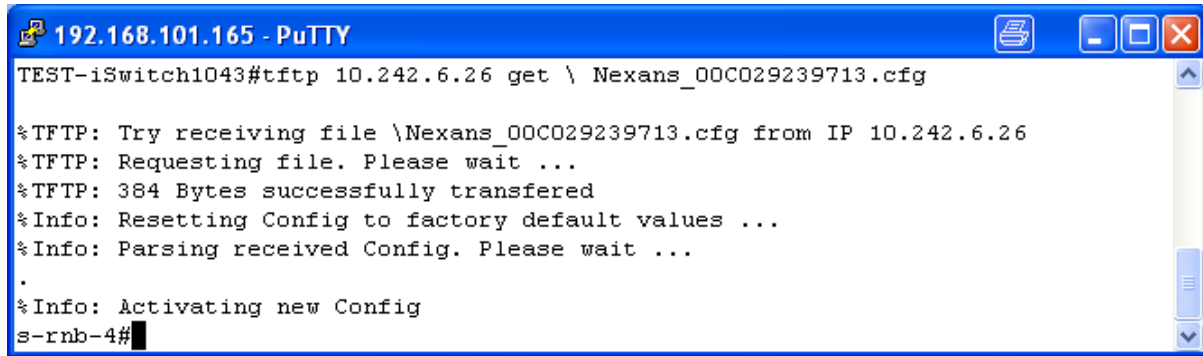
- Switch Name und Location
- IP Adresse, Gateway und Netzwerkmaske
- Admin Account Name und Passwort
- User Account Name und Passwort
- Password Encryption Mode

Falls gewünscht, können die obigen Parameter durch entsprechende Console Kommandos in der geladenen Datei dennoch überschrieben werden.

Hier ein Beispiel für den Inhalt einer solchen Datei:



Ein erfolgreicher Ladevorgang per Console sieht dann wie folgt aus:

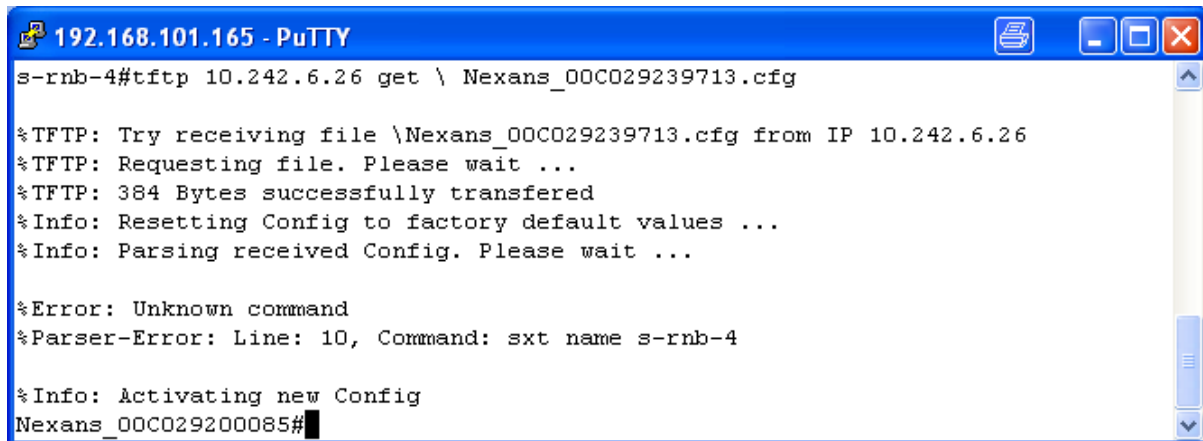


```

192.168.101.165 - PuTTY
TEST-iSwitch1043#tftp 10.242.6.26 get \ Nexans_00C029239713.cfg

%TFTP: Try receiving file \Nexans_00C029239713.cfg from IP 10.242.6.26
%TFTP: Requesting file. Please wait ...
%TFTP: 384 Bytes successfully transfered
%Info: Resetting Config to factory default values ...
%Info: Parsing received Config. Please wait ...
.
%Info: Activating new Config
s-rnb-4#
  
```

Sollte die Datei unbekannte oder unzulässige Kommandos enthalten, so wird eine entsprechende Fehlermeldung mit Angabe der Zeilennummer ausgegeben:



```

192.168.101.165 - PuTTY
s-rnb-4#tftp 10.242.6.26 get \ Nexans_00C029239713.cfg

%TFTP: Try receiving file \Nexans_00C029239713.cfg from IP 10.242.6.26
%TFTP: Requesting file. Please wait ...
%TFTP: 384 Bytes successfully transfered
%Info: Resetting Config to factory default values ...
%Info: Parsing received Config. Please wait ...

%Error: Unknown command
%Parser-Error: Line: 10, Command: sxt name s-rnb-4

%Info: Activating new Config
Nexans_00C029200085#
  
```

Nach Verarbeitung aller Kommandos (mit Ausnahme der fehlerhaften), wird die neue Konfiguration aktiviert und eine entsprechende Meldung ausgegeben: '%Info: Activating new Config'.

7.2.4.2. Konfiguration aus Binär-Datei laden

Befehlssyntax:

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

Parameter:

<ip-address>	IP Adresse des externen TFTP Servers
<path>	Relativer Pfad auf dem TFTP Server, z.B. '/' or '/nexans-cfg/iswitch/'
<filename>.dat	Name der Binär-Datei mit Extension ".dat", z.B. 'Nexans-00c029245634.dat'

Die Zeichenlängen der Parameter <path> und <filename.xxx> dürfen jeweils 25 Zeichen nicht überschreiten. Dies ist eine Limitierung des Console Kommando Interpreters.

Endet der Dateiname mit der Extension 'dat', so wird die Datei als Binärdatei interpretiert. Binärdateien können mittels NEXMAN sehr komfortabel erstellt und verwaltet werden. Dabei wird zunächst im Device-Editor über das Menü 'Config-Templates -> Save as BOOTP Config' eine Konfigurationsvorlage erstellt. In der Device-List kann dann per Menübefehl 'Config-Templates -> Edit BOOTP Config' die Konfiguration editiert werden.

WICHTIG:

Beim Laden einer Binär-Datei werden die IP-Parameter und der Name des Switches beibehalten. Aus diesem Grund sind diese Parameter im BOOTP-Editor des NEXMAN ausgeblendet.

Ein erfolgreicher Ladevorgang per Console sieht wie folgt aus:

```

192.168.101.165 - PuTTY
Nexans_00C029200085#tftp 10.242.6.26 get \ Nexans_00c029245634.dat

%TFTP: Try receiving file \Nexans_00c029245634.dat from IP 10.242.6.26
%TFTP: Requesting file. Please wait ...
%TFTP: 21504 Bytes successfully transfered
%Info: Activating new Config
Nexans_00C029200085#

```

Nach dem Empfang einer fehlerfreien Binär-Datei wird die enthaltene Konfiguration aktiviert und eine entsprechende Meldung ausgegeben: '%Info: Activating new Config'.

Sollte die Checksumme der Konfiguration fehlerhaft sein, so wird die Konfiguration nicht übernommen und stattdessen folgende Fehlermeldung ausgegeben: '%Error: Config has wrong checksum'.

7.2.5. Switch-Konfiguration automatisch per DHCP/BootP und TFTP laden

HINWEIS: Diese Funktion benötigt die Management Hardwareversion HW2 oder höher.

Im Gegensatz zum Laden der Konfiguration per Console Kommando, wird hier die IP-Adresse des TFTP-Servers und der Name der Konfigurationsdatei per DHCP Protokoll übermittelt. Für das Erstellen der entsprechenden Kommando- oder Binär-Dateien siehe Kapitel [7.2.4 Switch-Konfiguration per Telnet/SSH/V.24 Console und TFTP laden](#)

Voraussetzung um diese Funktion nutzen zu können ist, dass der Switch auf DHCP konfiguriert ist (dies ist die Factory-Default Einstellung). Der DHCP Server muss dabei zwei optionale Felder im DHCP-Protokoll mit entsprechenden Informationen füllen. Dies ist zum einen der 'server host name' und zum anderen der 'boot file name' (siehe RFC2131). Dabei können sowohl die Felder 'sname' und 'file' im Protokollheader, als auch die Optionen 66 und 67 verwendet werden. Werden für den 'server host name' oder 'boot file name' keine Wert übermittelt, so wird der Inhalt beider Felder ignoriert und keine Aktion zum Laden der Konfiguration ausgeführt.

HINWEIS: Der TFTP Download kann global abgeschaltet werden um das Laden einer Konfigurationsdatei beim Reboot des Switches zu unterbinden. Dies ist insbesondere hilfreich falls nur beim ersten Booten nach der Installation eine Konfigurationsdatei geladen werden darf aber DHCP weiterhin eingeschaltet bleiben soll. Durch Einfügen des CLI Kommandos „dhcp tftp-download disable“ in die Erstkonfigurationsdatei wird jeder weitere TFTP download unterbunden. Diese Einstellung lässt sich auch mit dem Switch Manager nachträglich vornehmen.

- **server host name**

Dieses Feld ist mit der IP-Adresse des TFTP-Servers (a.b.c.d) zu füllen. Ein DNS-Name ist hier nicht zulässig.

- **boot file name**

Hierbei sind zwei Varianten möglich:

- **Angabe eines Dateinamens:**

In diesem Fall wird ausschließlich die angegebene Datei beim TFTP-Server angefragt. Ist diese Datei auf dem TFTP-Server nicht vorhanden, bootet der Switch mit der aktuellen Flash Konfiguration.

Beispiele:

```

Configuration.cfg
Configuration.dat
/Update/Configuration.cfg
/Update/Configuration.dat

```

- **Angabe eines Verzeichnisnamens:**

Bei der Angabe eines Verzeichnisses muss am Ende immer ein Slash '/' stehen.

Beispiel:

```

/
/Config/

```

In diesem Fall versucht der Switch verschiedene fest definierte Dateinamen im angegebenen Verzeichnis zu finden. Die Reihenfolge der Konfigurationsanfragen ist dabei wie folgt:

- NEXANS-XXXXXXXXXXXXX.cfg (Kommando-Datei)
- NEXANS-XXXXXXXXXXXXX.dat (Binär-Datei)
- Nexans.cfg (Kommando-Datei)
- Nexans.dat (Binär-Datei)

XXXXXXXXXXXXX ist hierbei die MAC Adresse des Switches.

Sollte keine der Dateien auf dem TFTP Server vorhanden sein, so läuft der Switch mit der beim Booten geladenen Flash Konfiguration weiter.

WICHTIG:

Die im DHCP Paket enthaltenen Angaben bzgl. der IP-Adresse des TFTP-Servers und dem Namen der Konfigurationsdatei werden nur beim ersten DHCP-Acknowledge Paket des DHCP Servers nach dem reboot des Switches ausgewertet und die entsprechende Konfigurationsdatei per TFTP geladen. Bei Ablauf der halben DHCP Lease-Time bzw. durch Eingabe des Console Kommandos 'dh:cp r:renew' und dem dadurch ausgelösten DHCP-Request, werden die Angaben im DHCP-Acknowledge ignoriert.

Ein erneutes Laden der Konfigurationsdatei per DHCP/BOOTP kann wie folgt ausgelöst werden:

- durch einen reboot des Switches (z.B. durch das Console Kommando 'rel:oad')
- durch das Console Kommando 'dh:cp rel:oad-config' (dabei wird kein reboot ausgelöst)

WICHTIG:

Beim Laden einer Binär-Datei werden folgende Parameter beibehalten:

- Switch Name

Falls gewünscht, kann der Name des Switches über die DHCP Option 12 'Host Name' überschrieben werden.

Beim laden einer Kommando-Datei werden folgende Parameter beibehalten:

- Switch Name und Location
- Admin Account Name und Passwort
- User Account Name und Passwort
- Password Encryption Mode

Falls gewünscht, können die obigen Parameter durch entsprechende Console Kommandos in der geladenen Datei überschrieben werden.

7.2.6. Switch-Konfiguration per PC Console und TFTP lesen und schreiben

Hier wird für das Lesen bzw. Schreiben der Switch-Konfiguration ein TFTP-Client auf dem PC benötigt. Hier kann z.B. das bei Windows mitgelieferte 'tftp.exe' Programm verwendet werden.

WICHTIG:

Ein Lesen und Schreiben der Konfiguration vom PC aus ist nur möglich, wenn der 'Manager Authentication Mode' im Switch auf {none} eingestellt ist (siehe Kapitel [10.10. Manager Authentication Mode](#)) oder zuvor eine Authentifizierung per SNMP durchgeführt wurde (siehe Kapitel [10.3 Switch Name / Location / Contact / Domain](#)).

Für das Lesen der Konfiguration im Binär-Format gilt folgende Syntax:

Windows: `tftp -i <a.b.c.d> get config.bin a_b_c_d.dat`

Für das Schreiben der Konfiguration im Binär-Format gilt folgende Syntax:

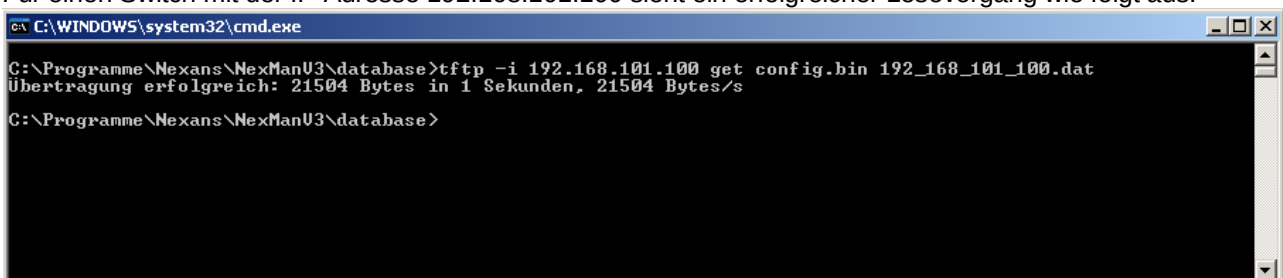
Windows: `tftp -i <IP-Adresse> put a_b_c_d.dat config.bin`

HINWEIS:

Per PC Console ist ein Lesen bzw. Schreiben der Konfiguration im Kommando-Format ausschließlich mittels SCP möglich (siehe Kapitel [7.2.7 Switch-Konfiguration per PC Console und SCP lesen und schreiben](#)).

Beispiel:

Für einen Switch mit der IP-Adresse 192.168.101.100 sieht ein erfolgreicher Lesevorgang wie folgt aus:



```
C:\WINDOWS\system32\cmd.exe
C:\Programme\Nexans\NexManU3\database>tftp -i 192.168.101.100 get config.bin 192_168_101_100.dat
Übertragung erfolgreich: 21504 Bytes in 1 Sekunden, 21504 Bytes/s
C:\Programme\Nexans\NexManU3\database>
```

Ein erfolgreicher Schreibvorgang sähe wie folgt aus:

```

C:\WINDOWS\system32\cmd.exe

C:\Programme\Nexans\NexManU3\database>tftp -i 192.168.101.100 put 192.168.101_100.dat config.bin
Übertragung erfolgreich: 21504 Bytes in 1 Sekunden, 21504 Bytes/s

C:\Programme\Nexans\NexManU3\database>

```

Nachdem die Konfiguration erfolgreich in den Switch übertragen wurde wird diese sofort, ohne reboot, wirksam.

WICHTIGER HINWEIS:

Die per TFTP gelesene Konfiguration ist binär formatiert und daher nicht mit einem Texteditor anzeigbar. Sie kann nur vom NEXMAN gelesen werden. Um diese per NEXMAN anzuzeigen und ggf. zu verändern, sollte die Konfigurationsdatei mit der oben angegebenen Namenskonvention in den 'Database folder' des NEXMAN kopiert werden. Anschließend kann diese per NEXMAN Rechts-Klick Funktion 'Open Switcheditor from Database' in den Switcheditor geladen werden.

7.2.7. Switch-Konfiguration per PC Console und SCP lesen und schreiben

HINWEIS: Diese Funktion benötigt die Management Hardwareversion HW3 oder höher.

Die Switch-Konfiguration kann mittels Secure Copy (SCP) Protokoll zum Switch geschrieben bzw. vom Switch gelesen werden. Eine Verwendung von Secure FTP (SFTP) ist nicht möglich. Unter Windows kann hierzu z.B. das Programm „pscp.exe“ verwendet, das im Paket des SSH/Telnet Client „PuTTY“ enthalten ist (siehe <http://www.putty.org>). Bei Linux Betriebssystemen steht hierfür der Standardbefehl „scp“ zur Verfügung.

7.2.7.1. CLI Konfiguration per PC Console und SCP lesen

Für das Lesen der Konfiguration im CLI Kommando-Format, die ausschließlich die Parameter enthält welche vom Factory Default abweichen, gilt folgende Syntax:

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

Für das Lesen der Konfiguration im CLI Kommando-Format, die alle Parameter enthält, gilt folgende Syntax:

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. CLI Konfiguration per PC Console und SCP schreiben

Für das Schreiben der Konfiguration im CLI Kommando-Format, mit Reset auf Factory Default, gilt folgende Syntax:

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

Für das Schreiben der Konfiguration im CLI Kommando-Format, ohne Reset auf Factory Default, gilt folgende Syntax:

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. Binär-Konfiguration per PC Console und SCP lesen

Für das Lesen der Konfiguration im Binär-Format gilt folgende Syntax:

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. Binär-Konfiguration per PC Console und SCP schreiben

Für das Schreiben der Konfiguration im Binär-Format gilt folgende Syntax:

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. Customer-CLI Konfigurationen per PC Console und SCP lesen

Für das Lesen der Customer Default Konfiguration im CLI Kommando-Format gilt folgende Syntax:

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

Für das Lesen der Customer Reboot Konfiguration im CLI Kommando-Format gilt folgende Syntax:

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. Customer-CLI Konfiguration per PC Console und SCP schreiben

Für das Schreiben der Customer Default Konfiguration im CLI Kommando-Format gilt folgende Syntax:

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

Für das Schreiben der Customer Reboot Konfiguration im CLI Kommando-Format gilt folgende Syntax:

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

WICHTIG:

Beim Schreiben der Konfiguration im CLI Kommando-Format, mit Reset auf Factory Default werden folgende Parameter beibehalten:

- Switch Name und Location
- Admin Account Name und Passwort
- User Account Name und Passwort
- Password Encryption Mode

Falls gewünscht, können die obigen Parameter durch entsprechende Console Kommandos in der geladenen Datei überschrieben werden.

7.2.8. Switch-Konfiguration ab Werk

Die Switch Vorkonfiguration ab Werk ist z.Z. ausschließlich für Switches vom Typ "GigaSwitch V5" möglich.

Dabei werden die Switches in einem eigenen Fertigungsschritt mit einer kundenspezifischen Konfiguration programmiert und anschließend mit einem Kopfeinleger versehen, der die IP-Adresse, die MAC-Adresse und optional den Text „Telefon“ aufgedruckt hat:



Der Kunde muss dafür die gewünschte Switch-Konfiguration in Form einer CLI Kommando-Datei zur Verfügung stellen. Diese lässt sich einfach über den Nexans Manager im Device-Editor per Menü "Configure > Read CLI Config (Only with parameters changed from Factory Default)" erstellen.

Zusätzlich werden folgende Angaben vom Kunden benötigt:

- Erste IP-Adresse des gewünschten IP-Adressen Bereiches. Die letzte Stelle muss dabei .1 sein (x.x.x.1)
- Festlegung, ob eine Memory Card installiert werden soll. In diesem Fall wird die MAC-Adresse der Memory Card (statt die MAC-Adresse des Switches) auf den Einleger aufgedruckt.

- Festlegung, ob der Text „Telefon“ über TP Port 4 auf den Einleger aufgedruckt werden soll.
- Festlegung, ob der Kopf entgegen der horizontalen Standardposition in der vertikalen Position ausgeliefert werden soll.

Für jede unterschiedliche Switch-Konfiguration muss eine eigene Erzeugnisnummer durch Nexans angelegt werden, die dann bei der Beauftragung der Switches zusätzlich mitbestellt werden muss.

WICHTIGER HINWEIS:

Aus Sicherheitsgründen können die Login Passwörter bei der Vorkonfiguration nicht gesetzt werden. Die Switches werden immer mit den Factory-Default-Passwörtern ausgeliefert. Individuelle Passwörter können nach der Installation der Geräte global via Master-Configuration verteilt werden.

7.3. Zero Touch Configuration

Auf HW5-Switchen können mit Zero Touch Configuration (ZTC) der Konfigurationsprozess und die Programmierung von Firmware-Upgrades automatisiert werden. Wenn Zero Touch Configuration aktiviert ist, werden neue Switch-Konfigurationen und Firmware Versionen automatisch vom Zero Touch Configuration Controller (im Weiteren *Controller* genannt) zur Verfügung gestellt. Der Controller ist ein separates Serversystem oder ein virtueller Server auf einem festgelegten Rechner im Netzwerk. Zero Touch Configuration ist standardmäßig aktiviert, sofern der Admin Account factory default ist (name: "admin", password: "nexans").

Beim Starten prüft der Switch, ob Zero Touch Configuration aktiviert ist. Falls dies der Fall ist, registriert sich der Switch beim Controller, um neue Konfigurationen oder Firmware zu erhalten. Dafür muss der Switch die IP-Adresse des Controllers kennen, die der Switch über drei verschiedenen Wege erhalten kann:

1. über die *Nexans*-specific DHCP Option 43 (falls DHCP aktiviert ist)
2. über einen DNS-Server mit Hilfe der DHCP Optionen 6 und 15 (falls DHCP aktiviert ist)
3. über die statische Controller-IP-Adresse, die im Switch konfiguriert ist

Die IP-Adresse des Controllers kann eine IPv4- oder IPv6-Adresse sein.

Zum Anzeigen des aktuellen Status von Zero Touch Configuration, DHCP-Server und DNS-Server kann der folgende Consolen-Befehl eingegeben werden:

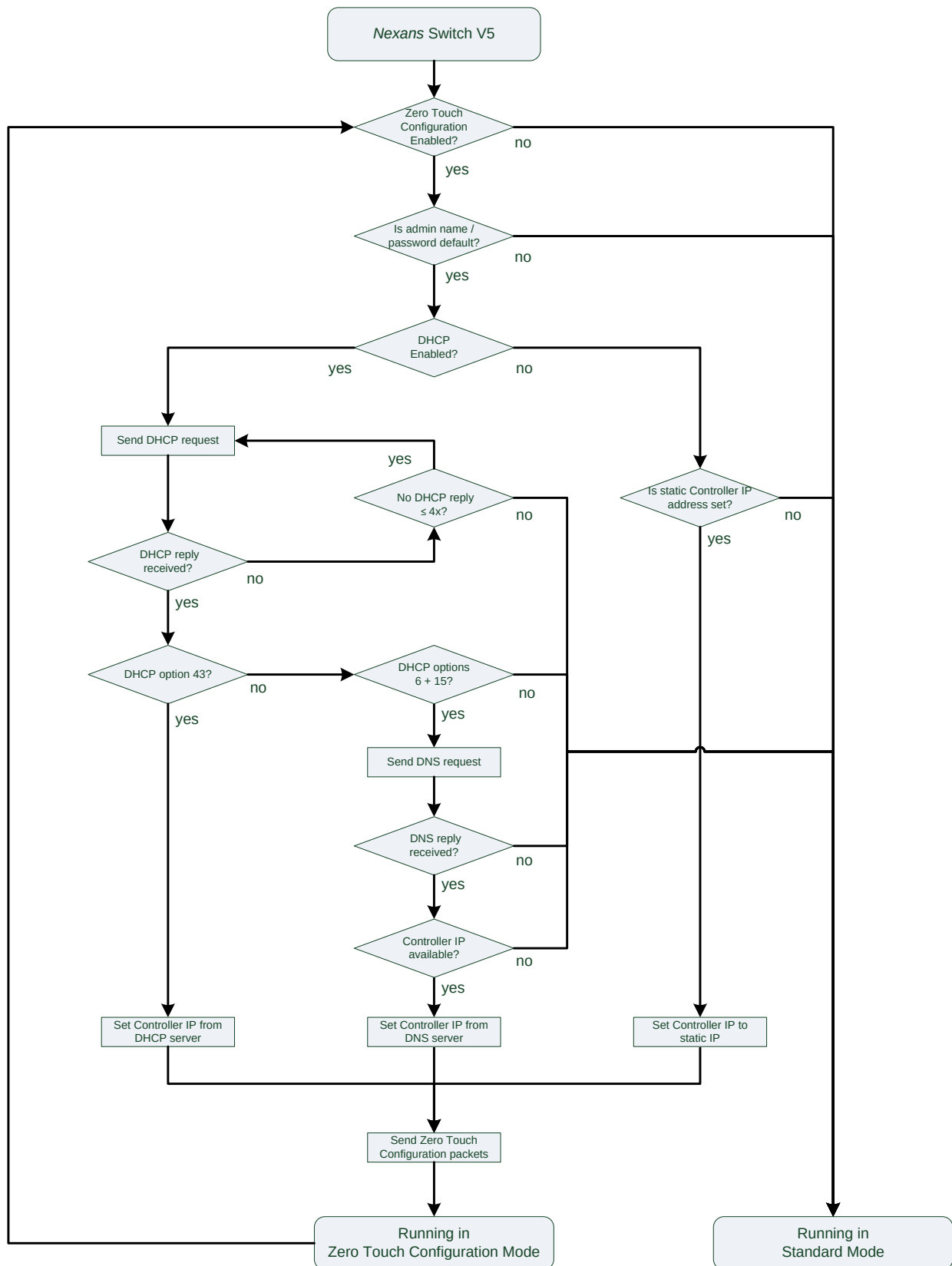
```
sh:ow zero-:touch-config
```

HINWEISE:

Dieses Feature ist nur für *Nexans* V5-Switches verfügbar.

Dieses Feature erfordert den NEXMAN Controller. Der NEXMAN Controller ist eine Server-Software, die auf dem Controller installiert ist und permanent im Hintergrund läuft.

Der allgemeine Funktionsablauf bei aktiver Zero Touch Configuration, ist im folgenden Ablaufdiagramm dargestellt:



7.3.1. Zero Touch Configuration-Einstellungen

Die folgende Tabelle zeigt eine Übersicht der Zero Touch Configuration-Einstellungen:

Bez. im NEXMAN	Default Wert	Funktion
Zero Touch Configuration Mode	enabled	Über den Zero Touch Configuration Mode kann das Feature aktiviert oder deaktiviert werden.
Controller IP Address	0.0.0.0	Die statische Controller-IPv4- oder IPv6-Adresse. Diese IP-Adresse wird nur verwendet, wenn DHCP deaktiviert ist. Mit dem Consolen-Befehl 'sh:ow zero-:touch-config' kann die momentan active Controller IP-Adresse überprüft werden.

7.3.2. Controller IP-Adresse über DHCP Option 43 ermitteln

Um die Controller IP-Adresse von einem DHCP-Server zu erhalten, muss DHCP aktiviert sein und auf dem DHCP-Server muss die Option 43 als *vendor-encapsulated-option* entsprechend dem folgenden *Nexans*-spezifischen Textformat konfiguriert sein:

```
0x01 <Textlänge> "NEXANS_cip_<IPv4/IPv6-Adresse>"
```

wobei 0x01 der Code der Suboption „Controller IP Adresse“ und <Text länge> die Länge des nachfolgenden Textfeldes ohne NULL-Terminator sind. Bei manchen DHCP-Servern wird die Textlänge automatisch über die Länge des nachfolgenden Textfeldes ermittelt und muss nicht explizit angegeben werden.

Darüber hinaus muss der DHCP-Server so eingestellt sein, dass Option 43 gesendet wird, wenn es sich bei dem anfragenden Gerät um einen *Nexans*-Switch handelt. Bei *Nexans*-Switchen beginnt der *vendor-class-identifier* in DHCP-Option 60 des DHCP-Requests mit dem fixen String "266" (z.B. "266:085").

Beispiel für einen *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. Controller IP-Adresse über DHCP Optionen 6 und 15 ermitteln

Um die Controller IP-Adresse von einem DNS-Server zu erhalten, muss DHCP aktiviert sein und auf dem DHCP-Server müssen die Optionen 6 und 15 für den DNS-Server konfiguriert sein, der die Controller IP-Adresse bereitstellt. Option 6 muss dabei die entsprechende IP-Adresse des DNS-Servers enthalten, und Option 15 muss den Namen der Domain, in der sich der DNS-Server befindet, enthalten.

Des Weiteren muss der DNS-Server mit der IP-Adresse und dem Computernamen des Controllers, sowie mit dem Namen der Domain. Der Controller-Name muss "nexans-controller" heißen.

7.3.4. Statische Controller IP-Adresse

Die statische IP-Adresse des Controllers ist Teil der Switch-Konfiguration und kann über den NexMan oder über das CLI konfiguriert werden. Um die statische IP-Adresse des Controllers zu aktivieren, muss DHCP inaktiv sein und eine gültige IPv4- oder IPv6-Adresse konfiguriert sein. Für Details zur Switch-Konfiguration von Zero Touch Configuration siehe Kapitel [9.18 Management > Zero Touch Configuration](#).

7.4. Skripting

HINWEIS: Diese Funktion benötigt die Management Hardwareversion HW5 oder höher.

Durch Skripting können eventbasierte kundenspezifische Konfigurationsänderungen vorgenommen werden. Basierend auf einem vordefinierten Systemereignis (Event) wird eine Liste von CLI-Befehlen gestartet. Die Liste der Befehle, die einem bestimmten Event zugewiesen sind, wird als *CLI-Skript* bezeichnet. Ein vordefiniertes Event kann die Statusänderung eines Ports oder eines Funktionseingangs oder ein zeitbasiertes Event sein.

7.4.1. Skript-Dateien

Alle CLI-Skripte, die für ein vordefiniertes Event ausgeführt werden sollen, sind in einer Skript-Datei enthalten. Grundsätzlich ist das Format der Skript-Datei identisch mit dem Format der CLI-Konfiguration (siehe Kapitel [7.2.1 Dateiformate der Switch-Konfiguration](#)). Mit dieser Lösung können Sie jeden verfügbaren CLI-Befehl ausführen.

Die Skript-Datei ist nicht Teil der laufenden Konfiguration und muss separat auf den Switch hochgeladen werden, entsprechend der Neustart- / Standardkonfiguration des Kunden.

Eine Skript-Datei kann bis zu 128 kB groß sein und ist in zwei Teile unterteilt: den Teil "CLI Script Definitions" und den Teil "Running CLI Configuration".

“CLI Script Definitions” Teil:

Der Teil „CLI Script Definitions“ besteht aus bis zu 1024 CLI-Skript-Abschnitten, wobei jeder Abschnitt ein CLI-Skript mit einer maximalen Größe von 4 kB definiert. Die Syntax eines CLI-Skript-Abschnitts sieht wie folgt aus:

```
#START <CLI Script name>#
```

```
<List of CLI commands>
```

```
#END <CLI Script name>#
```

Hier gehören alle CLI-Befehle, die von den Tags START und END umschlossen sind, zum CLI-Skript mit dem Namen <CLI Script name>. Der CLI-Skript-Name muss eine eindeutige Textbezeichnung sein.

“Running CLI Configuration” Teil:

Im Teil "Running CLI Configuration" werden die vordefinierten Events konfiguriert, d.h. ein CLI-Skript wird den entsprechenden Events zugewiesen. Ein CLI-Skript kann einem oder mehreren Events zugewiesen werden. Wenn mehrere CLI-Skripte nacheinander demselben Event zugewiesen werden, wird das zuletzt zugewiesene CLI-Skript ausgeführt.

Für jedes Event, das Sie konfigurieren möchten, müssen Sie einen entsprechenden CLI-Befehl hinzufügen. Derzeit können die folgenden vordefinierten Events für CLI-Skripte konfiguriert werden:

Event	Resultierende Aktion
Link-Up	Startet das CLI-Skript, wenn ein Link an dem/den konfigurierten Port/Ports besteht
Link-Down	Startet das CLI-Skript, wenn ein Link an dem/den konfigurierten Port/Ports unterbrochen ist
Link-Change	Startet das CLI-Skript, wenn sicher der Link-Status an dem/den konfigurierten Port/Ports von Link-Down nach Link-Up oder umgekehrt geändert hat

WICHTIGER HINWEIS:

Je nach Kundenwunsch können wir den Support für weitere Events kurzfristig nach Bedarf erweitern. Grundsätzlich können wir für jedes nützliche Alarm- oder Aktions-Event, das in der Alarm Destination Table verfügbar ist, eine CLI-Skript-Zuweisung implementieren (siehe Kapitel [10.54. Alarm Destination Table](#)).

7.4.1.1. CLI-Skript einem Event für Statusänderung an Ports zuordnen

Um einem Link-Up-, Link-Down- oder Link-Change-Event an einem oder mehreren Ports ein CLI-Skript zuzuweisen, müssen Sie den folgenden CLI-Befehl aufrufen:

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

7.4.1.2. CLI-Skript von einem Event für Statusänderung an Ports entfernen

Um das zugeordnete CLI-Skript von einem Link-Up-, Link-Down- oder Link-Change-Event an einem oder mehreren Ports zu entfernen, müssen Sie den folgenden CLI-Befehl aufrufen:

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

7.4.2. Skripting per NEXMAN

Die Änderung und das Verwalten der Skript-Datei kann über den Nexans Switch Manager (NEXMAN) erfolgen. Die Skript-Dateien werden vom NEXMAN im sogenannten 'Database folder' abgelegt. Für jeden Switch wird dabei eine Datei mit dem Namen a_b_c_d.script angelegt (a_b_c_d ist dabei die IP Adresse a.b.c.d des Switches).

Das Lesen und Schreiben der Skript-Datei über NEXMAN erfolgt ausschließlich über SCP. Hier arbeitet der Switch als SCP-Server über den TCP-Port 50271. Weitere Informationen finden Sie im Kapitel 7.4.3 Skript-Datei per PC Console und SCP lesen und schreiben.

7.4.3. Skript-Datei per PC Console und SCP lesen und schreiben

Die Skript-Datei kann mittels Secure Copy (SCP) Protokoll zum Switch geschrieben bzw. vom Switch gelesen werden. Unter Windows kann hierzu z.B. das Programm „pscp.exe“ verwendet werden, das im Paket des SSH/Telnet Client „PuTTY“ enthalten ist (siehe <http://www.putty.org>). Bei Linux Betriebssystemen steht hierfür der Standardbefehl „scp“ zur Verfügung.

7.4.3.1. Skript-Datei per PC Console und SCP lesen

Für das Lesen der Skript-Datei vom Switch gilt folgende Syntax:

```
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. Skript-Datei per PC Console und SCP schreiben

Für das Schreiben der Skript-Datei zum Switch gilt folgende Syntax:

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

HINWEIS:

Zum Löschen des Scriptings müssen Sie eine leere Skript-Datei zum Switch schreiben.

7.4.4. Skripting Beispiele

7.4.4.1. Switch-Name bei Link-Up / Link-Down Event ändern

```
# 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. Admin-Status und VLANs bei Link-Up / Link-Down Event ändern

```
# 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 Authentifizierung per SNMP

Die hier beschriebene Authentifizierungsmethode mittels SNMP gilt nur für den TFTP Transfers per PC Console. Grundsätzlich benötigt das Lesen und Schreiben der Konfiguration und das Firmware-Update per PC Console eine vorausgehende Authentifizierung, die, bei Verwendung des NEXMAN, über ein proprietäres Protokoll mittels UDP Port 50266 durchgeführt wird.

Alternativ hierzu kann die Authentifizierung auch per SNMP Get- bzw. Set-Request erfolgen.

Die entsprechende MIB Variabel lautet:

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

Diese kann die nachfolgenden Werte annehmen:

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

In welcher Art und Weise über diese Variable eine Authentifizierung zulässig ist, kann über die Einstellung 'TFTP Authentication via SNMP' konfiguriert werden.

Hierbei stehen folgende Modi zur Verfügung:

- Disabled: Authentifizierung per SNMP nicht möglich
- Read/Only Nur Authentifizierung für das Lesen der Konfiguration möglich
- Read/Write: Authentifizierung für Lesen/Schreiben der Konfiguration und Firmware-Update möglich

Nach erfolgreicher Authentifizierung per SNMP darf ein einziger TFTP Transfer ausgeführt werden. Nach Beendigung des TFTP Transfers wird der TFTP Zugriff sofort wieder gesperrt.

Disabled (Factory-Default):

Authentifizierung per SNMP nicht möglich.

Read/Only:

Bei dieser Einstellung kann nur das Lesen der Konfiguration authentifiziert werden.

Die Authentifizierung kann dabei auf mehrere Arten erfolgen:

- a) SNMP Get-Request mit der korrekten Read/Trap Community
- b) SNMP Set-Request mit dem Wert tftpAccessReadOnly(2) und der korrekten Write/Read Community
- c) SNMP Set-Request mit dem Wert tftpAccessReadWrite(3) und der korrekten Write/Read Community

Read/Write:

Bei dieser Einstellung kann das Lesen und Schreiben der Konfiguration und ein Firmware-Update authentifiziert werden.

Die Authentifizierung für das Lesen der Konfiguration kann dabei auf dieselbe Art erfolgen wie oben bei 'Read/Only' aufgeführt. Die Authentifizierung für das Schreiben der Konfiguration und das Firmware-Update kann dagegen ausschließlich über einen SNMP Set-Request mit dem Wert tftpAccessReadWrite(3) und der korrekten Write/Read Community erfolgen.

HINWEIS:

Die Authentifizierung per SNMP **Set**-Request ist nur dann möglich, wenn der 'SNMP access mode' auf {Read/Write} eingestellt ist.

8. Rücksetzen auf Werkseinstellungen

Folgende Befehle zum Rücksetzen stehen zur Verfügung:

- 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)

Der Switch führt einen „Cold Start“ durch. Ist eine „Customer Reboot“ Konfiguration vorhanden, so wird die aktuelle Konfiguration mit den Parametern der Reboot Konfiguration überschrieben.

Reboot with Factory Default :

Das Rücksetzen auf Werkseinstellungen ist primär erforderlich, wenn der Switch unbeabsichtigt falsch konfiguriert wurde und dadurch über das Management nicht mehr erreichbar ist. Das Rücksetzen kann per Konfigurationsschalter erfolgen (siehe nächstes Kapitel), oder, falls das Management noch ansprechbar ist, per Management Funktion via WEB, CLI, SNMP und Manager Interface.

Reboot with Factory Default (Except IP Parameters):

Bei dieser Funktion werden alle Einstellungen, ausgenommen der IP Parameter auf Factory Default gestellt.

Reboot without customer reboot settings

Bei vorhandener „Customer Reboot Konfiguration“ wird bei dieser Option eine Reboot durchgeführt, ohne die aktuelle Konfiguration mit den Parametern der Reboot Konfiguration zu überschreiben.

Reboot with customer default settings

Durch diese Funktion wird der Switch mit der hinterlegten „Customer Default Konfiguration“ gebootet. Hierbei werden alle Parameter auf Factory-Default gesetzt und danach die Parameter der „Customer Default Konfiguration“ geladen.

Reset Total Boots Counter:

Mit dieser Funktion kann der Counter für die Anzahl der Reboots zurückgesetzt werden.

HINWEIS:

Ein löschen dieses Counters per "Reboot with Factory Default" ist nicht möglich.

Reset Total Operation Time:

Durch diesen Befehl wird die angezeigte Total Operation Time zurückgesetzt.

HINWEIS:

Die Total Operation Time wird nur für Switches mit einem Herstellungsdatum ab 2009 unterstützt. Ein löschen des Wertes per "Reboot with Factory Default" ist nicht möglich.

Reset Local Logging:

Diese Funktion löscht das lokale SYSLOG des Switches.

Reset Firmware on Memory Card:

Diese Funktion löscht die Firmware, die auf der MC-Karte gespeichert ist.

Reset Total Boots Counter, Port Counters, Total Operation Time, Local Logging and Firmware on Memory Card

Dieser Befehl kombiniert die aufgelisteten Reset-Befehle.

8.1. Rücksetzen auf Werkseinstellungen per Konfigurationsschalter

WICHTIGER HINWEIS:

Falls die Konfigurationsschalter per Management deaktiviert wurden, ist entsprechend Kapitel 3.5 Management Konfigurationsschalter deaktivieren vorzugehen.

Bei aktivierten Konfigurationsschalter ist die Vorgehensweise ist wie folgt:

1	Booten mit Factory-Default Einstellungen Switch per Konfigurationsschalter mit Factory-Default Einstellungen booten. Detaillierte Vorgehensweise siehe Kapitel <u>3.4. Management Konfigurations-Schalter bzw. -Taster</u>
2	Prüfen ob die Status-LED auf dem Management Modul permanent leuchtet Hinweise zur Funktion der Status-LED siehe Kapitel <u>3.3 Management Status-LED</u> .
3	Booten mit Flash Konfiguration Switch per Konfigurationsschalter mit Flash Konfiguration booten. Detaillierte Vorgehensweise siehe Kapitel <u>3.4. Management Konfigurations-Schalter bzw. -Taster</u>
4	Prüfen ob die Status-LED auf dem Management Modul permanent leuchtet Jetzt ist der Switch erfolgreich auf die Factory-Default-Einstellungen zurückgesetzt.

9. Liste der Status- und Konfigurationsparameter

Die nachfolgenden Tabellen zeigen eine Übersicht aller Status- und Konfigurationsparameter. Die Überschriften der einzelnen Kapitel sind dabei identisch zur Bezeichnung der Menü-Reiter im NEXMAN.

Für jeden Parameter ist dabei angegeben, wie dieser im WEB, in der Telnet/SSH/V.24-Console und per SNMP angezeigt bzw. konfiguriert werden kann.

Zeilen mit einem '-' bedeuten, dass dieser Parameter über die betreffende Schnittstelle nicht angezeigt bzw. konfiguriert werden kann.

WICHTIG:

Die in diesem Handbuch beschriebenen Funktionen werden nicht von allen Switchtypen bzw. Firmware-Versionen unterstützt.

Die Angaben in den einzelnen Zeilen haben folgende Bedeutung:

Kapitel:

Hier wird auf das jeweilige Kapitel verwiesen, in dem nähere Informationen zur Funktionsweise des Parameters zu finden sind.

WEB:

Angaben ist die Bezeichnung des Links im oberen Browser-Frame. Nach Klick auf den angegebenen Link wird die entsprechende Page angezeigt auf der der jeweilige Parameter aufgeführt ist.

Console Show:

Mit dem angegebenen Console Kommando kann der jeweilige Status in der Telnet und V.24 Console angezeigt werden. Bei Konfigurationsparametern wird die aktuell im Flash gespeicherte Konfigurationseinstellung angezeigt.

Console Set:

Mit dem angegebenen Console Kommando kann der jeweilige Konfigurationsparameter in der Telnet bzw. V.24 Console verändert werden.

SNMP OID:

Hier ist jeweils die entsprechende MIB und der Name der MIB Variablen angegeben. Sollte ein Parameter in mehreren MIBs verfügbar sein, so sind diese MIBs untereinander aufgeführt. Für die komplette OID sollte die jeweils angegebene MIB konsultiert werden.

9.1. Hinweise zur Console Kommando Syntax

Fast alle Kommandos und Parameter können abgekürzt eingegeben werden, wobei der Doppelpunkt gemäß Kommando-Übersicht die minimale Zeichenanzahl kennzeichnet. Der Doppelpunkt gehört nicht zum Kommando und muss bei der Eingabe weggelassen werden.

Folgende Sonderzeichen werden hier verwendet:

# ...	Kommando steht nur im 'Admin' Access-Level zur Verfügung.
> ...	Kommando steht im 'Admin' und 'User' Access-Level zur Verfügung.
:	Trennzeichen für verkürzte Eingabe des Kommandos. Z.B. darf beim Kommando 'show' sowohl 'sh', 'sho' als auch 'show' eingegeben werden.
{...}	Parameter-Optionsliste. Nur einer der aufgeführten Parameter darf eingegeben werden.
[...]	Der Parameter ist optional und darf ggf. weggelassen werden.
(a...b)	Numerischer Parameter mit Angabe des zulässigen Min.- und Max.-Wertes
<string ...>	String Parameter mit Angabe der zulässigen Anzahl von Zeichen
<ip-address>	IP-Adresse im Format a.b.c.d

Die Telnet Console unterstützt einen History-Buffer, der die letzten 10 eingegeben Kommandos speichert. Mit den Tasten '↑' bzw. '↓' kann durch den Buffer gescrollt werden.

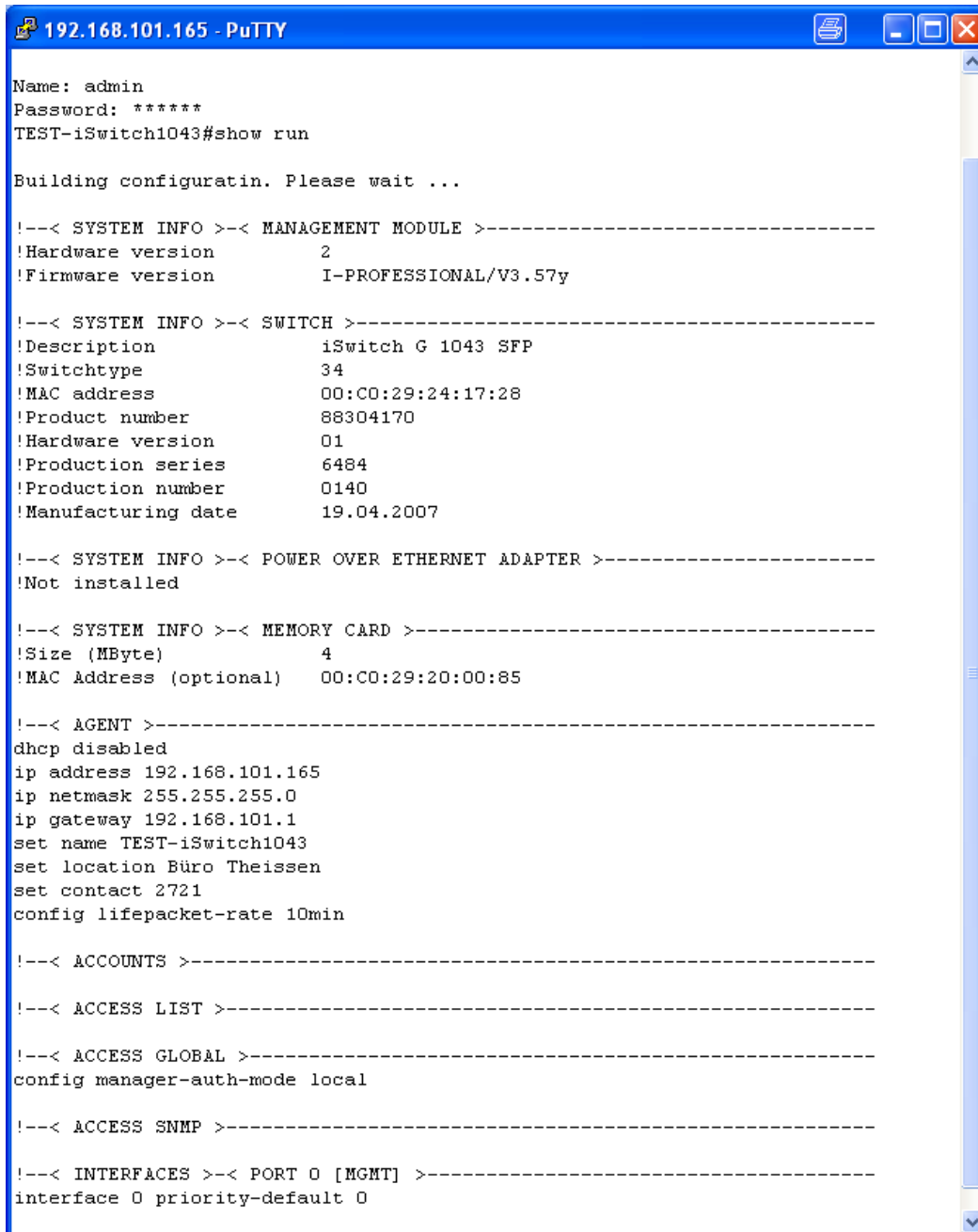
9.2. Aktuelle Konfiguration auf der Console ausgeben

Die aktuelle Konfiguration des Switches kann über das Console Kommando `sh:ow ru:nning-config [a:ll]` angezeigt werden.

Ohne Angabe des optionalen Parameters "all" werden nur solche Einstellungen angezeigt, die vom Factory-Default abweichen. Mit Angabe des Parameters "all" werden alle Konfigurationseinstellungen angezeigt, auch solche, die auf Factory-Default eingestellt sind.

Nach Absenden des Kommandos wird zunächst die Konfigurationsdatei im Speicher erstellt und anschließend seitenweise an der Console ausgegeben.

Beispiel:



```

192.168.101.165 - PuTTY
Name: admin
Password: *****
TEST-iSwitch1043#show run

Building configuratin. Please wait ...

!--< SYSTEM INFO >--< MANAGEMENT MODULE >-----
!Hardware version      2
!Firmware version      I-PROFESSIONAL/V3.57y

!--< SYSTEM INFO >--< SWITCH >-----
!Description           iSwitch G 1043 SFP
!Switchtype            34
!MAC address           00:CO:29:24:17:28
!Product number        88304170
!Hardware version       01
!Production series      6484
!Production number      0140
!Manufacturing date     19.04.2007

!--< SYSTEM INFO >--< POWER OVER ETHERNET ADAPTER >-----
!Not installed

!--< SYSTEM INFO >--< MEMORY CARD >-----
!Size (MByte)          4
!MAC Address (optional) 00:CO:29:20:00:85

!--< AGENT >-----
dhcp disabled
ip address 192.168.101.165
ip netmask 255.255.255.0
ip gateway 192.168.101.1
set name TEST-iSwitch1043
set location Büro Theissen
set contact 2721
config lifepacket-rate 10min

!--< ACCOUNTS >-----

!--< ACCESS LIST >-----

!--< ACCESS GLOBAL >-----
config manager-auth-mode local

!--< ACCESS SNMP >-----

!--< INTERFACES >--< PORT 0 [MGMT] >-----
interface 0 priority-default 0

```

HINWEIS: Das Kommando 'sh:ow ru:nning-config [a:ll]' benötigt ein installiertes Management Modul mit der Hardwareversion 2.

Alternativ kann die Konfiguration auch nach Funktionszugehörigkeiten getrennt angezeigt werden. Hier stehen u.a. folgende Kommandos zur Verfügung:

```

# sh:ow con:figuration acce:ss [a:ll]
# sh:ow con:figuration acco:unts [a:ll]

```

```
# show configuration al:arm-destinations [a:ll]
# show configuration agent [a:ll]
> show configuration discovery [a:ll]
# show configuration dot1x [a:ll]
> show configuration global [a:ll]
> show configuration igmp [a:ll]
> show configuration interfaces [a:ll]
> show configuration prioritisation [a:ll]
# show configuration radius [a:ll]
> show configuration redundancy [a:ll]
> show configuration sf:p-limits [a:ll]
> show configuration sntp [a:ll]
> show configuration v:lan [a:ll]
```

Die Funktion des optionalen Parameters "all" ist dabei identisch zum Kommando 'show running-config [a:ll]'.

9.3. Reset-Befehle

Bezeichnung	Zugriff
Globale Reset-Befehle	
Reboot (Cold Start)	Kapitel: 3.6.1. Booten mit Flash Konfiguration (Normalbetrieb) WEB: Switch Setup → Reset Command → Reboot (Cold Start) Console Set: # reload SNMP OID: NEXANS-BM-MIB → adminReset → rebootSwitch
Reboot with Factory Default	Kapitel: 8. Rücksetzen auf Werkseinstellungen WEB: Switch Setup → Reset Command → Reboot with Factory Default Console Set: # reload factory-a:ll SNMP OID: NEXANS-BM-MIB → adminReset → rebootToFactoryDefaults
Reboot with Factory Default (Except IP Parameters)	Kapitel: 8. Rücksetzen auf Werkseinstellungen WEB: - Console Set: # reload factory-w:thout-ip SNMP OID: -
Reset Total Boots Counter	Kapitel: 8. Rücksetzen auf Werkseinstellungen WEB: Switch Setup → Reset Command → Reset Total Boots Counter Console Set: # reset b:oots SNMP OID: -
Reset Total Operation Time	Kapitel: 8. Rücksetzen auf Werkseinstellungen WEB: Switch Setup → Reset Command → Reset Total Operation Time Console Set: # reset o:peration-time SNMP OID: -
Reset Port Counters	Kapitel: 10.27. Reset all Port Counters WEB: Switch Setup → Reset Command → Reset all counters Console Set: > reset c:ounter SNMP OID: NEXANS-BM-MIB → adminReset → resetCounters
Renew IP- und VLAN-Parameter	Kapitel: 10.8. Konfiguration der IP- und VLAN-Parameter WEB: Switch Setup → Renew IP- and VLAN Parameter Console Set: # renew SNMP OID: NEXANS-BM-MIB → adminReset → renewIpAndVlanParameter

Reset Local Logging	Kapitel: <u>10.54. Alarm Destination Table</u> WEB: Local Log → Delete Log Console Set: # sh:ow l:og delete SNMP OID: -
Reset Firmware on Memory Card	Kapitel: <u>4.5 Memory Card Firmware-Update</u> WEB: Switch Setup → Reset Command → Reset Firmware on Memory Card Console Set: > res:et f :irmware-memory-card SNMP OID: -
Port Reset-Befehle	
Renew Portsecurity	Kapitel: <u>10.36.5. Portsecurity – Renew-Befehl</u> 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	Kapitel: <u>11.1.7. PoE</u> 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

Bezeichnung	Zugriff
Global	
Show all Counters	Kapitel: <u>10.52. Statistic- / RMON-Counter</u> 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	Kapitel: <u>10.70. Link Layer Discovery Protocol (LLDP)</u> <u>10.72. Cisco Discovery Protocol (CDP)</u> WEB: - Console Show: > sh:ow n:ighbors-table [<if-no> c:lear-table] SNMP OID: -
Show SFP Info	Kapitel: <u>10.25. SFP Info, Diagnose</u> WEB: Port+Alarm State Console Show: > sh:ow sf:p-info [<if-no>] SNMP OID: -
Show IGMP State	Kapitel: <u>10.69.1. IGMP Snooping</u> WEB: - Console Show: > sh:ow ig:mp SNMP OID: -

Show STP State	Kapitel: <u>10.73. Rapid Spanning Tree Protocol (RSTP)</u> <u>10.74. Multiple Spanning Tree Protocol (MSTP)</u> WEB: Spanning Tree State Console Show: > sh:ow rs:tp > sh:ow ms:tp [instance-id] SNMP OID: -
Cable Diagnostic all TP Ports	Kapitel: <u>10.23. Kabel Diagnose bei Twisted-Pair Ports</u> WEB: Cable Diagnostic Console Show: > ca:ble-diagnostic {<if-no> a:ll} SNMP OID: -
Show MRP State	Kapitel: <u>10.76 Media Redundancy Protocol (MRP)</u> WEB: - Console Show: > sh:ow mr:p SNMP OID: -
Global State	
Temperature (°C)	Kapitel: <u>10.29. Switch Temperatur</u> WEB: Info Console Show: > sh:ow inf:o SNMP OID: NEXANS-BM-MIB → infoTemperature
Internal Voltage 1 (V) Internal Voltage 2 (V)	Kapitel: <u>10.30. Switch Betriebsspannungen</u> WEB: Info Console Show: > sh:ow inf:o SNMP OID: NEXANS-BM-MIB → infoPowerVoltage2500 NEXANS-BM-MIB → infoPowerVoltage3300
PoE Input Voltage (V)	Kapitel: <u>11.1.1. PoE-Messwerte</u> WEB: PoE State Console Show: > sh:ow p:oe SNMP OID: NEXANS-BM-MIB → infoPoeInputVoltage
Uptime	Kapitel: <u>10.28.1. System Up Time</u> WEB: Info Console Show: > sh:ow inf:o SNMP OID: MIB-II → sysUpTime
Time from time server	Kapitel: <u>10.28.3. Network Time Protokoll - SNTP</u> WEB: Info Console Show: > sh:ow inf:o SNMP OID: NEXANS-BM-MIB → infoLastSntpTime
Active MAC Address	Kapitel: <u>10.2. Ermittlung der aktiven MAC Adresse</u> WEB: Info Console Show: > sh:ow inf:o SNMP OID: NEXANS-BM-MIB → adminAgentPhysAddress
Memory Card	Kapitel: <u>4. Memory Card (MC)</u> WEB: Info Console Show: > sh:ow inf:o SNMP OID: -

Power Input S1 (V)	Kapitel: <u>10.30. Switch Betriebsspannungen</u> WEB: Port+Alarm State Console Show: > sh:ow al:arms SNMP OID: NEXANS-BM-MIB → infoS1InputVoltage
Power Input S2 (V)	Kapitel: <u>10.30. Switch Betriebsspannungen</u> WEB: Port+Alarm State Console Show: > sh:ow al:arms SNMP OID: NEXANS-BM-MIB → infoS1InputVoltage
Industrial State	
Alarm Output M1	Kapitel: <u>10.47 Alarmausgänge bei Industrie Switchen</u> WEB: Port+Alarm State Console Show: > sh:ow al:arms SNMP OID: NEXANS-BM-MIB → infoAlarmStateM1
Alarm Output M2	Kapitel: <u>10.47 Alarmausgänge bei Industrie Switchen</u> WEB: Port+Alarm State Console Show: > sh:ow al:arms SNMP OID: NEXANS-BM-MIB → infoAlarmStateM2
Function Input	Kapitel: <u>10.47 Alarmausgänge bei Industrie Switchen</u> WEB: Port+Alarm State Console Show: > sh:ow al:arms SNMP OID: -
Port Link State	
Link State	Kapitel: <u>10.21. Link / EEE State</u> WEB: Port State Console Show: > sh:ow int:erfaces [<if-no>] SNMP OID: NEXANS-BM-MIB → portLinkState
Time since last link change	Kapitel: <u>10.28.2. Time since last link change</u> WEB: - Console Show: - SNMP OID: MIB-II → ifLastChange
Error Counter	Kapitel: <u>10.26. Error Counter</u> WEB: Port State Console Show: > sh:ow int:erfaces SNMP OID: NEXANS-BM-MIB → portErrorCounter
Security State	Kapitel: <u>10.36.4. Portsecurity - Security State</u> WEB: Port State Console Show: > sh:ow se:curity SNMP OID: NEXANS-BM-MIB → portSecurityForwardingState
Active Default VLAN	Kapitel: <u>10.31.11. Port Active Default-VLAN-ID</u> WEB: Port State Console Show: > sh:ow int:erfaces SNMP OID: NEXANS-BM-MIB → portActiveDefaultVlanId

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

9.5. State > MAC + Security State

Bezeichnung	Zugriff
Global	
MAC Table	Kapitel: <u>10.37. MAC Adressen Tabelle</u> 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	Kapitel: - WEB: - Console Show: > pi:ng <ip-address> SNMP OID: -
Port Security State	
Security State	Kapitel: <u>10.36.4. Portsecurity - Security State</u> WEB: Port State Console Show: > sh:ow se:curity SNMP OID: NEXANS-BM-MIB → portSecurityForwardingState
Active Default VLAN-ID	Kapitel: <u>10.31.11. Port Active Default-VLAN-ID</u> WEB: Port State Console Show: > sh:ow int:erfaces SNMP OID: NEXANS-BM-MIB → portActiveDefaultVlanId

Active Voice VLAN	Kapitel: <u>10.31.12. Port Active Voice-VLAN-ID</u> WEB: Port State Console Show: > sh:ow int:erfaces SNMP OID: NEXANS-BM-MIB → portActiveVoiceVlanId
Allowed MACs Overflow Address	Kapitel: <u>10.36.3. Portsecurity - Allowed MACs Overflow Address</u> WEB: Port State → [Failure MAC Address] Console Show: - SNMP OID: NEXANS-BM-MIB → infoSecurityFailMacAddr
MAC Address 1 MAC Address 2 MAC Address 3	Kapitel: <u>10.36.10. Portsecurity - MAC Adressen</u> 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	Kapitel: <u>10.36.11. Portsecurity - MAC State</u> WEB: Port State → (MAC State) Console Show: > sh:ow se:curity SNMP OID: -

9.6. State > PoE State

Bezeichnung	Zugriff
Port PoE State	
PoE Voltage (V)	Kapitel: <u>11.1.1. PoE-Messwerte</u> WEB: PoE State Console Show: > sh:ow p:oe SNMP OID: NEXANS-BM-MIB → portPoeVoltage
PoE Current (mA)	Kapitel: <u>11.1.1. PoE-Messwerte</u> WEB: PoE State Console Show: > sh:ow p:oe SNMP OID: NEXANS-BM-MIB → portPoeCurrent
PoE Power (W)	Kapitel: <u>11.1.1. PoE-Messwerte</u> WEB: PoE State Console Show: > sh:ow p:oe SNMP OID: NEXANS-BM-MIB → portPoePower (in mw)
PoE Powerclass	Kapitel: <u>11.1.1. PoE-Messwerte</u> WEB: PoE State Console Show: > sh:ow p:oe SNMP OID: -
Power Supply State	
PoE Input Voltage (V)	Kapitel: <u>11.1.1. PoE-Messwerte</u> WEB: PoE State Console Show: > sh:ow p:oe SNMP OID: NEXANS-BM-MIB → infoPoeInputVoltage

PoE Input Current (mA)	Kapitel: <u>11.1.1. PoE-Messwerte</u> WEB: PoE State Console Show: > sh:ow p:oe SNMP OID: -
PoE Input Power (W)	Kapitel: <u>11.1.1. PoE-Messwerte</u> WEB: PoE State Console Show: > sh:ow p:oe SNMP OID: NEXANS-BM-MIB → infoPoeInputPower (in mW)

9.7. State > Radius State

Bezeichnung	Zugriff
RADIUS Server State	
Global Authentication Server 1 - 4	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: > sh:ow ra:dius SNMP OID: -
Management Authentication Server 1 - 4	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: > sh:ow ra:dius SNMP OID: -
Accounting Server 1 - 4	Kapitel: <u>10.60. RADIUS Accounting</u> WEB: - Console Show: > sh:ow ra:dius SNMP OID: -

9.8. State > TACACS+ State

Bezeichnung	Zugriff
TACACS+ Server State	
Authentication Server 1 - 4	Kapitel: <u>10.61 TACACS+ Authentication</u> WEB: - Console Show: > sh:ow ta:cacs+ SNMP OID: -
Authorization Server 1 - 4	Kapitel: <u>10.62 TACACS+ Authorization</u> WEB: - Console Show: > sh:ow ta:cacs+ SNMP OID: -
Accounting Server 1 - 4	Kapitel: <u>10.63 TACACS+ Accounting</u> WEB: - Console Show: > sh:ow ta:cacs+ SNMP OID: -

9.9. Device Info

Bezeichnung	Zugriff
Management Info	
Management Hardwareversion	Kapitel: <u>10.1. Ermittlung von Switchtyp und Managementversion</u> WEB: Device Info Console Show: > sh:ow inf:o SNMP OID: NEXANS-BM-MIB → infoMgmtHardwareVersion
Management Firmware-Version	Kapitel: <u>10.1. Ermittlung von Switchtyp und Managementversion</u> WEB: Device Info Console Show: > sh:ow inf:o SNMP OID: NEXANS-BM-MIB → infoMgmtFirmwareVersion
Backup Firmware-Version (nur HW5 Switches)	Kapitel: <u>10.1. Ermittlung von Switchtyp und Managementversion</u> WEB: Device Info Console Show: > sh:ow inf:o SNMP OID: -
Switch Info	
Description	Kapitel: <u>10.1. Ermittlung von Switchtyp und Managementversion</u> WEB: Device Info Console Show: > sh:ow inf:o SNMP OID: NEXANS-BM-MIB → infoDescr
Switchtype	Kapitel: <u>10.1. Ermittlung von Switchtyp und Managementversion</u> WEB: Device Info Console Show: > sh:ow inf:o SNMP OID: NEXANS-BM-MIB → infoType
MAC Address	Kapitel: <u>10.1. Ermittlung von Switchtyp und Managementversion</u> WEB: Device Info Console Show: > sh:ow inf:o SNMP OID: NEXANS-BM-MIB → adminAgentPhysAddress
Part Number (P/N)	Kapitel: <u>10.1. Ermittlung von Switchtyp und Managementversion</u> WEB: Device Info Console Show: > sh:ow inf:o SNMP OID: NEXANS-BM-MIB → infoProductNo
Switch Hardwareversion	Kapitel: <u>10.1. Ermittlung von Switchtyp und Managementversion</u> WEB: Device Info Console Show: > sh:ow inf:o SNMP OID: NEXANS-BM-MIB → infoSwitchHardwareVersion
Production Lot	Kapitel: <u>10.1. Ermittlung von Switchtyp und Managementversion</u> WEB: Device Info Console Show: > sh:ow inf:o SNMP OID: NEXANS-BM-MIB → infoSerie
Series Number (S/N)	Kapitel: <u>10.1. Ermittlung von Switchtyp und Managementversion</u> WEB: Device Info Console Show: > sh:ow inf:o SNMP OID: NEXANS-BM-MIB → infoSeriesNo

Manufacturing Date	Kapitel: <u>10.1. Ermittlung von Switchtyp und Managementversion</u> WEB: Device Info Console Show: > sh:ow inf:o SNMP OID: NEXANS-BM-MIB → infoManufactureDate
PoE Adapter Info	
Description	Kapitel: <u>11. Funktionsbeschreibung PoE (Power-over-Ethernet)</u> WEB: Device Info Console Show: > sh:ow inf:o SNMP OID: -
Part Number (P/N)	Kapitel: <u>11. Funktionsbeschreibung PoE (Power-over-Ethernet)</u> WEB: Device Info Console Show: > sh:ow inf:o SNMP OID: -
Adapter Hardwareversion	Kapitel: <u>11. Funktionsbeschreibung PoE (Power-over-Ethernet)</u> WEB: Device Info Console Show: > sh:ow inf:o SNMP OID: -
Production Lot	Kapitel: <u>11. Funktionsbeschreibung PoE (Power-over-Ethernet)</u> WEB: Device Info Console Show: > sh:ow inf:o SNMP OID: -
Series Number (S/N)	Kapitel: <u>11. Funktionsbeschreibung PoE (Power-over-Ethernet)</u> WEB: Device Info Console Show: > sh:ow inf:o SNMP OID: -
Manufacturing Date	Kapitel: <u>11. Funktionsbeschreibung PoE (Power-over-Ethernet)</u> WEB: Device Info Console Show: > sh:ow inf:o SNMP OID: -
Memory Card Info	
Card Type	Kapitel: <u>4. Memory Card (MC)</u> WEB: Device Info Console Show: > sh:ow inf:o SNMP OID: -
Write-Protection (DIP F2) (nur HW5 iSwitches)	Kapitel: <u>4. Memory Card (MC)</u> WEB: Device Info Console Show: > sh:ow inf:o SNMP OID: -
MAC Address	Kapitel: <u>4. Memory Card (MC)</u> WEB: Device Info Console Show: > sh:ow inf:o SNMP OID: -

Licence	Kapitel: <u>4. Memory Card (MC)</u> WEB: Device Info Console Show: > sh:ow inf:o SNMP OID: -
---------	---

9.10. Port Setup

Bezeichnung	Zugriff
Port Global	
Name	Kapitel: <u>10.40. Port Name</u> 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	Kapitel: <u>10.41. Port Typ</u> WEB: Port State → Setup Console Show: > sh:ow con:figuration in:terfaces [a:ll] SNMP OID: -
Port Link-Setup	
Link Type	Kapitel: <u>10.20.1. Link-Typ</u> 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-protect} SNMP OID: NEXANS-BM-MIB → portLinkType
Admin State	Kapitel: <u>10.20.2. Admin State</u> 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	Kapitel: <u>10.20.3. Shutdown if no link</u> WEB: - Console Show: > sh:ow con:figuration in:terfaces [a:ll] 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	Kapitel: <u>10.20.4. Speed / Duplex Setup</u> 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	Kapitel: <u>10.20.8. Autocrossover/Autopolarity</u> 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	Kapitel: <u>10.24. Remote Fault</u> 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	Kapitel: <u>10.22. Send Link Alarms</u> WEB: - Console Show: > sh:ow con:figuration in:terfaces [a:ll] Console Set: # in:terface {if-no range} link-a:alarm {e:nabled d:isabled} SNMP OID: -
Automatic Powersave	Kapitel: <u>10.20.5 Automatic Powersave</u> 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	Kapitel: <u>10.20.6 Energy-Efficient Ethernet (EEE)</u> 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	Kapitel: <u>10.20.7 Extended Powersave</u> 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	Kapitel: <u>10.20.9. Client Remove Alarm</u> 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)	Kapitel: <u>10.20.9. Client Remove Alarm</u> 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	Kapitel: <u>11.1.2. PoE Power Setup</u> 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)	Kapitel: <u>11.1.3. PoE Powerlimit pro Port</u> 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	Kapitel: <u>10.36. Portsecurity</u> <u>10.59. Portsecurity mit Authentifizierung per RADIUS Server</u> 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: {d:isabled 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:uppllicant} SNMP OID: NEXANS-BM-MIB → portSecurityAdminState
MAC Address 1	Kapitel: <u>10.36. Portsecurity</u> 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	Kapitel: <u>10.36. Portsecurity</u> 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	Kapitel: <u>10.36. Portsecurity</u> 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	Kapitel: <u>10.59.7. Portsecurity Option {Toggle Link}</u> WEB: - Console Show: > sh:ow con:figuration ra:dus [a:ll] Console Set: # rad:ius l:ink-interrupt i:nterface <if-no> {e:nabled d:isable} SNMP OID: -
Renew	Kapitel: <u>10.36.5. Portsecurity – Renew-Befehl</u> WEB: - Console Set: in:terface {if-no range} se:curity-mode re:new SNMP OID: NEXANS-BM-MIB → portSecurityAdminState
Port Prioritisation	
Default 802.1p Priority Level (Queue)	Kapitel: <u>10.38.5. Port Default 802.1p Priorityvalue</u> 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	Kapitel: <u>10.38.2Priorisierung nach IEEE802.1p</u> 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	Kapitel: <u>10.38.3. IEEE802.1p VLAN based Priority Override</u> 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	Kapitel: <u>10.38.4. Priorisierung nach IPv4/IPv6</u> 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	Kapitel: <u>10.42. Programmierung der Port Status-</u> 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	Kapitel: <u>10.42. Programmierung der Port Status-</u> 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	Kapitel: <u>10.43. Bandwidth-Limiter</u> 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	Kapitel: <u>10.43. Bandwidth-Limiter</u> 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	Kapitel: <u>10.43.2. Limiter Packet Type</u> 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

Bezeichnung	Zugriff
IPv4 Setup	
DHCP enable	Kapitel: <u>10.8. Konfiguration der IP- und VLAN-Parameter</u> 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	Kapitel: <u>7.2.5. Switch-Konfiguration automatisch per DHCP/BootP und TFTP laden</u> 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	Kapitel: <u>10.8. Konfiguration der IP- und VLAN-Parameter</u> 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	Kapitel: <u>10.8. Konfiguration der IP- und VLAN-Parameter</u> 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	Kapitel: <u>10.8. Konfiguration der IP- und VLAN-Parameter</u> 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	Kapitel: <u>10.8. Konfiguration der IP- und VLAN-Parameter</u> WEB: - Console Show: > sh:ow d:hcp Console Set: - SNMP OID: NEXANS-BM-MIB → adminAgentDhcpServerIpAddress
IPv6 Setup	
IPv6 Access Mode	Kapitel: <u>10.8. Konfiguration der IP- und VLAN-Parameter</u> 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: {d:isable s:tatic-address au:to-stateless pr:ivacy- auto-stateless dh:cpv6} SNMP OID:

IPv6 Link Local Address	Kapitel: <u>10.8. Konfiguration der IP- und VLAN-Parameter</u> WEB: Switch Setup Console Show: > sh:ow con:figuration ip [a:ll] Console Set: n/a SNMP OID:
IPv6-Address	Kapitel: <u>10.8. Konfiguration der IP- und VLAN-Parameter</u> 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	Kapitel: <u>10.8. Konfiguration der IP- und VLAN-Parameter</u> 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	Kapitel: <u>10.8. Konfiguration der IP- und VLAN-Parameter</u> 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	Kapitel: <u>10.8. Konfiguration der IP- und VLAN-Parameter</u> WEB: - Console Show: > sh:ow d:hcp Console Set: - SNMP OID:

9.12. Management > Agent

Bezeichnung	Zugriff
Reset Action	
Reboot (Cold Start)	Kapitel: <u>3.6.1. Booten mit Flash Konfiguration (Normalbetrieb)</u> WEB: Switch Setup → Reset Command → Reboot (Cold Start) Console Set: # rel:oad SNMP OID: NEXANS-BM-MIB → adminReset → rebootSwitch
Reboot with Factory Default	Kapitel: <u>8. Rücksetzen auf Werkseinstellungen</u> WEB: Switch Setup → Reset Command → Reboot with Factory Default Console Set: # rel:oad factory-a:ll SNMP OID: NEXANS-BM-MIB → adminReset → rebootToFactoryDefaults
Reboot with Factory Default (Except IP Parameters)	Kapitel: <u>8. Rücksetzen auf Werkseinstellungen</u> WEB: Switch Setup → Reset Command → Reboot with Factory Default Console Set: # rel:oad factory-w:ithout-ip SNMP OID: -
Reboot without customer reboot settings	Kapitel: <u>8. Rücksetzen auf Werkseinstellungen</u> WEB: - Console Set: # rel:oad w:ithout-cust-reboot SNMP OID: -

Reboot with customer default settings	Kapitel: <u>8. Rücksetzen auf Werkseinstellungen</u> WEB: - Console Set: # rel:oad c:ust-default SNMP OID: -
Reset Total Boots Counter	Kapitel: <u>8. Rücksetzen auf Werkseinstellungen</u> WEB: Switch Setup → Reset Command → Reset Total Boots Counter Console Set: # res:et b:oots SNMP OID: -
Reset Port Counters	Kapitel: <u>10.27. Reset all Port Counters</u> 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	Kapitel: <u>8. Rücksetzen auf Werkseinstellungen</u> WEB: Switch Setup → Reset Command → Reset Total Operation Time Console Set: # res:et o:peration-time SNMP OID: -
Reset Local Logging	Kapitel: <u>8. Rücksetzen auf Werkseinstellungen</u> WEB: Local Log → Delete Log Console Set: # sh:ow l:og [delete] SNMP OID: -
Reset Firmware on Memory Card	Kapitel: <u>4.5 Memory Card Firmware-Update</u> 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	Kapitel: <u>8. Rücksetzen auf Werkseinstellungen</u> WEB: - Console Set: # N/A SNMP OID: -
Switch to backup firmware (nur HW5 Switche)	Kapitel: <u>7.1.1 Duale Firmware-Speicherung</u> WEB: - Console Set: # rel:oad b:ackup-firmware SNMP OID: -
Memory Card Mode	Kapitel: <u>4.6 Memory Card Mode</u> 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)	Kapitel: <u>10.3. Switch Name / Location / Contact / Domain</u> 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)	Kapitel: <u>10.3. Switch Name / Location / Contact / Domain</u> 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)	Kapitel: <u>10.3. Switch Name / Location / Contact / Domain</u> 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)	Kapitel: <u>10.3. Switch Name / Location / Contact / Domain</u> 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	Kapitel: <u>10.45. Layer-2 Discovery Functionen</u> WEB: - Console Show: > sh:ow con:figuration ag:ent [a:ll] Console Set: # co:nfig li:fepacket-rate {1min 10min 1h 10h d:isabled a:ll-disabled} SNMP OID: -
Basic Configurator	Kapitel: <u>10.45.2 Basic Configurator abschalten</u> 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

Bezeichnung	Zugriff
Admin Account Setup (Read/Write)	
Admin Name	Kapitel: <u>10.5. Admin / User Accounts beim Management</u> Zugriff 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	Kapitel: <u>10.5. Admin / User Accounts beim Management</u> Zugriff 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	Kapitel: <u>10.5. Admin / User Accounts beim Management</u> Zugriff 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	Kapitel: <u>10.5. Admin / User Accounts beim Management</u> Zugriff 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	Kapitel: <u>10.5. Admin / User Accounts beim Management</u> Zugriff 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	Kapitel: <u>10.5. Admin / User Accounts beim Management</u> Zugriff 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	Kapitel: <u>10.5. Admin / User Accounts beim Management</u> Zugriff 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	Kapitel: <u>10.6 Passwort Encryption</u> 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	Kapitel: <u>10.7 Passwort strength checker</u> 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:disable} SNMP OID: -
Minimum password length	Kapitel: <u>10.7 Passwort strength checker</u> 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	Kapitel: <u>10.18 Global Access / Access policy</u> WEB: - Console Show: # sh:ow con:figuration acce:ss [a:ll] Console Set: # co:nfig g:lobal-security m:ode {e:nabled d:disable} SNMP OID:
Accesslist Setup	
Accesslist Mode	Kapitel: <u>10.19. Accesslist / Accesslist-Mode</u> 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:disable m:anager-only s:nmp-only a:ll} SNMP OID: NEXANS-BM-MIB → adminMgmtAccessList

Accesslist IPv4	Kapitel: <u>10.19. Accesslist / Accesslist-Mode</u> WEB: - Console Show: # show configuration access [a:ll] Console Set: # accesslist (1..16) <ip-addr-1> <ip-addr-2> {mode} Valid values for {mode} are: {read-write read-only none} SNMP OID: -
Accesslist IPv6	Kapitel: <u>10.19. Accesslist / Accesslist-Mode</u> WEB: - Console Show: # show configuration access [a:ll] Console Set: # ipv6 access-list (1..8) <ipv6-addr-1> <ipv6-addr-2> {access-mode} Valid values for {access-mode} are: {read-write read-only none} SNMP OID: -
Manager Setup	
Manager authentication mode	Kapitel: <u>10.10. Manager Authentication Mode</u> WEB: - Console Show: # show configuration access [a:ll] Console Set: # config manager-auth-mode {mode} Valid values for {mode} are: {none local radius both-radius-local disabled} SNMP OID: -
Console Setup	
Telnet authentication mode	Kapitel: <u>10.48 Telnet Console Authentication Mode</u> WEB: - Console Show: # show configuration access [a:ll] Console Set: # config telnet-auth-mode {mode} Valid values for {mode} are: {local radius both-radius-local tacacs+ both-tacacs+-local disable-telnet} SNMP OID: -
SSHv2 authentication mode	Kapitel: <u>10.49. SSHv2 Console Authentication Mode</u> WEB: - Console Show: # show configuration access [a:ll] Console Set: # config ssh-auth-mode {mode} Valid values for {mode} are: {local radius both-radius-local tacacs+ both-tacacs+-local disable-ssh} SNMP OID: -
SCP authentication mode	Kapitel: <u>10.50 SCP Authentication Mode</u> WEB: - Console Show: # show configuration access [a:ll] Console Set: # config scp-auth-mode {setup} Sets the SCP authentication mode or disables the SCP interface. Valid values for {setup} are: {use-ssh-mode local radius both-radius-local tacacs+ both-tacacs+-local disable} SNMP OID: -

V.24 authentication mode	Kapitel: <u>10.14. V.24 Console Authentication Mode</u> WEB: - Console Show: # show configuration access [a:ll] Console Set: # config v2:4-auth-mode {mode} Valid values for {mode} are: {l:ocal r:adius both-r:adius-local t:acacs+ both-t:acacs+-local d:disable-v24} SNMP OID: -
Console password mode	Kapitel: <u>10.15. Console Password Mode</u> WEB: - Console Show: # show configuration access [a:ll] Console Set: # config console-p:assword-mode {i:nvisible v:isible} SNMP OID: -
Encrypt passwords in CLI	Kapitel: <u>10.16 Encrypt password mode</u> WEB: - Console Show: # show configuration access [a:ll] Console Set: config console-e:ncryption {d:isabled e:nabled} SNMP OID: -
Console logout time (seconds)	Kapitel: <u>10.17 Console logout time</u> WEB: - Console Show: # show configuration access [a:ll] Console Set: config console-l:ogout-timeout (5...65535) SNMP OID: -
WEB Setup	
Refresh Rate for State pages	Kapitel: - WEB: Switch Setup Console Show: # show configuration access [a:ll] Console Set: # config web-r:efresh-rate {setup} Valid values for {setup} are: {d:isabled 5:sec 10:sec 30:sec} SNMP OID: -
HTTP authentication mode	Kapitel: <u>10.11.1. HTTP Authentication Mode</u> WEB: - Console Show: # show configuration access [a:ll] Console Set: # config web-a:uth-mode {l:ocal r:ead-only d:disable-web} SNMP OID: -
HTTP TCP port	Kapitel: <u>10.11.2. HTTP TCP Port</u> WEB: - Console Show: # show configuration access [a:ll] Console Set: # config web-t:cp-port (1...65535) SNMP OID: -
HTTPS authentication mode	Kapitel: <u>10.12.1. HTTPS Authentication Mode</u> WEB: - Console Show: # show configuration access [a:ll] Console Set: # config https-a:uth-mode {setup} Valid values for {setup} are: {l:ocal r:ead-only d:disable-https} SNMP OID: -

HTTPS TCP port	Kapitel: <u>10.12.2. HTTPS TCP Port</u> 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	Kapitel: <u>10.12.3. HTTPS Allowed TLS Versions</u> 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	Kapitel: <u>7.5 TFTP Authentifizierung per SNMP</u> 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	Kapitel: <u>3.5 Management Konfigurationsschalter deaktivieren</u> 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	Kapitel: <u>3.5 Management Konfigurationsschalter deaktivieren</u> 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

Bezeichnung	Zugriff
SNMP Global Setup	
SNMP protocol version	Kapitel: <u>10.53.1. SNMP Protocol Version</u> 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	Kapitel: <u>10.53.2. SNMP Access Mode</u> 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)	Kapitel: <u>10.53.3. SNMPv1/v2c Communities</u> 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)	Kapitel: <u>10.53.3. SNMPv1/v2c Communities</u> 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)	Kapitel: <u>10.53.3. SNMPv1/v2c Communities</u> 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	Kapitel: <u>10.53.4. SNMPv1 MAC Table Mode</u> 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)	Kapitel: <u>10.53.5. SNMPv3 Engine ID</u> 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	
Username (max 32 chars)	Kapitel: <u>10.53.6. SNMPv3 User Setup</u> WEB: - Console Show: # sh:ow con:figuration acce:ss [a:ll] Console Set: # snm:p v:3 u:username w:rite-read [<string max. 32 chars>] SNMP OID: -

Authentication password (8...32 chars)	Kapitel: <u>10.53.6. SNMPv3 User Setup</u> WEB: - Console Show: # sh:ow con:figuration acce:ss [a:ll] Console Set: # snm:p v:3 pa:ssword w:rite-read [<string max. 32 chars>] SNMP OID: -
Privacy password (8...32 chars)	Kapitel: <u>10.53.6. SNMPv3 User Setup</u> 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	
Username (max 32 chars)	Kapitel: <u>10.53.6. SNMPv3 User Setup</u> 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: -
Authentication password (8...32 chars)	Kapitel: <u>10.53.6. SNMPv3 User Setup</u> WEB: - Console Show: # sh:ow con:figuration acce:ss [a:ll] Console Set: # snm:p v:3 pa:ssword r:ead [<string max. 32 chars>] SNMP OID: -
Privacy password (8...32 chars)	Kapitel: <u>10.53.6. SNMPv3 User Setup</u> 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)	Kapitel: <u>10.53.6. SNMPv3 User Setup</u> 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)	Kapitel: <u>10.53.6. SNMPv3 User Setup</u> 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)	Kapitel: <u>10.53.6. SNMPv3 User Setup</u> WEB: - Console Show: # sh:ow con:figuration acce:ss [a:ll] Console Set: # snm:p v:3 pa:ssword f:lexible [<string 8...32 chars>] SNMP OID: -
Privacy password (8...32 chars)	Kapitel: <u>10.53.6. SNMPv3 User Setup</u> 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)	Kapitel: <u>10.53.6. SNMPv3 User Setup</u> WEB: - Console Show: # sh:ow con:figuration acce:ss [a:ll] Console Set: # snm:p v:3 u:ername t:rap [<string max. 32 chars>] SNMP OID: -
Authentication password (8...32 chars)	Kapitel: <u>10.53.6. SNMPv3 User Setup</u> 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)	Kapitel: <u>10.53.6. SNMPv3 User Setup</u> 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 IEC61850

Bezeichnung	Zugriff
IEC 61850 Global Setup	
IEC 61850 access mode	Kapitel: <u>10.79. IEC61850 Protokoll Unterstützung</u> 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

Bezeichnung	Zugriff
Banner Setup	
Banner	Kapitel: 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

Bezeichnung	Zugriff
Zero Touch Configuration Setup	
Zero Touch Configuration Mode	Kapitel: 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	Kapitel: 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	Kapitel: 7.3 Zero Touch Configuration WEB: - Console Show: # sh:ow zero-:touch-config Console Set: - SNMP OID: -

9.19. Management > Skripting

Bezeichnung	Zugriff
Skripting Setup	
Script File Content	Kapitel: 7.4 Skripting WEB: - Console Show: > sh:ow cli-script [{n:o-pause d:delete}] 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

Bezeichnung	Zugriff
LED Setup	
Global LED Mode	Kapitel: <u>10.33 Global LED Mode</u> 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	Kapitel: <u>10.32. VLAN Portmirror</u> 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	Kapitel: <u>10.34. Portmonitor</u> WEB: Port Monitor Console Show: > sh:ow con:figuration g:lobal [a:ll] Console Set: # co:nfig mo:nitor m:ode {d:isable r:x-only t:x-only b:oth} SNMP OID: -
Portmonitor → Source-Port	Kapitel: <u>10.34. Portmonitor</u> 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	Kapitel: <u>10.34. Portmonitor</u> 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)	Kapitel: <u>10.39. Address Ageing Time der Fowarding Tabelle</u> 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	Kapitel: <u>10.44. Flow Control</u> 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

Bezeichnung	Zugriff
VLAN Table Global Setup	
VLAN Table Mode	Kapitel: <u>10.31.2. VLAN Table Mode</u> 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 → adminSwitchVlanTableModel
Tagging Ethertype	Kapitel: <u>10.31.6. Tagging Ethertype</u> 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	Kapitel: <u>10.31.3 Fabric Attach</u> 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)	Kapitel: <u>10.31.1. VLAN Table</u> 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:etele (1...4095) SNMP OID: NEXANS-BM-MIB → vlanId
VLAN Name (0...50 chars)	Kapitel: <u>10.31.1. VLAN Table</u> 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	Kapitel: <u>10.31.10 Port VLAN-Tagging</u> 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 = Anzahl der Ports)	Kapitel: <u>10.31.10 Port VLAN-Tagging</u> 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	Kapitel: <u>10.38.3. IEEE802.1p VLAN based Priority Override</u> 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	Kapitel: <u>10.31.3 Fabric Attach</u> 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

Bezeichnung	Zugriff
VLAN Port Setup	
Default VLAN-ID (1...4095, 0 disables VLAN)	Kapitel: <u>10.31.8. Port Default-VLAN-ID</u> 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)	Kapitel: <u>10.31.9. Port Voice-VLAN-ID</u> 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	Kapitel: <u>10.31.7. Port Trunking Mode</u> 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	Kapitel: <u>10.31.5 Pro-Port VLAN Port Isolation</u> 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	Kapitel: <u>10.31.4. Globale VLAN Port Isolation</u> 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)	Kapitel: <u>10.31.15. RADIUS Unsecure VLAN-ID</u> 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)	Kapitel: <u>10.31.16. RADIUS Guest VLAN-ID</u> 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)	Kapitel: <u>10.31.17. RADIUS Inaccessible VLAN-ID</u> 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)	Kapitel: <u>10.31.18. IEEE802.1X Authentication Failure VLAN-ID</u> 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

Bezeichnung	Zugriff
Link-Layer-Discovery-Protocol Setup (IEEE802.1AB)	
LLDP Mode	Kapitel: <u>10.70. Link Layer Discovery Protocol (LLDP)</u> 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)	Kapitel: <u>10.70. Link Layer Discovery Protocol (LLDP)</u> WEB: - Console Show: > sh:ow con:figuration di:scovey [a:ll] Console Set: # co:nfig lldp-i:nterval (5..32678) SNMP OID: -
TX Holdtime Multiplier	Kapitel: <u>10.70. Link Layer Discovery Protocol (LLDP)</u> WEB: - Console Show: > sh:ow con:figuration di:scovey [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	Kapitel: <u>10.71. LLDP for Media Endpoint Devices (LLDP-MED)</u> WEB: - Console Show: > sh:ow con:figuration di:scovey [a:ll] Console Set: # co:nfig lldp-me:d layer2-p:riority (0..7) SNMP OID: -
Layer 3 Voice DSCP value	Kapitel: <u>10.71. LLDP for Media Endpoint Devices (LLDP-MED)</u> WEB: - Console Show: > sh:ow con:figuration di:scovey [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	Kapitel: <u>10.71. LLDP for Media Endpoint Devices (LLDP-MED)</u> WEB: - Console Show: > sh:ow con:figuration di:scovey [a:ll] Console Set: # co:nfig lldp-me:d layer2-s:ig-priority (0..7) SNMP OID: -
Layer 3 Voice Signaling DSCP value	Kapitel: <u>10.71. LLDP for Media Endpoint Devices (LLDP-MED)</u> WEB: - Console Show: > sh:ow con:figuration di:scovey [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)	Kapitel: <u>10.71. LLDP for Media Endpoint Devices (LLDP-MED)</u> WEB: - Console Show: > sh:ow con:figuration di:scovey [a:ll] Console Set: # co:nfig lldp-me:d lo:cation-id b:uilding [<string 1...50 chars>] SNMP OID: -
Unit (25)	Kapitel: <u>10.71. LLDP for Media Endpoint Devices (LLDP-MED)</u> WEB: - Console Show: > sh:ow con:figuration di:scovey [a:ll] Console Set: # co:nfig lldp-me:d lo:cation-id u:nit [<string 1...50 chars>] SNMP OID: -

Place Type (29)	Kapitel: <u>10.71. LLDP for Media Endpoint Devices (LLDP-MED)</u> WEB: - Console Show: > show configuration discovery [a:ll] Console Set: # config lldp-med location-id place-type [string 1...50 chars] SNMP OID: -
Cisco-Discovery-Protocol Setup (IEEE802.1AB)	
CDP Mode	Kapitel: <u>10.72. Cisco Discovery Protocol (CDP)</u> WEB: - Console Show: > show configuration discovery [a:ll] Console Set: # config cdp-mode {setup} Valid values for {setup} are: {disabled filter-disabled enabled forward-enabled lldp-enabled} SNMP OID: -
TX Message Interval (seconds)	Kapitel: <u>10.72. Cisco Discovery Protocol (CDP)</u> WEB: - Console Show: > show configuration discovery [a:ll] Console Set: # config cdp-interval (5..255) SNMP OID: -
TX Holdtime (seconds)	Kapitel: <u>10.72. Cisco Discovery Protocol (CDP)</u> WEB: - Console Show: > show configuration discovery [a:ll] Console Set: # config cdp-holdtime (10..255) SNMP OID: -

9.24. Prioritisation

Bezeichnung	Zugriff
Prioritisation Global Setup	
Priority Scheme	Kapitel: <u>10.38.1. Priorisierungsschema</u> WEB: - Console Show: > show configuration prioritisation [a:ll] Console Set: # config priority-scheme {setup} Valid values for {setup} are: strict weighted-fair mixed-strict-q3 mixed-strict-q2:-and-q3 SNMP OID: -
Priority Setup IEEE802.1p	
Priority Setup: 802.1p	Kapitel: <u>10.38.2. Priorisierung nach IEEE802.1p</u> WEB: 802.1p Priority Console Show: > show configuration prioritisation [a:ll] Console Set: # config priority-dot1p (priority value=0..7) (queue=0..3) SNMP OID: -

Priority Setup IPv4/IPv6

Priority Setup:	Kapitel: <u>10.38.4. Priorisierung nach IPv4/IPv6</u>
IPv4-DSCP-Diffserv	WEB: IPv4/Ipv6 Priority
IPv4-TOS	Console Show: > sh:ow con:figuration p:rriorisation [a:ll]
IPv6-Traffic-Class	Console Set: # co:nfig priority-i:p (priority value=0..63) (queue=0..3)
	SNMP OID: -

9.25. Alarms > Alarm Destinations

Bezeichnung	Zugriff
Alarm Destinations	
Test Traps/Syslog	Kapitel: <u>10.54. Alarm Destination Table</u> WEB: - Console Set: # te:st-traps-syslog SNMP OID: -
Syslog Severity	Kapitel: <u>10.54. Alarm Destination Table</u> 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: -
Syslog Facility	Kapitel: <u>10.54. Alarm Destination Table</u> WEB: - Console Show: # sh:ow con:figuration al:arms [a:ll] Console Set: # tr:ap-syslog f:acility (1...31) SNMP OID: -
Local Logging Mode	Kapitel: <u>10.54. Alarm Destination Table</u> 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: -
Destination Type	Kapitel: <u>10.54. Alarm Destination Table</u> WEB: - Console Show: # sh:ow con:figuration al:arms [a:ll] Console Set: # tr:ap-syslog t:type (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	Kapitel: <u>10.54. Alarm Destination Table</u> WEB: - 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	Kapitel: <u>10.54. Alarm Destination Table</u> WEB: - 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: all 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 port-s:ecu-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)	Kapitel: <u>10.29. Switch Temperatur</u> 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)	Kapitel: <u>10.29. Switch Temperatur</u> WEB: - Console Show: # sh:ow con:figuration al:arms [a:ll] Console Set: # co:nfig temp-h:igh-alarm (30..100) SNMP OID: -

Overttemperature Powersave Action	Kapitel: <u>10.29.2. Übertemperatur Powersave Funktion</u> WEB: - Console Show: # sh:ow con:figuration al:arms [a:ll] Console Set: # co:nfig o:verttemp-action {d:disable s:peed-eco} SNMP OID: -
PoE Input Alarm Setup	
PoE Power Source	Kapitel: <u>11.1.6. PoE Power Source</u> 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)	Kapitel: <u>11.1.4. PoE Input Power Limit</u> 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)	Kapitel: <u>11.1.5. PoE Input Voltage Alarm Limits</u> 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)	Kapitel: <u>11.1.5. PoE Input Voltage Alarm Limits</u> 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 Name	Kapitel: <u>10.46. Funktionseingänge bei Industrie und Office Switchen</u> WEB: - Console Show: # Console Set: # co:nfig io-input-n:ame {1..4} [<string max 32 chars>] SNMP OID: -
Function Input Alarm Mode	Kapitel: <u>10.46.1. Funktionseingang Alarm Mode</u> 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:disable 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 Remote Alarm Group	Kapitel: <u>10.46.1. Funktionseingang Alarm Mode</u> 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	Kapitel: <u>10.46. Funktionseingänge bei Industrie und Office Switchen</u> 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	Kapitel: <u>10.46.1. Funktionseingang Alarm Mode</u> 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	Kapitel: <u>10.46.1. Funktionseingang Alarm Mode</u> 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	Kapitel: <u>10.47 Alarmausgänge bei Industrie Switchen</u> 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	Kapitel: <u>10.47 Alarmausgänge bei Industrie Switchen</u> 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	Kapitel: <u>10.47 Alarmausgänge bei Industrie Switchen</u> 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	Kapitel: <u>10.47 Alarmausgänge bei Industrie Switchen</u> 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	Kapitel: <u>10.47 Alarmausgänge bei Industrie Switchen</u> 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	Kapitel: <u>10.47 Alarmausgänge bei Industrie Switchen</u> WEB: - Console Show: # sh:ow con:figuration al:arms [a:ll] Console Set: # co:nfig alarm1 remote-g:roup (0...255) SNMP OID: -
Industrial Link Down Alarms	
Link Down Alarm M1	Kapitel: <u>10.47 Alarmausgänge bei Industrie Switchen</u> WEB: Industrial Alarm Console Show: # sh:ow con:figuration al:arms [a:ll] Console Set: # in:terface {if-no range} alarm1 {e:nable d:disable} SNMP OID: -
Link Down Alarm M2	Kapitel: <u>10.47 Alarmausgänge bei Industrie Switchen</u> WEB: Industrial Alarm Console Show: # sh:ow con:figuration al:arms [a:ll] Console Set: # in:terface {if-no range} alarm2 {e:nable d:disable} SNMP OID: -

9.30. Alarms > SFP Alarms

SFP Alarms Limits Setup	
Laser Bias Current (mA) Upper Limit	Kapitel: <u>10.25. SFP Info, Diagnose und Alarme</u> WEB: - Console Show: # show configuration alarms [a:ll] Console Set: # interface {if-no range} sfp-b:ias-current-limit (0..1000) SNMP OID: NEXANS-BM-MIB → sfpAlarmTxBiasCurrentUpperLimit
TX Output Power (uW) Lower Limit	Kapitel: <u>10.25. SFP Info, Diagnose und Alarme</u> WEB: - Console Show: # show configuration alarms [a:ll] Console Set: # interface {if-no range} sfp-t:x-power-limit (0..1000) SNMP OID: NEXANS-BM-MIB → sfpAlarmTxOutputPowerLowerLimit
RX Input Power (uW) Lower Limit	Kapitel: <u>10.25. SFP Info, Diagnose und Alarme</u> WEB: - Console Show: # show configuration alarms [a:ll] Console Set: # interface {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	Kapitel: <u>10.36.1. Portsecurity - Failure Action</u> WEB: - Console Show: > show configuration global [a:ll] Console Set: # config security-action {mode} Valid values for {mode} are: {d:disable-port t:rap-syslog-only i:mediately-disable auth-fail-disable} SNMP OID: -
Re-enable time for Security-Disabled ports	Kapitel: <u>10.36.1. Portsecurity - Failure Action</u> WEB: - Console Show: > show configuration global [a:ll] Console Set: # config r:e-enable s:ecurity-disable (0...60000) SNMP OID: -
Re-enable time for Loop-Disabled ports	Kapitel: <u>10.36.1. Portsecurity - Failure Action</u> WEB: - Console Show: > show configuration global [a:ll] Console Set: # config r:e-enable l:oop-disable (0...60000) SNMP OID: -

Voice VLAN Authentication Mode	Kapitel: <u>10.36.2. Portsecurity - Voice VLAN Authentication Mode</u> 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)	Kapitel: <u>10.36.12. Portsecurity - MAC Adressen Ageing</u> WEB: - Console Show:> sh:ow con:figuration g:lobal [a:ll] Console Set: # co:nfig auto-a:geing (0 1..255) SNMP OID: -
Portsecurity ageing time for PC behind IP-Phone (minutes)	Kapitel: <u>10.36.12. Portsecurity - MAC Adressen Ageing</u> 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)	Kapitel: <u>10.36.12. Portsecurity - MAC Adressen Ageing</u> 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

Bezeichnung	Zugriff
Authentication Server Setup	
Server 1 Address Server 2 Address Server 3 Address Server 4 Address	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: # sh:ow con:figuration ra:dus [a:ll] Console Set: # rad:ius se:rver-ip (1 2 3 4) <ip-address> SNMP OID: -
Authentication UDP Port (1...65535)	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: # sh:ow con:figuration ra:dus [a:ll] Console Set: # rad:ius au:th po:rt (1...65535) SNMP OID: -
Shared secret (0...50 chars)	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: # sh:ow con:figuration ra:dus [a:ll] Console Set: # rad:ius au:th s:ecret [<string max 50 chars>] SNMP OID: -

Request timeout (1...255 sec.)	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: # sh:ow con:figuration ra:dus [a:ll] Console Set: # rad:ius t:imeout (1...255) SNMP OID: -
Request retries (0...255)	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: # sh:ow con:figuration ra:dus [a:ll] Console Set: # rad:ius ret:ries (0...255) SNMP OID: -
VLAN attribute	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: # sh:ow con:figuration ra:dus [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	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: # sh:ow con:figuration ra:dus [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	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: # sh:ow con:figuration ra:dus [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)	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: # sh:ow con:figuration ra:dus [a:ll] Console Set: # rad:ius ma:c-separator [<string max 1 char>] SNMP OID: -
Portsecurity password (0...50 chars) (Default = 'port')	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: # sh:ow con:figuration ra:dus [a:ll] Console Set: # rad:ius au:th pa:ssword <string 1 to 14 char> SNMP OID: -

Startup VLAN-ID	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius startup-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)	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius realm port [<string max 50 char.>] SNMP OID: -
Management Authentication	
Management realm (0...50 chars)	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius realm mgmt [<string max 50 char.>] SNMP OID: -
Global Realm Setup	
Realm location	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius realm location {p:refix s:uffix} SNMP OID: -
Realm separator (0...50 character)	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius realm separator [<string max 1 char>] SNMP OID: -

9.33. Security > RADIUS Management Authentication

Bezeichnung	Zugriff
Authentication Server Setup	
Management Authentication Mode	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius mgmt-auth mode {g:lobal-auth-settings m:gmt-auth-settings} SNMP OID: -
Server 1 Address Server 2 Address Server 3 Address Server 4 Address	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius mgmt-auth server-ip (1 2 3 4) <ip-address> SNMP OID: -

Authentication UDP Port (1...65535)	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius mg:mt-auth a:uth p:ort (1...65535) SNMP OID: -
Shared secret (0...50 chars)	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius mg:mt-auth a:uth s:ecret [<string max 50 chars>] SNMP OID: -
Request timeout (1...255 sec.)	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius mg:mt-auth t:imeout (1...255) SNMP OID: -
Request retries (0...255)	Kapitel: <u>10.55. RADIUS Authentication</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius mg:mt-auth r:etries (0...255) SNMP OID: -

9.34. Security > RADIUS Accounting

Bezeichnung	Zugriff
Accounting Enable	
IEEE802.1X accounting enable	Kapitel: <u>10.60. RADIUS Accounting</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius ac:counting do:t1x {e:nable d:isable} SNMP OID: -
MAC based accounting enable	Kapitel: <u>10.60. RADIUS Accounting</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius 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	Kapitel: <u>10.60. RADIUS Accounting</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius ac:counting ser:ver-ip (1 2 3 4) <ip-address> SNMP OID: -

Authentication UDP Port (1...65535)	Kapitel: <u>10.60. RADIUS Accounting</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius accounting port (1...65535) SNMP OID: -
Shared secret (0...50 chars)	Kapitel: <u>10.60. RADIUS Accounting</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius accounting sec:ret [<string max 50 chars>] SNMP OID: -
Request timeout (1...255 sec.)	Kapitel: <u>10.60. RADIUS Accounting</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius accounting t:imeout (1...255) SNMP OID: -
Request retries (0...255)	Kapitel: <u>10.60. RADIUS Accounting</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius accounting r:etries (0...255) SNMP OID: -
Accounting Options	
Alive packets enable	Kapitel: <u>10.60. RADIUS Accounting</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius accounting sen:d-alive-packets {e:nable d:isable} SNMP OID: -
Alive packets interval (1...240 minutes)	Kapitel: <u>10.60. RADIUS Accounting</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius accounting a:live-packets-intervall (1...240) SNMP OID: -
User-Name for 802.1X	Kapitel: <u>10.60. RADIUS Accounting</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius accounting 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	Kapitel: <u>10.60. RADIUS Accounting</u> WEB: - Console Show: # show configuration radius [a:ll] Console Set: # radius accounting di:scover-ip-address {setup} Valid values for {setup} are: {d:isabled f:ramed-ip-address} SNMP OID: -

9.35. Security > IEEE802.1X

Bezeichnung	Zugriff
IEEE802.1X Global Setup	
IEEE802.1X Transparency	Kapitel: <u>10.35. IEEE802.1X Transparenz</u> WEB: - Console Show: # sh:ow con:figuration do:t1x [a:ll] Console Set: # dot:1x t:ransparency {e:nable d:disable} SNMP OID: -
IEEE802.1X Authenticator Setup	
Re-Authentication enabled	Kapitel: <u>10.59. Portsecurity mit Authentifizierung per RADIUS Server</u> WEB: - Console Show: # sh:ow con:figuration do:t1x [a:ll] Console Set: # do:t1x rea:uthentication {e:nable d:disable} SNMP OID: -
Re-Authentication initial delay (seconds) (0...65535) (Set to 0 to use Re-authentication interval)	Kapitel: <u>10.59. Portsecurity mit Authentifizierung per RADIUS Server</u> 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)	Kapitel: <u>10.59. Portsecurity mit Authentifizierung per RADIUS Server</u> WEB: - Console Show: # sh:ow con:figuration do:t1x [a:ll] Console Set: # do:t1x rea:uthentication int:erval (1...65535) SNMP OID: -
Re-Authentication Inaccessible VLAN Mode	Kapitel: <u>10.59. Portsecurity mit Authentifizierung per RADIUS Server</u> 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)	Kapitel: <u>10.59. Portsecurity mit Authentifizierung per RADIUS Server</u> 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)	Kapitel: <u>10.59. Portsecurity mit Authentifizierung per RADIUS Server</u> 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)	Kapitel: <u>10.59. Portsecurity mit Authentifizierung per RADIUS Server</u> WEB: - Console Show: # show configuration dot1x [a:ll] Console Set: # dot1x request r:tries (0...255) SNMP OID: -
Max. Authentication retries (0...255)	Kapitel: <u>10.59. Portsecurity mit Authentifizierung per RADIUS Server</u> WEB: - Console Show: # show configuration dot1x [a:ll] Console Set: # dot1x authentication r:tries (0...255) SNMP OID: -
Radius MAC Bypass	Kapitel: <u>10.59.6. Portsecurity Option {IEEE802.1X Radius MAC Bypass}</u> WEB: - Console Show: # show configuration dot1x [a:ll] Console Set: dot1x m:ac-bypass {setup} Valid values for {setup} are: {d:disable e:enable s:single fallback-e:enable fallback-s:single immediate-e:enable immediate-fallback-e:enable immediate-fallback-s:single} SNMP OID: -
MAC bypass Quiet Time	Kapitel: <u>10.59. Portsecurity mit Authentifizierung per RADIUS Server</u> WEB: - Console Show: # show configuration dot1x [a:ll] Console Set: # dot1x m:ac-bypass q:uiet-time (0...65535) SNMP OID: -
EAP packets within Voice-VLAN	Kapitel: <u>10.59.8. Portsecurity Option {EAP Packets within Voice-VLAN}</u> WEB: - Console Show: # show configuration dot1x [a:ll] Console Set: # dot1x v:oice-vlan-eap-packets {t:agged u:ntagged} SNMP OID: -
IEEE802.1X Supplicant Setup	
MD5 Name (0...50 chars)	Kapitel: <u>10.59.9. Portsecurity Modus {IEEE802.1X Supplicant mit MD5}</u> WEB: - Console Show: # show configuration dot1x [a:ll] Console Set: # dot1x s:upplicant n:ame [<string max 50 chars>] SNMP OID: -
MD5 Password (0...50 chars)	Kapitel: <u>10.59.9. Portsecurity Modus {IEEE802.1X Supplicant mit MD5}</u> WEB: - Console Show: # show configuration dot1x [a:ll] Console Set: # dot1x s:upplicant p:assword [<string max 50 chars>] SNMP OID: -

9.36. Security > TACACS+ Authentication

Bezeichnung	Zugriff
Authentication Server Setup	
Server 1 Address	Kapitel: <u>10.61 TACACS+ Authentication</u>
Server 2 Address	WEB: -
Server 3 Address	Console Show: # sh:ow con:figuration t:acacs+ [a:ll]
Server 4 Address	Console Set: # ta:cacs+ authe:ntication ser:ver-ip (1...4) {<ip-address> di:sable}
	SNMP OID: -
Authentication TCP Port (1...65535)	Kapitel: <u>10.61 TACACS+ Authentication</u>
	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)	Kapitel: <u>10.61 TACACS+ Authentication</u>
	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.)	Kapitel: <u>10.61 TACACS+ Authentication</u>
	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	Kapitel: <u>10.61 TACACS+ Authentication</u>
	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

Bezeichnung	Zugriff
Authorization Server Setup	
Authorization Mode	Kapitel: <u>10.62 TACACS+ Authorization</u>
	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	Kapitel: <u>10.62 TACACS+ Authorization</u> 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	Kapitel: <u>10.62 TACACS+ Authorization</u> 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)	Kapitel: <u>10.62 TACACS+ Authorization</u> 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)	Kapitel: <u>10.62 TACACS+ Authorization</u> 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.)	Kapitel: <u>10.62 TACACS+ Authorization</u> 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	Kapitel: <u>10.62 TACACS+ Authorization</u> 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

Bezeichnung	Zugriff
Accounting Server Setup	
Accounting Mode	Kapitel: <u>10.63 TACACS+ Accounting</u> 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	Kapitel: <u>10.63 TACACS+ Accounting</u> 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)	Kapitel: <u>10.63 TACACS+ Accounting</u> 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)	Kapitel: <u>10.63 TACACS+ Accounting</u> 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.)	Kapitel: <u>10.63 TACACS+ Accounting</u> 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	Kapitel: <u>10.63 TACACS+ Accounting</u> 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

Bezeichnung	Zugriff
Access Control List Mode	
Enable Static	Kapitel: <u>10.68.6 Statische ACLs</u> 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	Kapitel: <u>10.68.7 Dynamische ACLs</u> WEB: - Console Show: # sh:ow acl d:ynamic Console Set: # acl dy:namic {e:nable d:isable} SNMP OID: -

Show ACL State	Kapitel: <u>10.68.9 ACL-Status</u> WEB: - Console Show: # sh:ow acl statu:s Console Set: # - SNMP OID: -
Access Control List Commands	
Access Control List Commands	Kapitel: <u>10.68.4 ACL-Definition</u> <u>10.68.3 ACL Regel-Definition</u> 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:etele (1..200) SNMP OID: -

9.40. Multicasts

Bezeichnung	Zugriff
IGMP Snooping Setup	
IGMP Snooping enable	Kapitel: <u>10.69.1. IGMP Snooping</u> 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)	Kapitel: <u>10.69.1. IGMP Snooping</u> 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	Kapitel: <u>10.69.1. IGMP Snooping</u> 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	Kapitel: <u>10.69.1. IGMP Snooping</u> 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	Kapitel: <u>10.69.1. IGMP Snooping</u> WEB: - Console Show: > sh:ow con:figuration ig:mp [a:ll] Console Set: # ig:mp s:nooping l:ease-mode {accept-u:ser-ports accept-a:ll i:gnore-all} SNMP OID: -
Clear Snoop Tables	Kapitel: <u>10.69.1. IGMP Snooping</u> WEB: - Console Set: # ig:mp s:nooping c:lear-tables SNMP OID: -
IGMP Querier Setup	
IGMP Querier enable	Kapitel: <u>10.69.2. IGMP Querier</u> 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)	Kapitel: <u>10.69.2. IGMP Querier</u> 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	Kapitel: <u>10.69.2. IGMP Querier</u> WEB: - Console Show: > sh:ow con:figuration ig:mp [a:ll] SNMP OID: -

9.41. Time Client > SNTP Setup

Bezeichnung	Zugriff
SNTP Client Setup	
Client enabled	Kapitel: <u>10.28.3. Network Time Protokoll - SNTP</u> 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	Kapitel: <u>10.28.3. Network Time Protokoll - SNTP</u> WEB: - Console Show: > sh:ow con:figuration s:ntp [a:ll] Console Set: # snt:p server-ip {<ip-address> di:sable} SNMP OID: -
Time server IP 2	Kapitel: <u>10.28.3. Network Time Protokoll - SNTP</u> 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)	Kapitel: <u>10.28.3. Network Time Protokoll - SNTP</u> 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)	Kapitel: <u>10.28.3. Network Time Protokoll - SNTP</u> WEB: - Console Show: > sh:ow con:figuration s:ntp [a:ll] Console Set: # snt:p v:ersion (1..4) SNMP OID: -

Accept SNTP broadcasts	Kapitel: <u>10.28.3. Network Time Protokoll - SNTP</u> WEB: - Console Show: > sh:ow con:figuration s:ntp [a:ll] Console Set: # snt:p b:roadcast {e:nable d:disable} SNMP OID: -
UTC local offset (minutes)	Kapitel: <u>10.28.3. Network Time Protokoll - SNTP</u> WEB: - Console Show: > sh:ow con:figuration s:ntp [a:ll] Console Set: # snt:p o:ffset (-720..720) SNMP OID: -
Summer time correction	Kapitel: <u>10.28.3. Network Time Protokoll - SNTP</u> WEB: - Console Show: > sh:ow con:figuration s:ntp [a:ll] Console Set: # snt:p su:mmertime {d:disable e:st} SNMP OID: -
Manual Time Request	Kapitel: <u>10.28.3. Network Time Protokoll - SNTP</u> WEB: - Console Set: # snt:p r:request-now SNMP OID: -

9.42. Time Client > Powersave Setup

Bezeichnung	Zugriff
Powersave Times	
End time hour	Kapitel: <u>10.20.5 Automatic Powersave</u> 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: -
Start time hour	Kapitel: <u>10.20.5 Automatic Powersave</u> 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

Bezeichnung	Zugriff
RSTP Global Setup	
Spanning Tree Global enable	Kapitel: <u>10.73.2. RSTP - Globale Konfigurationsparameter</u> 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	Kapitel: <u>10.73.2. RSTP - Globale Konfigurationsparameter</u> 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	Kapitel: <u>10.73.2. RSTP - Globale Konfigurationsparameter</u> 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)	Kapitel: <u>10.73.2. RSTP - Globale Konfigurationsparameter</u> 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	Kapitel: <u>10.73.2. RSTP - Globale Konfigurationsparameter</u> 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)	Kapitel: <u>10.73.2. RSTP - Globale Konfigurationsparameter</u> 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	Kapitel: <u>10.73.2. RSTP - Globale Konfigurationsparameter</u> 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	Kapitel: <u>10.73.3. RSTP - Port Konfigurationsparameter</u> 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	Kapitel: <u>10.73.2. RSTP - Globale Konfigurationsparameter</u> 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	Kapitel: <u>10.73.3. RSTP - Port Konfigurationsparameter</u> 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:disable b:pdu-disable} SNMP OID: BRIDGE-MIB → dot1dStpPortEnable
Priority	Kapitel: <u>10.73.3. RSTP - Port Konfigurationsparameter</u> 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	Kapitel: <u>10.73.3. RSTP - Port Konfigurationsparameter</u> 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	Kapitel: <u>10.73.3. RSTP - Port Konfigurationsparameter</u> 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	Kapitel: <u>10.73.3. RSTP - Port Konfigurationsparameter</u> 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	Kapitel: <u>10.73.3. RSTP - Port Konfigurationsparameter</u> 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	Kapitel: <u>10.73.4. RSTP - Globale Statusparameter</u> WEB: - Console Show: > sh:ow rs:tp SNMP OID: -
Root Bridge ID	Kapitel: <u>10.73.4. RSTP - Globale Statusparameter</u> WEB: - Console Show: > sh:ow rs:tp SNMP OID: BRIDGE-MIB → dot1dStpDesignatedRoot
Root Port	Kapitel: <u>10.73.4. RSTP - Globale Statusparameter</u> WEB: - Console Show: > sh:ow rs:tp SNMP OID: BRIDGE-MIB → dot1dStpRootPort
Root Cost	Kapitel: <u>10.73.4. RSTP - Globale Statusparameter</u> WEB: - Console Show: > sh:ow rs:tp SNMP OID: BRIDGE-MIB → dot1dStpRootCost
Learned Max Age	Kapitel: <u>10.73.4. RSTP - Globale Statusparameter</u> WEB: - Console Show: > sh:ow rs:tp SNMP OID: BRIDGE-MIB → dot1dStpMaxAge
Learned Hello Time	Kapitel: <u>10.73.4. RSTP - Globale Statusparameter</u> WEB: - Console Show: > sh:ow rs:tp SNMP OID: BRIDGE-MIB → dot1dStpHelloTime
Learned Forward Delay	Kapitel: <u>10.73.4. RSTP - Globale Statusparameter</u> WEB: - Console Show: > sh:ow rs:tp SNMP OID: BRIDGE-MIB → dot1dStpForwardDelay
Topology Changes	Kapitel: <u>10.73.4. RSTP - Globale Statusparameter</u> WEB: - Console Show: > sh:ow rs:tp SNMP OID: BRIDGE-MIB → dot1dStpTopChanges
Time since last Topology Change	Kapitel: <u>10.73.4. RSTP - Globale Statusparameter</u> WEB: - Console Show: > sh:ow rs:tp SNMP OID: BRIDGE-MIB → dot1dStpTimeSinceTopologyChange
RSTP Port Status	
State	Kapitel: <u>10.73.5. RSTP - Port Statusparameter</u> WEB: Port State Console Show: > sh:ow rs:tp SNMP OID: BRIDGE-MIB → dot1dStpPortState

Path Cost	Kapitel: <u>10.73.5. RSTP - Port Statusparameter</u> WEB: - Console Show: > sh:ow rs:tp SNMP OID: BRIDGE-MIB → dot1dStpPortPathCost BRIDGE-MIB → dot1dStpPortPathCost32
Designated Root	Kapitel: <u>10.73.5. RSTP - Port Statusparameter</u> WEB: - Console Show: > sh:ow rs:tp SNMP OID: BRIDGE-MIB → dot1dStpPortDesignatedRoot
Designated Cost	Kapitel: <u>10.73.5. RSTP - Port Statusparameter</u> WEB: - Console Show: > sh:ow rs:tp SNMP OID: BRIDGE-MIB → dot1dStpPortDesignatedCost
Designated Bridge	Kapitel: <u>10.73.5. RSTP - Port Statusparameter</u> WEB: - Console Show: > sh:ow rs:tp SNMP OID: BRIDGE-MIB → dot1dStpPortDesignatedBridge
Designated Port	Kapitel: <u>10.73.5. RSTP - Port Statusparameter</u> WEB: - Console Show: > sh:ow rs:tp SNMP OID: BRIDGE-MIB → dot1dStpPortDesignatedPort
Port Role	Kapitel: <u>10.73.5. RSTP - Port Statusparameter</u> WEB: - Console Show: > sh:ow rs:tp SNMP OID: -
Edge Port	Kapitel: <u>10.73.5. RSTP - Port Statusparameter</u> WEB: - Console Show: > sh:ow rs:tp SNMP OID: RSTP-MIB → dot1dStpPortOperEdgePort
Point-to-Point Link	Kapitel: <u>10.73.5. RSTP - Port Statusparameter</u> WEB: - Console Show: > sh:ow rs:tp SNMP OID: RSTP-MIB → dot1dStpPortOperPointToPoint
Spanning Tree Protocol detected	Kapitel: <u>10.73.5. RSTP - Port Statusparameter</u> WEB: - Console Show: > sh:ow rs:tp SNMP OID: -

9.44. Redundancy > Multiple Spanning Tree

Bezeichnung	Zugriff
Multiple Spanning Tree - Identifier Setup	
MSTP Name	Kapitel: <u>10.74.2. MSTP - Identifier Setup</u> 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	Kapitel: <u>10.74.2. MSTP - Identifier Setup</u> 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	Kapitel: <u>10.74.3. MSTP - Instance Setup</u> 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	Kapitel: <u>10.74.3. MSTP - Instance Setup</u> 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:etele SNMP OID: -
Bridge Priority	Kapitel: <u>10.74.3. MSTP - Instance Setup</u> 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

Bezeichnung	Zugriff
Link Aggregation - Global Setup	
Link Aggregation global enable	Kapitel: <u>10.75.2 Link Aggregation - Global Setup</u> 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	Kapitel: <u>10.75.2 Link Aggregation - Global Setup</u> WEB: - Console Show: > sh:ow con:figuration re:dundancy [a:ll] Console Set: # li:nk-aggr t:imeout {f:ast s:low} SNMP OID: -
Link Aggregation – Group Setup	
Mode	Kapitel: <u>10.75.3 Link Aggregation – Group Setup</u> 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	Kapitel: <u>10.75.3 Link Aggregation – Group Setup</u> 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	Kapitel: <u>10.75.3 Link Aggregation – Group Setup</u> 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:elate-port <if-no> SNMP OID: -

9.46. Redundancy > MRP

Bezeichnung	Zugriff
Media Ring Redundancy - Global Setup	
MRP global enable	Kapitel: 10.76 Media Redundancy Protocol (MRP) WEB: - Console Show: > sh:ow mr:p Console Set: # mrp mo:de {e:nabled d:isabled} SNMP OID: -
Max. Recovery Time	Kapitel: 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	Kapitel: 10.76 Media Redundancy Protocol (MRP) WEB: - Console Show: > sh:ow mr:p Console Set: # mrp i:nstance (0...4) ro:le {d:isable m:anager p:riority-manager c:lient} SNMP OID: -
Domain-ID	Kapitel: 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	Kapitel: 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	Kapitel: 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	Kapitel: 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:	Kapitel: 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:	Kapitel: 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

Zero loss global enable	Kapitel: <u>10.77 Zero loss</u> WEB: - Console Show: > sh:ow z:eroloss Console Set: # z:eroloss m:ode {e:nabled d:isabled} SNMP OID: -
Zero loss Port Setup	Kapitel: <u>10.77 Zero loss</u> 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: -
Zero loss Port Setup	Kapitel: <u>10.77 Zero loss</u> WEB: - Console Show: > sh:ow z:eroloss Console Set: # z:eroloss i:nterface <if-no> e:thertype (0x8800...0xFF) SNMP OID: -

9.48. DHCP Relay / Snooping

Bezeichnung	Zugriff
DHCP Snooping	
DHCP Snooping enable	Kapitel: <u>10.78.2 DHCP Snooping – Global Setup</u> 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: -
Re-enable time for DHCP Snooping Disabled ports (seconds)	Kapitel: <u>10.78.2 DHCP Snooping – Global Setup</u> 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	Kapitel: <u>10.78.3 DHCP Relay Agent</u> WEB: - Console Show: > sh:ow d:hcp r:elay Console Set: # dh:cp rela:y mo:de {e:nabled d:isabled} SNMP OID: -

10. Funktionsbeschreibung Switch

10.1. Ermittlung von Switchtyp und Managementversion

Der aktuelle Switchtyp und die installierte Management Firmware- und Hardwareversion kann über WEB, Telnet/SSH/V.24-Console, SNMP und NEXMAN abgefragt werden. Eine Liste aller unterstützten Switchtypen finden Sie im Kapitel 2.Switchausführungen.

HINWEIS:

Auf HW5-Switchen werden zwei Firmware-Versionen parallel auf verschiedenen Bootpartitionen gespeichert. Wenn ein Firmware-Update installiert wird, wird die aktuell ausgeführte Firmware als Backup gesichert und die installierte Firmware wird zur neuen ausgeführten Firmware (siehe Kapitel 7.1.1 Duale Firmware-Speicherung). Daher wird für HW5-Switche neben der Running-Firmware-Version auch die Backup-Firmware-Version in CLI und Manager angezeigt, die sich auf der anderen Boot-Partition befindet.

10.1.1. Abfrage per WEB

Menüpunkt **Device Info**:

The screenshot shows the 'Device Info' page in the Nexans Switch Management web interface. The page is divided into two main sections: 'Management Module' and 'Switch'.

Management Module	
Hardware version	5.20
Firmware version	HW5-F46-P10-INDUSTRIAL-V6.03ad
Uptime	0 days : 1 hours : 24 min : 23 sec
Total operation time	0 years : 3 days : 19 hours : 24 min
Time from Time server	13.11.2019 12:23:47
Active MAC address	00:C0:29:26:1E:C2
Total Boots	128

Switch	
Description	iGigaSwitch 1002 E+ SFP-2VI PRO4
Switchtype	85
MAC address	00:C0:29:26:1E:C2
Part number (PIN)	88306422
Hardware version	00
Serial number (S/N)	06422N000012
Manufacturing date	09.06.2017
Temperature	41 °C (OK)
Internal voltage 1	2.489 V (OK)
Internal voltage 2	3.303 V (OK)
Supply voltage S1	0 V
Supply voltage S2	53 V
Supply voltage S3	0 V

PoE Adapter	
Not installed	

Memory Card	
Not installed	

10.1.2. Abfrage per SNMP

SNMP-Variable 'infoType' bzw. 'infoMgmtFirmwareVersion' in der Private-MIB

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

10.1.3. Abfrage per Telnet/SSH/V.24-Console

Kommando **show info**:

Für HW5-Switche wird neben Parameter „Firmware-Version“ auch der Parameter „Backup-Firmware-Version“ für die Backup-Firmware angezeigt. In diesem Fall wird die Zeichenfolge "Firmware-Version" durch "Running Firmware-Version" ersetzt und die entsprechende Boot-Partition (1 oder 2) beider Versionen wird in eckigen Klammern hinter der Versionszeichenfolge angezeigt:

```

192.168.5.17 - PuTTY

AWR 10-Port Switch Linux#sh info

!--< SYSTEM INFO >--< MANAGEMENT MODULE >-----
!Hardware version          5.20
!Running firmware version  HW5-F46-P10-INDUSTRIAL-V6.03ad [Boot partition 1]
!Backup Firmware version   HW5-F46-P10-INDUSTRIAL-V6.03ad [Boot partition 2]
!Scheduled update          <none>
!Uptime                   0 days : 2 hours : 19 min : 6 sec
!Total operation time      0 years : 3 days : 20 hours : 19 min
!Time from Time server     13.11.2019 13:18:31
!Active MAC address        00:C0:29:26:1E:C2
!Total Boots               128

!--< SYSTEM INFO >--< SWITCH >-----
!Description               iGigaSwitch 1002 E+ SFP-2VI PRO4
!Switchtype                85
!MAC address               00:C0:29:26:1E:C2
!Part number (P/N)         88306422
!Hardware version          00
!Serial number (S/N)       06422N000012
!Manufacturing date        09.06.2017
!Temperature               40 degree celsius (OK)
!Internal voltage 1        2,506 V (OK)
--More-- press <space> / --Abort-- press <enter>

```

Für HW3-Switche und für Firmware-Versionen älter als V6.01ef wird nur der Parameter „Firmware-Version“ neben den Parametern „Switchtype“ und „Hardware version“ angezeigt:

```

192.168.5.77 - PuTTY

AWR 16-Port Switch Ubicom 2#sh info

!--< SYSTEM INFO >--< MANAGEMENT MODULE >-----
!Hardware version          3.31
!Firmware version          HW3-F30-P16-INDUSTRIAL-V5.04W 2019-10-31 18:07:01
!Scheduled update          <none>
!Uptime                   0 days : 4 hours : 52 min : 24 sec
!Total operation time      0 years : 17 days : 16 hours : 52 min
!Time from Time server     No time received from Time server
!Active MAC address        00:C0:29:0A:E6:60
!Total Boots               84

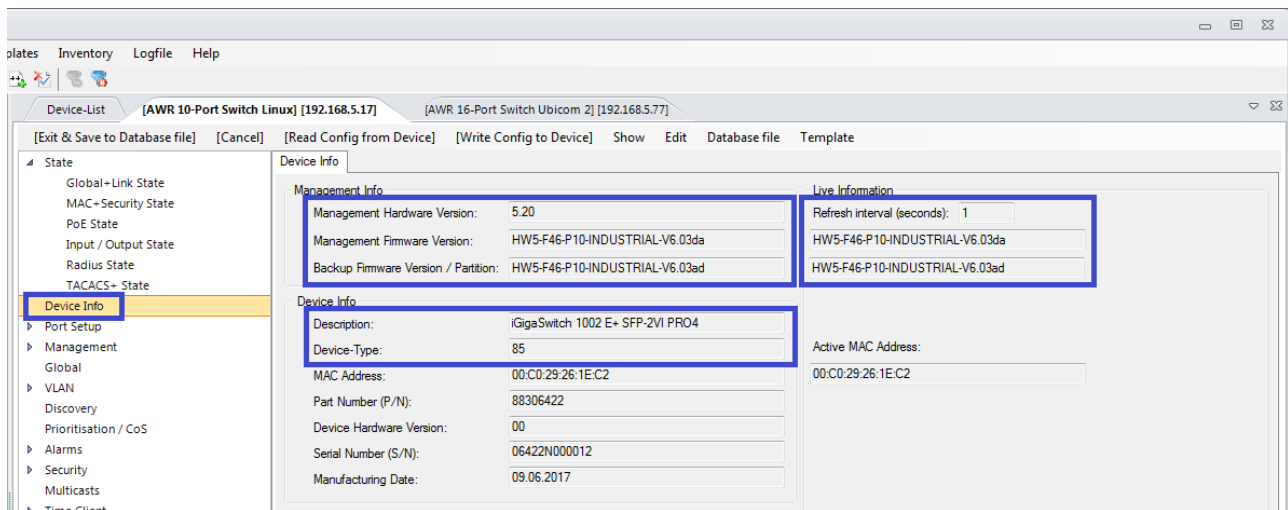
!--< SYSTEM INFO >--< SWITCH >-----
!Description               iGigaSwitch 160C E+ SFP-12VI PRO3
!Switchtype                42
!MAC address               00:C0:29:0A:E6:60
!Part number (P/N)         88306412
!Hardware version          02
!Serial number (S/N)       06412N000113
!Manufacturing date        29.09.2015
!Temperature               41 degree celsius (OK)
!Internal voltage 1        2,494 V (OK)
!Internal voltage 2        3,294 V (OK)
--More-- press <space> / --Abort-- press <enter>

```

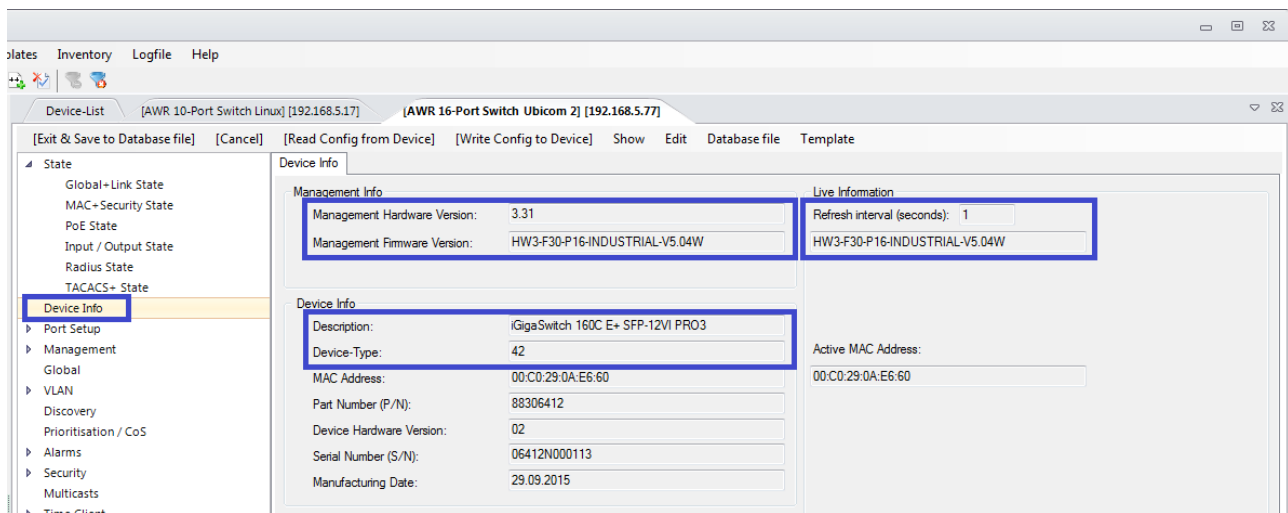
10.1.4. Abfrage per NEXMAN

Reiter Device Info:

Für HW5-Switche wird neben Parameter „Management Firmware Version“ auch der Parameter „Backup-Firmware-Version“ für die Backup-Firmware als Management Info und als Live Information angezeigt.



Für HW3-Switche und für Firmware-Versionen älter als V6.01ef wird nur der Parameter „Management-Firmware-Version“ neben den Parametern „Device-Type“ und „Management Hardware Version“ angezeigt:



10.2. Ermittlung der aktiven MAC Adresse

Die MAC Adresse, über die der Management Agent im Netzwerk ansprechbar ist, wird als 'Active MAC Address' bezeichnet. Dies ist bei Kabelkanal und Desk Switches grundsätzlich die auf dem Geräteaufkleber aufgedruckte MAC Adresse.

Bei Industrieswitches kann dies aber auch die MAC Adresse einer gesteckten Memory Card sein (siehe Kapitel 4. *Memory Card* (MC)). Da die MAC Adresse der Memory Card nur beim Booten des Switches übernommen wird, kann über die Anzeige der aktiven MAC Adresse eine eindeutige Aussage über die momentan verwendete MAC Adresse getroffen werden.

HINWEIS: Wenn der Switch mit der fixen IP Adresse gebootet wurde, sendet und empfängt er grundsätzlich mit der fixen MAC Adresse 00:C0:29:01:FF:FF. Als aktive MAC Adresse wird aber trotzdem die MAC Adresse angezeigt, die im normalen Betriebsmodus aktiv wäre.

10.3. Switch Name / Location / Contact / Domain

Im Switch werden folgende Informationen nichtflüchtig gespeichert:

- Name
- Location
- Contact
- Domain

Name:

Dies ist der zentrale Name des Switches. Er hat folgende zusätzliche Funktionen:

- er wird bei DHCP als 'hostname' eingetragen (Details siehe [5.3. Einstellung der IP-Adresse per DHCP](#))
- er wird in der NEXMAN Switchliste angezeigt und kann dort als Sortierkriterium verwendet werden
- er wird im Telnet/SSH/V.24Console-Prompt angezeigt

Location:

Hier kann z.B. der Einbauort des Switches eingetragen werden.

Contact:

Dient z.B. zur Angabe einer Kontaktadresse und/oder Telefonnummer des verantwortlichen Administrators.

Domain:

Dient zur Angabe einer übergeordneten Domain.

10.4. Banner

Es können 12 Zeilen a 80 Zeichen konfiguriert werden. Der Banner wird vor dem CLI, sowie vor dem WEB Login angezeigt. Folgende Zeichen stehen zur Verfügung:

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

10.5. Admin / User Accounts beim Management Zugriff

Grundsätzlich werden beim Web, Telnet/SSH/V.24-Console und NEXMAN Zugriff zwei Accounts unterschieden:

- Admin-Accounts: voller Read/Write Zugriff auf alle Einstellungen
- User-Account: nur Read/Only Zugriff erlaubt

Die Factory-Default Einstellungen sind:

- Admin-Account: Name = admin Password = nexans
- Admin-1...5 Account: Deaktiviert
- User-Account: Name = user Password = nexans

Wurde ein falscher Login-Name bzw. ein falsches Passwort eingegeben, so wird bei der Telnet/SSH/V.24-Console und beim NEXMAN eine Fehlermeldung ausgegeben bzw. beim Web das leere Login Fenster erneut angezeigt.

Für den Admin-1 Account können zusätzlich folgende Zugriffsrechte konfiguriert werden:

- Read/Write for all parameters
- Read/Only for all parameters except Port-Monitor on WEB

Read/Write for all parameters:

Der Admin-1 Account hat volle Read/Write Zugriffsrechte.

Read/Only for all parameters except Port-Monitor on WEB:

Der Admin-1 Account hat grundsätzlich nur Read/Only Rechte, mit einer Ausnahme:

Die Port-Monitor Einstellung für "Mode" und "Source Port" kann per WEB Interface konfiguriert werden. Der "Destination-Port" kann dabei nicht verändert werden und muss daher von einem Admin Account mit vollen Read/Write Zugriffsrechten voreingestellt sein.

Folgende ASCII Zeichen sind für Name und Passwort zulässig und werden in den Eingabemasken von WEB, CLI und Manager überprüft:

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

Die einzigen Ausnahmen sind die folgenden ASCII Zeichen:

? (ASCII 63) Wird im CLI Interface grundsätzlich als Hilfe-Kommando interpretiert

` (ASCII 96) Hier muss der Benutzer die Tastenfolge <shift + `> + <space> drücken, was nicht praktikabel ist

10.6. Passwort Encryption

Die Speicherung der lokalen Passwörter für den Admin- und User-Account kann auf vier Arten erfolgen:

- Standard Proprietäres Verfahren
- DES DES Encryption
- MD5-Hash Modifizierter MD5-Hash Algorithmus

- SHA1-Hash Modifizierter SHA1-Hash Algorithmus
- SHA256-Hash Modifizierter SHA256-Hash Algorithmus

Standard (Factory-Default):

Hier werden die lokalen Passwörter nach einem proprietären Encryptionverfahren im FLASH gespeichert. Für einen Hacker, der den Algorithmus kennt, wäre es möglich die Passwörter zu recovern.

DES:

Bei diesem Verfahren werden die Passwörter in verschlüsselte DES-Werte umgewandelt. Diese Einstellung ist notwendig, falls man den Manager Authentication Mode auf "Local via SNMPv3" konfiguriert hat und gleichzeitig CLI Konfigurationen laden möchte, die verschlüsselte Passwörter enthalten sollen.

MD5-Hash:**SHA1-Hash:****SHA256-Hash:**

Bei diesen beiden Verfahren werden die Passwörter in irreversiblen Hash-Werte umgewandelt und im Flash gespeichert.

Bei MD5 kommt dabei folgende Formel zur Anwendung:

Hash = "!" + base64(md5(<Clear-text password>))

Bei SHA1 wird folgender Algorithmus mit Salting verwendet:

Hash = "&" + base64(sha1(<Clear-text password> xor 0x0102..))

Bei SHA256 wird folgender Algorithmus verwendet:

Hash = "#" + base64(sha256(<Clear-text password>))

Die besondere Eigenschaft eines Hash-Wertes ist, dass es praktisch unmöglich ist aus diesem Hash das ursprüngliche Passwort zu berechnen. Bedingung ist allerdings, dass das Passwort eine ausreichende Länge und Komplexität hat (mindestens 8 Zeichen, bei erhöhten Anforderungen 12 Zeichen).

Sobald man den Encryption Mode von Standard oder DES auf MD5-, SHA1- oder SHA256-Hash umstellen, so werden die im Flash gespeicherten Passwörter automatisch in den Hash-Wert umgewandelt. Möchte man eines der Passwörter ändern, so gibt man im Manager, im WEB oder in der CLI Console das Klartext Passwort ein und der Switch wandelt dieses in den MD5- bzw. SHA1-Hash um.

Wenn man den "Password Encryption Mode" von MD5-, SHA1- oder SHA256-Hash auf einen anderen „Password Encryption Mode“ umstellt werden alle Passwörter auf Factory-Default gestellt.

An der CLI Console kann statt des Klartext Passwortes auch direkt der entsprechende Hash- oder DES-Wert angegeben werden. Dies ist hilfreich, wenn man CLI-Skripte erstellen möchte, die auch die Passwörter enthalten sollen. Falls der Encryption-Mode auf Standard eingestellt ist und man über die CLI Console eines der Passwörter per MD5-/SHA1-Hash oder DES-Wert konfiguriert, so wird der Encryption-Mode automatisch auf MD5, SHA1 bzw. DES umgestellt.

Über das Console Kommando "show config accounts" bzw. "show running-config" können die Hash- bzw. DES-Werte angezeigt werden um diese ggf. für ein Skript zu verwenden.

10.7. Passwort strength checker

Durch aktivieren des Password Strength Checker werden ausschließlich sichere Passwörter für den Admin und User Account vom Switch akzeptiert. Als sicher eingestuft werden Passwörter, die die folgenden Kriterien erfüllen:

8...14 Zeichen mit mindestens:

einem Kleinbuchstaben (a-z)

einem Großbuchstaben (A-Z)

einer Zahl (0-9)

einem Sonderzeichen (. , ; ! " # \$ % ^ ~ @ * : + - _ / \ | () [] { } < >)

Im Feld Minimum password length, gibt es die Möglichkeit die Mindestlänge der sicheren Passwörter zu definieren. Diese können zwischen 8 und 14 Zeichen lang sein. Die requirements bleiben hierbei erhalten.

Um den password strength checker über den NEXMAN zu aktivieren und diese Konfiguration auf den Switch zu schreiben, muss gleichzeitig ein sicheres Passwort für den Admin Account definiert sein. Ist dies nicht der Fall, wird der User vor dem Schreiben der Konfiguration aufgefordert ein sicheres Passwort einzugeben.

Ist beim Login per CLI oder WEB ein unsicheres Passwort aktiv, so wird zunächst eine Änderung des Passwortes erzwungen bevor man den Switch konfigurieren kann. Wird sich mit dem User Account eingeloggt, so kann nur das sichere Passwort für den User Account gesetzt werden. Auch dies ist nach der Anmeldung Pflicht.

10.8. Konfiguration der IP- und VLAN-Parameter

Konfigurationsänderungen an den IP- und VLAN-Parametern, die per Telnet/SSH/V.24-Console, Web oder SNMP vorgenommen werden, sind nicht sofort wirksam, sondern erst nach Ausführen des Befehls {Renew IP- and VLAN-Parameter}.

So können zunächst alle gewünschten IP- und VLAN-Einstellungen vorgenommen werden, bevor diese tatsächlich aktiviert werden. Dies verhindert, dass eine halbfertige Konfiguration den Switch in einen undefinierten Zustand bringt.

Für detaillierte Informationen zur Einstellung der IP- und VLAN-Parameter siehe Kapitel [5. Einstellung der IP-Adresse](#) bzw. [10.31 VLAN Unterstützung](#).

10.9. ARP Tabelle

Die ARP Tabelle des Switch Managment kann ausschließlich per CLI angezeigt bzw. gelöscht werden. Das entsprechende Kommando lautet:

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

10.10. Manager Authentication Mode

Für den NEXMAN Zugriff können im Switch folgende Authentifizierungs-Modi eingestellt werden:

- | | |
|--|---|
| • SCP – Use SCP authentication mode setting: | Authentifizierung via SCP |
| • UDP/TFTP – No authentication (Ignores Username and Password) | Keine Authentifizierung |
| • UDP/TFTP – Local Accounts | Lokale Authentifizierung |
| • UDP/TFTP – Radius Only | Authentifizierung ausschließlich durch den RADIUS Server |
| • UDP/TFTP – Radius first, then Local Accounts | Authentifizierung durch RADIUS, nur falls kein Server antwortet: lokale Authentifizierung |
| • SNMPv3 – Local Accounts | Lokale Authentifizierung |
| • Disable Manager access | Manager Zugriff per UDP, TFTP und SNMPv3 abgeschaltet |

SCP – Use SCP authentication mode setting:

Es wird der Authentication Mode benutzt unter Console Setup als SCP authentication mode eingetragen ist.

UDP/TFTP – No authentication (Ignores Username and Password):

Bei dieser Einstellung erwartet der Switch für den Zugriff per NEXMAN keine Authentifizierung. Außerdem wird in diesem Modus der direkte Zugriff auf den Switch per TFTP-Programm ermöglicht. Vor der Inbetriebnahme des Switches kann so z.B. ein Update bzw. Downgrade der Firmware durchgeführt werden, ohne dass ein Passwort übermittelt werden muss. Beim späteren Betrieb des Switches im Netzwerk sollte jedoch aus Sicherheitsgründen ein anderer Modus eingestellt werden. Beim Zugriff durch den NEXMAN wird zusätzlich eine Warnung im Logfenster ausgegeben, die darauf hinweist, dass dieser unsichere Modus eingestellt ist.

HINWEIS:

Eine Einschränkung des Zugriffs durch den NEXMAN kann bei der Einstellung {none} ausschließlich über die Accessliste erfolgen (siehe Kapitel [10.19. Accesslist / Accesslist-Mode](#)).

UDP/TFTP – Local Accounts:

Im Switch ist je ein Name und ein Passwort für den Admin- und User-Access gespeichert (siehe Kapitel [10.5. Admin / User Accounts beim Management](#) Zugriff). Diese Daten werden zur Authentifizierung des NEXMAN Zugriffs herangezogen und mit dem eingegebenen Login-Namen und Login-Passwort verglichen.

UDP/TFTP – Radius Only:

UDP/TFTP – Radius first, then Local Accounts:

Diese Modi sind ausschließlich bei Firmware-Versionen mit RADIUS Unterstützung auswählbar. Siehe Kapitel [10.57. RADIUS Manager Authentication Modes](#)

SNMPv3 – Local Accounts:

Bei diesem Mode werden, wie beim Mode " UDP/TFTP – Local Accounts:", die lokalen Passwörter zur Authentifizierung verwenden. Hier erfolgt die Authentifizierung und der anschließende Dateitransfer ausschließlich per SNMPv3.

Disable Manager access:

Der Manager Zugriff per UDP und TFTP ist komplett abgeschaltet. Diese Einstellung kann ausschließlich per CLI Kommando "**config manager-auth-mode disable**" konfiguriert werden.

10.11. HTTP Setup

Grundsätzliche Hinweise zur Konfiguration per WEB-Browser befinden sich im Kapitel 6.2. Switch Konfiguration mittels Web-Browser (HTTP / HTTPS).

10.11.1. HTTP Authentication Mode

Für HTTP können folgende Modi eingestellt werden:

- Local: Lokale Authentifizierung
- Read/Only Lokale Authentifizierung, ausschließlich Read/Only Zugriff erlaubt
- HTTP disabled: HTTP Interface disabled

Local (Factory-Default):

Im Switch ist je ein Name und ein Passwort für den Admin- und User-Access gespeichert (siehe Kapitel 10.5. Admin / User Accounts beim Management Zugriff). Diese Daten werden per Factory-Default beim HTTP Login zur Authentifizierung herangezogen und mit dem eingegebenen Login-Namen und Login-Passwort verglichen.

Read/Only:

Wie bei der Einstellung {Local} werden hier die lokalen Namen und Passwörter verwendet. Allerdings wird grundsätzlich nur Read/Only Access erlaubt.

HINWEIS: Auch wenn man sich mit dem korrekten Admin-Namen/Passwort anmeldet, wird nur Read/Only Access gewährt.

HTTP disabled:

Das HTTP Interface ist abgeschaltet. Ein Verbindungsaufbau auf dem TCP-Port des Web Interfaces wird vom Switch abgelehnt.

HINWEIS:

Nach dreimaliger falscher Eingabe von Name oder Passwort, werden alle WEB Interfaces (HTTP und HTTPS) für 60 Sekunden gesperrt.

10.11.2. HTTP TCP Port

Der TCP Port für den HTTP Zugriff kann im Bereich 1...65535 konfiguriert werden. Per Factory Default ist der Standard Port 80 voreingestellt.

10.12. HTTPS Setup

Grundsätzliche Hinweise zur Konfiguration per WEB-Browser befinden sich im Kapitel 6.2. Switch Konfiguration mittels Web-Browser (HTTP / HTTPS).

10.12.1. HTTPS Authentication Mode

Für den HTTPS Authentication können folgende Modi eingestellt werden:

- Local: Lokale Authentifizierung
- Read/Only Lokale Authentifizierung, ausschließlich Read/Only Zugriff erlaubt
- HTTPS disabled: HTTPS Interface disabled

Local (Factory-Default):

Im Switch ist je ein Name und ein Passwort für den Admin- und User-Access gespeichert (siehe Kapitel 10.5. Admin / User Accounts beim Management Zugriff). Diese Daten werden per Factory-Default beim Login zur Authentifizierung herangezogen und mit dem eingegebenen Login-Namen und Login-Passwort verglichen.

Read/Only:

Wie bei der Einstellung {Local} werden hier die lokalen Namen und Passwörter verwendet. Allerdings wird grundsätzlich nur Read/Only Access erlaubt.

HINWEIS: Auch wenn man sich mit dem korrekten Admin-Namen/Passwort anmeldet, wird nur Read/Only Access gewährt.

HTTPS disabled:

Das HTTPS Interface ist abgeschaltet.

HINWEIS:

Nach dreimaliger falscher Eingabe von Name oder Passwort, werden alle WEB Interfaces (HTTP und HTTPS) für 60 Sekunden gesperrt.

10.12.2. HTTPS TCP Port

Der TCP Port für den HTTPS Zugriff kann im Bereich 1...65535 konfiguriert werden. Per Factory Default ist der Standard Port 443 voreingestellt.

10.12.3. HTTPS Allowed TLS Versions

Die minimal zulässige TLS Version für den HTTPS Zugriff kann konfiguriert werden um einen gewünschten Sicherheitslevel sicherzustellen. Voraussetzung ist, dass der verwendete WEB Browser die konfigurierte TLS Version ebenfalls unterstützt.

Folgende Einstellungen stehen dabei zu Verfügung:

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

10.13. V.24 Console Interface

Die Konfiguration mittels V.24 Console Interface wird von allen Industrie-Switchen und von Desk-Switchen vom Typ 'GigaSwitch' unterstützt.

Für eine Übersicht der gültigen Console Kommandos siehe Kapitel 9. Liste der Status- und Konfigurationsparameter.

Für eine Beschreibung der Konfiguration mittels V.24 Console siehe Kapitel 6.3. Switch Konfiguration mittels V.24 Console.

10.14. V.24 Console Authentication Mode

Für die V.24-Console können sechs verschiedene Authentifizierungs-Modi eingestellt werden:

- | | |
|------------------------------|--|
| • Local: | Lokale Authentifizierung |
| • Disabled: | V.24-Console deaktiviert |
| • Radius only: | Authentifizierung ausschließlich durch den RADIUS Server |
| • Radius first, then local: | Authentifizierung durch RADIUS. Falls kein Server antwortet erfolgt eine lokale Authentifizierung |
| • TACACS+ only: | Authentifizierung ausschließlich durch den TACACS+ Server |
| • TACACS+ first, then local: | Authentifizierung durch TACACS+. Falls kein Server antwortet erfolgt eine lokale Authentifizierung |

Local (Factory-Default):

Im Switch ist je ein Name und ein Passwort für den Admin- und User-Access gespeichert (siehe Kapitel 10.5. Admin / User Accounts beim Management Zugriff). Diese Daten werden per Factory-Default beim V.24 Console Login zur Authentifizierung herangezogen und mit dem eingegebenen Login-Namen und Login-Passwort verglichen.

Disabled:

Ein Login an der V.24 Console ist nicht möglich.

Radius only:**Radius first, then local:**

Diese stehen ausschließlich bei den Firmware-Versionen mit RADIUS Unterstützung zur Verfügung.
Siehe Kapitel [10.56. RADIUS Console Authentication Modes](#).

TACACS+ only:

TACACS+ first, then local:

Diese stehen ausschließlich bei den Firmware-Versionen mit TACACS+ Unterstützung zur Verfügung.
Siehe Kapitel [10.64 TACACS+ Console Authentication Modes](#).

10.15. Console Password Mode

Über den 'Console Password Mode' kann eingestellt werden, ob das Passwort während der Telnet und V.24 Eingabe angezeigt wird oder nicht. Dies ist z.B. bei Verwendung eines RADIUS Servers sinnvoll, wenn One-Time-Passwörter verwendet werden und das eingegebene Passwort nur einmal verwendet werden kann.

Mögliche Einstellungen sind:

- Invisible (Default)
- Visible

10.16. Encrypt password mode

Die SNMPv1/v2 Communities, SNMP v3 Passwörter, RADIUS Secrets und TACACS+ Secrets können bei Aktivierung mit dem CLI Kommando „show running-config“ verschlüsselt ausgegeben werden. Die verschlüsselten Werte können dann als Eingabenwerte zum Konfigurieren der entsprechenden Parameter verwendet werden.

10.17. Console logout time

Setzt das inactivity timeout für die command line interface benutzung.

10.18. Global Access / Access policy

Durch das Einschalten der Access Policy, werden ausschließlich sichere Protokolle für den Zugriff per CLI, WEB, SNMP und Manager erlaubt. Gleichzeitig wird der Manager Authentication Mode auf 'SNMPv3' eingestellt, der Password Strength Checker aktiviert und der Password Encryption Mode auf MD5 konfiguriert (siehe Kapitel [10.7 Password strength checker](#)).

Zu den unsicheren Protokollen gehören:

TELNET, HTTP, SNMPv1, SNMPv2 und SNMPv3 ohne SHA-Auth. bzw. Encryption., Manager Access via UDP/TFTP

Verfügbar sind weiterhin die sicheren Protokolle:

SSHv2, HTTPS und SNMPv3 mit SHA-Auth. und DES-Encryption, Manager Access via SNMPv3 and SCP.

Bei Industrie Switches kann dieser Mode über den rückseitigen Schalter 3 (F1) bzw. über den frontseitigen Schalter F1 erzwungen werden, d.h., dieser Mode ist per Management Zugriff nicht abschaltbar.

10.19. Accesslist / Accesslist-Mode

Über eine 'Accessliste' kann festgelegt werden, welche IP-Adressen auf das Management des Switches zugreifen dürfen. Es können insgesamt 16 IP-Ranges angegeben werden, wobei jedem Eintrag Read/Write oder Read/Only Rechte zugeteilt werden können. Möchte man statt eines Ranges nur eine einzelne IP-Adresse angeben, so lässt man die 'Stop IP Address' leer.

Wird ein unzulässiger Zugriff erkannt, so wird bei den Firmware-Versionen mit SNMP-Agent, zusätzlich ein 'Authentication Failure Event' versendet, der die unzulässige IP-Adresse beinhaltet. Ferner wird die IP-Adresse in der SNMP-Variablen infoMgmtAuth eingetragen und kann per SNMP abgefragt werden.

Über den 'Accesslist Mode' kann festgelegt werden, für welche Art von Zugriff die Liste aktiviert wird. Folgende Einstellungen sind möglich:

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

Disabled:

Die Accessliste wird ignoriert

Enabled for Manager access only:

Die Accessliste wird ausschließlich für Zugriffe durch den NEXMAN aktiviert.

Falls der 'Manager Authentication Mode' auf {Local}, {Radius only} oder {Radius first, then local} eingestellt ist, muss beim NEXMAN Zugriff sowohl der Login-Name/Passwort korrekt sein als auch die IP-Adresse des Management-PC's in der Access-List aufgeführt sein.

Enabled for SNMP access only:

Die Accessliste wird ausschließlich für Zugriffe per SNMP aktiviert.

Beim SNMP-Zugriff muss sowohl die SNMP-Community korrekt sein, als auch die IP-Adresse des Management-PC's in der Access-List aufgeführt sein. Ansonsten antwortet der SNMP-Agent mit einem 'Authentication Failure'.

Enabled for all access:

Dieser Modus wendet die Accessliste auf alle Zugriffe an (NEXMAN, SNMP, Telnet und Web):

NEXMAN: Falls der 'Manager Authentication Mode' auf {Local}, {Radius only} oder {Radius first, then local} eingestellt ist, muss beim NEXMAN Zugriff sowohl der Login-Name/Passwort korrekt sein als auch die IP-Adresse des Management-PC's in der Access-List aufgeführt sein.

SNMP: Beim SNMP-Zugriff muss sowohl die SNMP-Community korrekt sein, als auch die IP-Adresse des Management-PC's in der Access-List aufgeführt sein. Ansonsten antwortet der SNMP-Agent mit einem 'Authentication Failure'.

Telnet: Beim Telnet-Zugriff muss sowohl der Login-Name/Passwort korrekt sein, als auch die IP-Adresse des Management-PC's in der Access-List aufgeführt sein.

Web: Beim Web-Zugriff muss sowohl der Login-Name/Passwort korrekt sein, als auch die IP-Adresse des Management-PC's in der Access-List aufgeführt sein.

10.20. Link Setup

Die folgenden Link Setup Parameter können für jeden Port separat konfiguriert werden:

- Link Type
- Admin State
- Speed/Duplex
- Autocross/Autopolarity

10.20.1. Link-Typ

Über den Link-Typ wird die Funktion des angeschlossenen Links konfiguriert. Dabei sind folgende Einstellungen möglich:

- Userport
- Userport with active Loop Protection
- Uplink / Downlink

Userport:

Diese Einstellung sollte gewählt werden, wenn an dem betreffenden Port ein fest installiertes Endgerät angeschlossen ist.

Userport with active Loop Protection:

Diese Einstellung sollte gewählt werden, wenn am Switch wechselnde Endgeräte angeschlossen werden und die Gefahr besteht, dass zwei Ports (versehentlich oder böswillig) kurzgeschlossen werden und dadurch eine Loop im Netzwerk entstehen könnte. Ferner werden Loops erkannt, die durch nachgeschaltete Hubs oder Switches verursacht werden.

Auf den betreffenden Ports werden dann in periodischen Abständen spezielle Loop-Protection-Pakete versendet und es wird geprüft, ob diese Pakete auf demselben oder einem anderen Port empfangen werden. Falls die Loop-Protection-Pakete über einen Uplink-Port oder User-Port mit aktiver Loop Protection empfangen werden, liegt eine Loop vor und der Port wird abgeschaltet. Darüber hinaus wird im Admin Status 'Disabled by Loop Detection' angezeigt (weitere Hinweise siehe Kapitel [10.20.2. Admin State](#)).

Abgeschaltete Ports können optional nach einer einstellbaren "Re-Enable Time for Loop-Disabled Ports" automatisch wieder aktiviert werden. Die Zeit ist dabei im Bereich von 1 bis 60 000 Sekunden konfigurierbar.

WICHTIG:

Damit Loops zuverlässig erkannt werden, darf das Management VLAN auf den betreffenden Ports nicht aktiviert sein.

HINWEIS:

Durch diese Funktion entsteht nach einem Link-Up eine zusätzliche Totzeit von ca. 5 Sekunden. Während dieser Zeit sendet der Switch bereits Loop-Protection-Pakete, jedoch wird jeder andere Traffic blockiert um im Falle eines Kurzschlusses eine temporäre Loop zu verhindern.

HINWEIS:

Diese Funktion ist nur aktivierbar, wenn Spanning Tree Global oder für den betreffenden Port deaktiviert ist.

Uplink / Downlink:

Alle Ports, die als Uplink zum zentralen Coreswitch bzw. als Downlink zum nachgeschalteten Switch dienen, sollten auf diesen Link Typ eingestellt werden.

Für diesen Port gelten dann folgende Besonderheiten:

- a) Der Port kann nicht abgeschaltet werden, weder manuell noch automatisch durch das Management. Sollte der Port bereits abgeschaltet sein, wird er automatisch wieder eingeschaltet.
- b) Beim Console Kommando 'sh:ow m:ac-address-table d:ynamic' werden die Adressen dieser Ports nicht angezeigt. Möchte man auch die Adressen an diesen Ports anzeigen, muss das Console Kommando um die Option 'a:ll' ergänzt werden.
- c) Für diese Ports werden keine 'Port Broadcast Failure' Events versendet, da am Uplink üblicherweise die Broadcasts vieler Endgeräte empfangen werden. Dies würde zu unnötigen und irreführenden Events führen.

10.20.2. Admin State

Über den Admin State kann der Port komplett abgeschaltet werden. Sofern für den betreffenden Port eine Security-Funktion aktiviert ist, kann eine Abschaltung auch automatisch durch das Management erfolgen.

Die folgende Übersicht zeigt die möglichen Zustände:

Admin State	
Bezeichnung	Funktion
Enabled	Der Port ist eingeschaltet und sendet ein Linksignal
Disabled	Der Port wurde vom Administrator manuell abgeschaltet und sendet kein Linksignal.
Disabled by Security Violation	Der Port wurde durch die aktivierte Portsecurityfunktion automatisch abgeschaltet. Im Falle einer automatischen Abschaltung wird außerdem ein 'Portsecurity-Failure' Event versendet
Disabled by Loop Detection	Der Port wurde automatisch abgeschaltet, weil die aktivierte 'Active Loop Protection' eine Loop erkannt hat. Im Fall einer automatischen Abschaltung wird außerdem ein 'Port-Loop-Detected' Event versendet.
Disabled by BPDU Detection	Der Port wurde automatisch abgeschaltet, weil für den betreffenden Port der Spanning Tree Mode „Disabled (BPDU disables Port)“ konfiguriert ist und auf diesem Port eine Spanning Tree BPDU empfangen wurde. Im Fall einer automatischen Abschaltung wird außerdem ein 'Port-Error-Disabled' Event versendet.
Disabled by Ring Loop Protection	Der Port wurde automatisch abgeschaltet, weil für den betreffenden Port der Spanning Tree Mode „Enabled (Ring Loop Protection)“ konfiguriert ist und eine Loop im Ring erkannt wurde. Im Fall einer automatischen Abschaltung wird außerdem ein 'Port-Error-Disabled' Event versendet.
Disabled by DHCP Snooping	Der Port wurde automatisch abgeschaltet, weil DHCP Snooping aktiviert ist und für den betreffenden Port der Link-Type auf „Userport“ oder „Userport with activ Loop Protection“ konfiguriert ist und auf diesem Port ein DHCP Paket von einem DHCP Server empfangen wurde. Im Fall einer automatischen Abschaltung wird außerdem ein 'Port-Error-Disabled' Event versendet.

10.20.3. Shutdown if no link

Über diese Funktion kann der Port, im Falle eines fehlenden Link Signals, automatisch abgeschaltet werden. Ist im Augenblick der Prüfung kein Link vorhanden, so wird der betreffende Port dauerhaft deaktiviert. Dies erfolgt indem der Admin State auf "Disabled" geschaltet wird. Diese Einstellung bleibt auch nach einem Reboot des Switches erhalten.

Folgende Einstellungen sind möglich:

- Disabled
- Check Link one time
- Check Link permanently
- Check Link permanently delayed

Disabled:

Eine automatische Abschaltung findet nicht statt.

Check Link one time:

Hier wird der Link ein einziges Mal überprüft, nämlich unmittelbar nach dem Setzen dieses Wertes.

Anschließend wird die Einstellung wieder auf "Disabled" zurückgesetzt.

Dieser Befehl ist insbesondere für CLI-Skripte oder Master-Configs sinnvoll um alle nicht beschalteten Ports aus Sicherheitsgründen abzuschalten.

Check Link permanently:

Hier wird der Link permanent überwacht und der Port innerhalb weniger Millisekunden nach Erkennen eines fehlenden Link Signals abgeschaltet.

Wird ein abgeschalteter Port per Management wieder einschaltet, muss innerhalb von 5 Sekunden ein Link Signal zustande kommen, ansonsten wird der Port erneut abgeschaltet.

Außerdem wird aus Sicherheitsgründen beim Reboot der Port abgeschaltet (auch falls vor dem Reboot das Link Signal vorhanden war).

Check Link permanently delayed:

Hier wird der Link permanent überwacht und der Port innerhalb weniger Millisekunden nach Erkennen eines fehlenden Link Signals abgeschaltet. Alternativ kann die Abschaltung jedoch verzögert erfolgen indem der „Client Remove Alarm“ für den betreffenden Port aktiviert wird. Die gewünschte Abschaltverzögerung wird in diesem Fall über das „Link Down Timeout“ konfiguriert. Bei aktiviertem „Client Remove Alarm“ wird bei erfolgter Abschaltung zusätzlich ein Client Remove Alarm versendet.

Wird ein abgeschalteter Port per Management wieder einschaltet, muss innerhalb von 5 Sekunden ein Link Signal zustande kommen, ansonsten wird der Port erneut abgeschaltet.

Weiterhin erfolgt nach einem Reboot die Überprüfung des Link Signals mit einer Verzögerung von 30 Sekunden. Dies verhindert z.B. eine Abschaltung des Ports nach einem Firmware-Update des Switches.

10.20.4. Speed / Duplex Setup

Die Einstellung 'Speed/Duplex Setup' bestimmt die zulässige Datenrate und den Duplex-Mode des betreffenden Ports.

Die folgende Übersicht zeigt die unterstützten Modi:

Speed/Duplex	
Bezeichnung	Funktion
Autoneg	Auto-Negotiation: Automatische Erkennung von Datenrate und Duplex-Mode. Dies ist die Factory-Default Einstellung für alle Twisted-Pair Ports.
ECO 10/100	Auto-Negotiation, jedoch wird kein 1 GigaBit/s Link zugelassen. Diese Einstellung wird ausschließlich von Gigabit Ports unterstützt, um die Leistungsaufnahme zu reduzieren. Dies ist z.B. für Endgeräte sinnvoll, die zwar einen Gigabit Link unterstützen, für die aber eine Datenrate von 100 MegaBits/s ausreichend ist. Ports, die unnötigerweise mit 1 GigaBit/s Link betrieben werden, benötigen nämlich eine um ca. 0,5 Watt höhere Leistung am Switch und am Endgerät. Dieser Mode kann zeitgesteuert aktiviert bzw. deaktiviert werden, um die Leistungsaufnahme in der Nacht oder am Wochenende zu reduzieren (siehe Kapitel 10.20.5 Automatic Powersave). Ferner können bei Übertemperatur alle Ports mit 1 GigaBit/s Link automatisch in diesen ECO Mode geschaltet werden (siehe Kapitel 10.29.2. Übertemperatur Powersave Funktion). HINWEIS: Dieser Mode wird nur von bestimmten Switchtypen unterstützt.
ECO 10/100 (Powersave)	Identische Funktionsweise wie 'ECO 10/100', jedoch wurde der ECO Mode automatisch aktiviert, weil für diesen Port eine automatische Powersave Funktion aktiviert ist. Für detaillierte Informationen siehe Kapitel 10.20.5 Automatic Powersave .
ECO 10/100 (Overtemp.)	Identische Funktionsweise wie 'ECO 10/100', jedoch wurde der ECO Mode automatisch aktiviert, weil die Temperatur des Switches den konfigurierten oberen Grenzwert überschritten hat. Für detaillierte Informationen siehe Kapitel 10.29.2. Übertemperatur Powersave Funktion .

1000 FDX	Feste Einstellung: 1 GigaBit/s - Full-Duplex Trotz fester Einstellung wird hier grundsätzlich die Autonegotiation Funktion für Speed und Flow-Control durchgeführt.
1000 FDX (Autoneg. disabled)	Feste Einstellung: 1 GigaBit/s - Full-Duplex Dieser Mode ist erforderlich, falls der Fiber Uplink an ein Gerät älterer Bauart angeschlossen wird (z.B. Fiber Converter). Hierbei wird die Autonegotiation Funktion für Speed und Flow-Control abgeschaltet da Autonegotiation von älteren Geräten u.U. nicht unterstützt wird.
100 FDX	Feste Einstellung: 100 MegaBit/s - Full-Duplex
100 HDX	Feste Einstellung: 100 MegaBit/s - Half-Duplex
10 FDX	Feste Einstellung: 10 MegaBit/s - Full-Duplex
10 HDX	Feste Einstellung: 10 MegaBit/s - Half-Duplex

WICHTIG:

Als Grundregel sollte beachtet werden, dass sowohl der Switchport als auch die Gegenseite (Endgerät bzw. Coreswitch) identisch eingestellt sein sollten, z.B. beide auf {Autoneg} oder beide fest auf {100FDX}.

HINWEIS:

Je nach Porttyp werden nur bestimmte Einstellungen unterstützt. Fiber-Optic Ports unterstützen z.B. grundsätzlich kein Autonegotiation.

10.20.5. Automatic Powersave

Über diese Funktion kann die Leistungsaufnahme des Ports automatisch reduziert werden.

Hier steht folgende Einstellung zur Verfügung:

- 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, die den Speed/Duplex Mode 'ECO 10/100' unterstützen, können zeitgesteuert auf diesen Mode geschaltet werden. Voraussetzung ist, dass der Port auf 'Autoneg' eingestellt ist und der Time Client eine gültige Uhrzeit von Time Server empfangen hat.

Set PoE Setup to 'Off' by Time Client:

Für Ports, die PoE (Power over Ethernet) unterstützen, kann die PoE-Spannung zeitgesteuert abgeschaltet werden. Voraussetzung ist, dass der Port nicht auf 'Off' eingestellt ist und der Time Client eine gültige Uhrzeit von Time Server empfangen hat.

Die Konfiguration der Zeitsteuerung für beide Modi erfolgt dabei global für alle entsprechend eingestellten Ports. Über das Powersave-Setup des Time Clients sind die Zeiten für jeden einzelnen Wochentag separat einstellbar.

Hier sind jeweils folgende Parameter konfigurierbar:

- Start time hour
- End time hour

Start time hour:

Dies ist die Uhrzeit (in vollen Stunden) zu der alle Twisted-Pair Ports, die auf den Speed/Duplex Mode 'Autoneg' eingestellt sind, automatisch in den Speed/Duplex Mode 'ECO 10/100 (Powersave)' geschaltet werden.

End time hour:

Dies ist die Uhrzeit (in vollen Stunden) zu der alle Twisted-Pair Ports, die auf den Speed/Duplex Mode 'ECO 10/100 (Powersave)' eingestellt sind, automatisch in den Speed/Duplex Mode 'Autoneg' geschaltet werden.

WICHTIG:

Wird eine Uhrzeit auf 0 eingestellt, so wird diese ignoriert. Möchte man z.B. für das Wochenende die Powersave Funktion aktivieren, so muss lediglich für Freitag die 'Start Time' konfiguriert werden (z.B. 18 Uhr) und für Montag die 'End Time' (z.B. 8 Uhr). Für Samstag und Sonntag können alle Zeiten auf 0 eingestellt bleiben.

10.20.6. Energy-Efficient Ethernet (EEE)

Bei HW5 Switchen kann die Powersave-Funktion Energy-Efficient Ethernet (EEE) für jeden Port separat eingeschaltet werden.

Diese Funktion aktiviert EEE für den betreffenden Port. Dabei wird bei Ports mit Gigabit Link die Datenrate auf 100 MegaBits/s reduziert, wenn diese für den Betrieb des angeschlossenen Endgeräts ausreicht (siehe Kapitel [10.20.4 Speed / Duplex Setup](#)).

HINWEIS:

Bei HW3 Switchen ist EEE standardmäßig eingeschaltet und kann nicht explizit eingestellt werden.

10.20.7. Extended Powersave

Bei bestimmten HW5 Switchen kann die Powersave-Funktion Extended Powersave für jeden Port separat eingeschaltet werden.

Ist diese Funktion aktiviert, wird zusätzlich zum Standard-EEE der Extended Powersave-Modus für den Port eingeschaltet. Dabei wird die Leistung des Ports reduziert, wenn für längere Zeit kein Link besteht. In regelmäßigen Abständen wird dann geprüft, ob die Leistung wieder hochgefahren und der Link wiederaufgebaut werden muss.

10.20.8. Autocrossover/Autopolarity

Diese Einstellung bestimmt, ob für den betreffenden Port eine automatische Kreuzung der TX und RX Aderpaare erfolgen soll (Autocrossover).

Sofern an den Port an ein 10 Mbit/s Endgerät angeschlossen ist, wird außerdem eine automatische Kreuzung des RX+/RX- Aderpaares vorgenommen (Autopolarity).

WICHTIGER HINWEIS:

Die Autocrossover Funktion sollte nur eingeschaltet werden, wenn gleichzeitig für Speed/Duplex 'Autoneg' oder 'ECO 10/100' eingestellt ist. Bei allen festen Einstellungen von Speed/Duplex ist, laut IEEE802-Standard, eine korrekte Linkerkennung nicht garantiert.

10.20.9. Client Remove Alarm

Mit dieser Funktion kann festgestellt werden, ob ein Endgerät dauerhaft vom Port entfernt wurde. Ist der Link des überwachten Ports für eine konfigurierbare Zeit (0...60000 Sekunden) auf Down, so wird ein "Client Remove Alarm" ausgelöst, der über die Alarm Destination Table verschickt werden kann, und ebenfalls im „Global+Link State“ des NEXMAN angezeigt wird. Dies gilt ebenfalls für Ports, die noch keinen aktiven Link hatten.

Wird die Link Down Zeit auf 0 eingestellt, so wird unmittelbar nach einem Link-Down ein Alarm versendet.

10.21. Link / EEE State

Der Link-Status zeigt die aktuelle Datenrate, den aktuellen Duplex-Mode und den Energy Efficient Ethernet (EEE) Status des betreffenden Ports an.

Die folgende Übersicht zeigt die möglichen Werte:

Link-Status	
Bezeichnung	Funktion
No Link	Es konnte kein gültiges Linksignal auf dem Port detektiert werden
Admin-Disabled	Der Port wurde vom Administrator per Management abgeschaltet.
Security-Disabled	Der Port wurde automatisch abgeschaltet, weil ein Portsecurity-Failure detektiert wurde (Siehe Kapitel 10.36.1. Portsecurity - Failure Action)
Loop-Disabled	Der Port wurde automatisch abgeschaltet, weil die aktivierte 'Active Loop Protection' einen Loop erkannt hat.
CLIENT-REMOVE-ALARM	Der Port wurde automatisch abgeschaltet, weil ein Client Remove Alarm ausgelöst wurde.
1000 FDX	1 GigaBit/s - Full-Duplex
1000 FDX / EEE	1 GigaBit/s - Full-Duplex und aktiviertem "Energy Efficient Ethernet (EEE)" Mode Dieser Mode wird nur dann aktiviert, falls der betreffende Switch und das angeschlossene Endgerät EEE unterstützen. HINWEIS: Im Device-Editor des Managers wird der EEE Status als separate Spalte auf dem Reiter "Global+Link State" angezeigt.

100 FDX	100 MegaBit/s - Full-Duplex
100 HDX	100 MegaBit/s - Half-Duplex
10 FDX	10 MegaBit/s - Full-Duplex
10 HDX	10 MegaBit/s - Half-Duplex

HINWEIS:

Bei der Speed/Duplex Einstellung 'Autoneg' und 'ECO 10/100' wird die Datenrate und der Duplex-Mode angezeigt, auf den sich der Switch und das angeschlossene Gerät per Autonegotiation geeinigt haben. Bei einem festen Link-Setup (z.B. 100 FDX) wird, bei einem gültigen Linksignal, grundsätzlich die Datenrate und der Duplex-Mode angezeigt, der beim Link-Setup eingestellt wurde.

10.22. Send Link Alarms

Diese Option ist im Auslieferungszustand aktiviert und bewirkt, dass für den betreffenden Port die Alarmtypen "Link Up", "Link Down" und "Link Change" versendet werden, vorausgesetzt, diese sind in der Alarm Destination Table ebenfalls aktiviert.

Wird diese Option deaktiviert, so werden für den betreffenden Port grundsätzlich keine Link Alarmer gesendet, auch dann nicht, wenn diese in der Alarm Destination aktiviert sind.

10.23. Kabel Diagnose bei Twisted-Pair Ports

Die Kabel-Diagnose Funktion ermöglicht die aktive Überprüfung von Twisted-Pair Ports in Bezug auf das angeschlossene Twisted-Pair Kabel. Selbst wenn am Port kein Link-Signal detektiert wird, lässt sich dennoch herausfinden, ob überhaupt ein Kabel angeschlossen ist und ob dieses am Ende offen ist oder ggf. einen Kurzschluss aufweist. Die Diagnose kann wahlweise für alle Ports oder für einen einzelnen Port gestartet werden.

Nach Start der Diagnose wird jedes verwendete Aderpaar einzeln gemessen (bei 100Mbit/s sind dies zwei Paare) und das Ergebnis mit Status 'open' (offenes Ende) bzw. 'short' (kurzgeschlossenes Ende) und der entsprechenden Entfernung angezeigt. Bei korrekt angeschlossener Gegenseite incl. richtiger Impedanzanpassung, wird als Status 'Good termination' angezeigt. Eine Leitungslänge kann in diesem Fall allerdings nicht bestimmt werden und wird deshalb mit 'n/a' (Not available) angezeigt.

ACHTUNG: Der Start der Kabel-Diagnose für einen Port mit aktivem Link-Signal führt zu einer Unterbrechung der Verbindung für ca. fünf Sekunden.

HINWEIS: Diese Funktion wird nur von bestimmten Switchtypen und Firmware-Versionen unterstützt.

10.24. Remote Fault

Diese Funktion wird ausschließlich für Fiber-Optic Ports unterstützt.

Bei eingeschalteter 'Remote Fault' Funktion wird der optische Sender des betreffenden Ports nur dann eingeschaltet, wenn ein optisches Eingangssignal empfangen wird.

Dies ist vor allem für zentrale Switches bzw. für Mediakonverter mit Managementfunktionen sinnvoll. Fällt nämlich an einer beliebigen Stelle ein Link aus, so wird dieser Ausfall bis zum zentralen Switch bzw. FiberCon durchgereicht und kann dort im Management als Link-Ausfall angezeigt werden.

Für detaillierte Erläuterungen ist das Handbuch des eingesetzten Switches zu beachten.

HINWEIS:

Zur einwandfreien Funktion müssen herstellersistenspezifische Linküberwachungsfunktion des zentralen Switches (z.B. UDLP) abgeschaltet werden.

10.25. SFP Info, Diagnose und Alarmer

SFP (Small Formfactor Pluggable) ist eine Spezifikation einer Generation von modularen optischen oder elektrischen Transceivern. SFP Module passen in einen speziellen SFP Slot und sind einfach und schnell austauschbar ("hot-swap"). Switches mit SFP Slots können daher leicht auf andere Medien umgestellt werden und sind im Falle eines Defektes schnell repariert.

SFP Module enthalten immer einen Speicher, der vom Hersteller programmiert wurde und Informationen über Hersteller, Typ usw. enthält. Spezielle SFP's enthalten darüber hinaus eine Diagnosefunktion, über die

Temperatur, Spannung, optische Leistungen und Laserstrom abgefragt werden können. Die aktuellen Switchtypen von Nexans unterstützen die Anzeige dieser Info und Diagnose Informationen.

Ferner können für die optischen Leistungen und für den Laserstrom Alarmlimits konfiguriert werden. Bei Verletzung dieser Limits wird dann ein sogenannter "SFP Event" per SNMP-Trap bzw. SYSLOG gesendet.

Folgende SFP Infos werden angezeigt:

- Vendor Name
- Revision Number
- Serial Number
- Date Code
- Bit Rate
- Wavelength (nm)
- Length 9µm (m)
- Length 50µm (m)
- Length 62.5µm (m)
- Connector Description

Folgende SFP Diagnosedaten angezeigt (sofern das betreffende SFP dies unterstützt):

- 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)

Folgende Alarme können konfiguriert werden:

- Transmitter Laser Bias Current, Upper Limit
- Transmitter Output Power, Lower Limit
- Received Input Power, Lower Limit

In der folgenden Tabelle sind die Kennwerte der gängigsten SFPs aufgelistet. Die in eckigen Klammern angegebenen Alarm Werte sind die empfohlenen Lower Limits für die "SFP Alarms" Konfiguration. Typisch sollte für RX Power eine Reserve von 3dB und für TX Power eine Reserve von 0dB eingehalten werden.

WICHTIG:

Die tatsächlichen Minimum und Maximum Werte für RX und TX Power, können, je nach Hersteller und SFP Typ, von den unten angegebenen Werten abweichen und sollten daher dem jeweiligen SFP Datenblatt entnommen werden. Für den Bias Current können meist keine konkreten Werte aus dem Datenblatt entnommen werden. Daher muss das Alarm Limit für den Bias Current, abhängig vom tatsächlich unter "Show SFP Info" angezeigten Wert, für jedes SFP individuell konfiguriert werden.

Nexans Artikel-Nr	Faser-typ	Wellenlänge TX/RX	Reichweite	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	Wellenlänge 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

Pro Port wird ein sogenannter Error Counter angezeigt, der die Summe aus folgenden Einzel-Countern darstellt:

- Rx FCS/CRC Error Packets
- Rx Alignment Error Packets
- Tx Late Collisions

Der Error-Counter dient primär zum Aufdecken von FDX/HDX Fehleinstellungen zwischen Switch und Endgerät. Liegt nämlich ein derartiger Fehler vor, zählt zumindest einer der Einzel-Counter hoch und erhöht somit auch den Error-Counter.

Die häufigsten Ursachen für eine Fehleinstellung sind

- Der Switchport steht auf {Autoneg} und das Endgerät fest auf {100FDX}
- Der Switchport steht fest auf {100FDX} und das Endgerät auf {Autoneg}

WICHTIG:

Als Grundregel sollte beachtet werden, dass sowohl der Switchport als auch die Gegenseite (Endgerät bzw. Coreswitch) identisch eingestellt sein sollten, z.B. beide auf {Autoneg} oder beide fest auf {100FDX}.

WICHTIG: Fehlerpakete, die meist durch ein-bzw. ausschalten von Endgeräten entstehen, werden unterdrückt. Ferner wird der Error-Counter nur um eins hoch gezählt falls innerhalb eines Zeitintervalls von zwei Sekunden FCS-Errors bzw. Late-Collisions aufgetreten sind. Dies verhindert, dass die absolute Anzahl der FCS bzw. Late-Collisions angezeigt wird. Diese können nämlich sehr hohe Werte annehmen, auch wenn der Fehlerzustand nur kurze Zeit bestand. Durch das Zeitintervall Verfahren, kann man genau ablesen, in wie vielen Zeitintervallen (zu zwei Sekunden) Fehler gezählt wurden und kann somit die Dauer des Problems besser erkennen

10.27. Reset all Port Counters

Durch den Befehl {Reset all Port Counters} werden folgende Counter auf 0 zurückgesetzt:

- Error Counter (siehe [10.26. Error Counter](#))
- Statistic Counter (siehe [10.52. Statistic- / RMON-Counter](#))

10.28. Switch Zeiten

10.28.1. System Up Time

Die 'System Up Time' zeigt die Betriebsdauer des Switches seit dem letzten Reboot an. Dies kann sowohl ein Software Reboot (z.B. durch Firmware Update) als auch ein Hardware Reboot (z.B. durch Einschalten der Betriebsspannung) sein.

10.28.2. Time since last link change

Hier wird pro Port die Zeit angezeigt, die seit der letzten Linkänderung (Link-Up oder Link-Down) des betreffenden Ports vergangen ist.

10.28.3. Network Time Protokoll - SNTP

Das Simple Network Time Protocol (SNTP) ist eine vereinfachte Version des NTP. Es wird im RFC 4330 beschrieben. Sofern ein entsprechender Time Server im lokalen Netzwerk erreichbar ist, kann über die Aktivierung des SNTP Clients im Switch, die aktuelle Uhrzeit in den Switch übernommen werden.

Diese Uhrzeit wird z.B. dazu verwendet, Syslog-Events mit einem aktuellen Zeitstempel zu versehen.

Die folgende Tabelle zeigt eine Übersicht aller SNTP Client Einstellungen:

Bez. im NEXMAN	Default Wert	Funktion
Client enable	disabled	Wenn ausgewählt, wird der SNTP Client im Switch aktiviert.
Time Server IP 1	<none>	Die IP Adresse des ersten Time Servers.
Time Server IP 2	<none>	Die IP Adresse des zweiten Time Servers. Falls beide Server IPs konfiguriert sind, so werden beide Server synchron angefragt und die erste gültige Antwort für die Aktualisierung der Systemzeit herangezogen.
Server Request Interval (seconds)	3600	Das Zeitintervall für die periodische Abfrage der aktuellen Zeit.
SNTP Protocol Version	3	Die SNTP Protokoll Version mit der die Requests an den Server ausgeführt werden.
Accept SNTP Broadcasts	disabled	Wenn ausgewählt, werden auch SNTP Broadcasts akzeptiert, die nicht vom oben konfigurierten Time Server stammen.
UTC Local Offset (minutes)	60	Der Zeitunterschied zwischen der lokalen Zeit und der koordinierten Weltzeit (Coordinated Universal Time, UTC). Eine automatische Umstellung zwischen Sommer- und Winterzeit durch den Switch erfolgt nicht.

Summer time correction	Disabled	Bestimmt, ob eine automatische Sommerzeitkorrektur durchgeführt werden soll. • Disabled Es wird keine Korrektur durchgeführt. • European summer time Es wird eine Korrektur durchgeführt, die für die meisten Staaten Europas anwendbar ist. Hier gilt die Sommerzeit vom letzten Sonntag des Monats März bis zum letzten Sonntag des Monats Oktober, jeweils ab 2 Uhr mitteleuropäischer Zeit (MEZ).
------------------------	----------	---

10.29. Switch Temperatur

Die Gehäusetemperatur des Switches wird in Grad Celsius angezeigt.

10.29.1. Temperatur Alarm Grenzwerte

Die Grenzwerte für die zulässige Temperatur können per Management konfiguriert werden:

- Low Alarm Limit (-20...+20 °C) [Default = 0 °C]

Dies ist das untere Limit. Bei Unterschreitung wird ein Alarm ausgelöst.

- High Alarm Limit (-30...+100 °C) [Default = 70 °C]

Dies ist das obere Limit. Bei Überschreitung wird ein Alarm ausgelöst.

Bei den Firmware-Versionen mit SNMP Unterstützung, wird zusätzlich bei Über- bzw. Unterschreitung der konfigurierten Temperaturgrenzen periodisch ein 'Temperature Failure' Event versendet.

10.29.2. Übertemperatur Powersave Funktion

Über die Funktion 'Overtemperature Powersave Action' kann eine Aktion konfiguriert werden, die bei Überschreitung der 'High Alarm Limit' Temperatur ausgelöst werden soll.

Hier steht folgende Funktion zur Verfügung:

- Set Speed/Duplex of ports with 'Autoneg.' or '1000FDX' to 'ECO 10/100'

Ports, die den Speed/Duplex Mode 'ECO 10/100' unterstützen, werden automatisch in diesen ECO Mode geschaltet um die Leistungsaufnahmen zu reduzieren. Jeder Port, der nicht mit 1 GigaBit/s betrieben wird, reduziert die Leistungsaufnahme um ca. 0,5 Watt im Switch und im Endgerät. Voraussetzung ist, dass der Port am Switch auf 'Autoneg' oder '1000 FDX' eingestellt ist.

WICHTIG: Für Ports, die wegen Übertemperatur in den ECO Mode geschaltet wurden, wird beim Speed/Duplex Setup die Einstellung 'ECO 10/100 (Overtemp.)' angezeigt. Nach Klärung der Ursache für die Übertemperatur, muss das Speed/Duplex Setup manuell auf die gewünschte Einstellung zurückgestellt werden.

10.30. Switch Betriebsspannungen

Die folgenden internen Betriebsspannungen werden mit 0,05 V Auflösung angezeigt:

- 2,5 V
- 3,3 V

Bei Über- bzw. Unterschreitung der zulässigen Grenzen (< 2,35 / > 2,65 V bzw. < 3,15 / > 3,45 V) wird ein "Internal Voltage Alarm" und ein IEC61850 "Power Supply Alarm" ausgelöst.

Bei Industrie Switches werden zusätzlich folgende externen Betriebsspannungen mit 1V Auflösung angezeigt:

- Power Input S1
- Power Input S2

Bei Über- bzw. Unterschreitung der zulässigen Grenzen (< 18 / > 60 V) wird ebenfalls ein IEC61850 "Power Supply Alarm" ausgelöst. Bei Ausfall einer der beiden Spannungen kann außerdem ein Alarm über die Alarmausgänge M1 bzw. M2 ausgelöst werden.

Alle internen und externen Betriebsspannungen können über die SNMP Private MIB abgefragt werden.

10.31. VLAN Unterstützung

Der Nexans Switch bietet volle VLAN Unterstützung einschließlich Trunking nach IEEE802.1Q und ist kompatibel mit allen marktüblichen Switchen anderer Hersteller.

Global für den Switch sind die folgenden Konfigurationseinstellungen möglich:

- VLAN Table
- VLAN Table Mode
- Tagging Ethertype

Pro Port können folgende Einstellungen vorgenommen werden:

- Default-VLAN-ID
- Voice-VLAN-ID
- Trunking Mode

Pro Port werden folgende Statusinformation angezeigt:

- Active Default-VLAN-ID
- Active Voice-VLAN-ID
- Active Trunking Mode

Die oben aufgeführten Parameter werden in den nachfolgenden Kapiteln detailliert erläutert.

10.31.1. VLAN Table

In der VLAN-Table müssen alle VLAN-ID's eingetragen werden, die vom Switch weitergeleitet werden sollen. Insgesamt können bis zu 64 verschiedene VLAN-ID's im Bereich 1...4095 konfiguriert werden. Alle Pakete, deren VLAN-ID nicht in der Table aufgeführt ist, werden vom Switch verworfen.

Folgende VLAN-ID's werden automatisch in die Table eingetragen und können nicht gelöscht werden:

- Default-VLAN-ID der einzelnen Ports
- Voice-VLAN-ID der einzelnen Ports
- RADIUS-Unsecure-VLAN-ID
- RADIUS-Guest-VLAN-ID
- RADIUS-Inaccessible-VLAN-ID
- IEEE802.1X-Authentication-Failure-VLAN-ID

Der manuelle Eintrag zusätzlicher VLAN-ID's ist nur dann erforderlich, wenn man zwei oder mehr Ports auf Trunking geschaltet hat. In diesem Fall muss dem Switch über die VLAN Table mitgeteilt werden, welche VLAN-ID's zwischen den getrunken Ports weitergeleitet werden dürfen.

WICHTIG:

Bei Switchen anderer Hersteller ist oftmals ein Default-VLAN fest vorgegeben und kann nicht gelöscht werden. Beim Nexans Switch ist zwar per Factory-Default die VLAN-ID '1' eingetragen, jedoch ist dieses Default-VLAN kein festes VLAN. Beispielsweise könnte man nach Umstellung aller Ports auf eine andere Default-VLAN-ID, die VLAN-ID 1 aus der VLAN-Table löschen.

10.31.2. VLAN Table Mode

Im Kapitel [10.31.1. VLAN Table](#) wurde beschrieben, wie VLAN-ID's in die Table aufgenommen werden.

Die Art und Weise bestehende Einträge zu löschen, wird dagegen durch den 'VLAN Table Mode' bestimmt.

Hier sind folgende Konfigurationseinstellungen möglich:

- 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)

WICHTIG:

Beim Wechsel des VLAN Table Mode wird die komplette VLAN Table gelöscht. Lediglich solche VLANs, die automatisch eingetragen werden, bleiben erhalten (siehe Kapitel [10.31.1. VLAN Table](#)).

Static - 802.1Q based (16 VLANs):

Bei dieser Einstellung müssen ID's in der VLAN-Table grundsätzlich manuell gelöscht oder mittels NEXMAN überschrieben werden. Diese Einstellung ist immer dann sinnvoll, wenn die Konfiguration der VLAN-ID's fest

vorgegeben ist und üblicherweise im laufenden Betrieb nicht geändert werden soll.

Ist die Table voll und man versucht z.B. die Default-VLAN-ID eines Ports auf eine unbekannte VLAN-ID zu setzen, so wird das Setzen der neuen VLAN-ID abgelehnt. Um dennoch die neue ID setzen zu können muss zunächst eine unbenutzte ID manuell aus der VLAN-Table gelöscht werden.

Static - 802.1Q based (64 VLANs):

Dieser Mode ist identisch zum obigen Mode "Static - 802.1Q based (16 VLANs)", jedoch werden hier bis 64 VLANs unterstützt.

Static - 802.1Q based (256 VLANs) (Supports Hybrid Trunking Mode):

Die dieser Mode ist identisch zum obigen Mode "Static - 802.1Q based (64 VLANs)", jedoch werden hier bis 256 VLANs unterstützt.

Ferner wird hierbei der sogenannte „Hybrid“ port trunking mode unterstützt, der für jeden Port separat konfiguriert werden kann (siehe Kapitel [10.31.7. Port Trunking Mode](#)).

Dynamic - 802.1Q based (16 VLANs):

Alle VLAN-ID's, die nicht als Port Default-VLAN-ID, Port Voice-VLAN-ID, RADIUS-Unsecure-VLAN-ID, RADIUS-Guest-VLAN-ID, RADIUS-Inaccessible-VLAN-ID oder IEEE802.1X-Authentication-Failure-VLAN-ID verwendet werden, werden automatisch aus der VLAN-Table entfernt. Dies ist z.B. sinnvoll, wenn die VLAN-ID's der Ports über RADIUS dynamisch eingestellt werden sollen und man verhindern möchte, dass die VLAN-Table überläuft. Der Dynamic Mode erkennt automatisch neue VLANs, unabhängig davon, ob diese per RADIUS oder manuell per CLI, SNMP, WEB oder Manager konfiguriert wurden. Auch allgemeine VLANs, wie z.B. das Management VLAN und das Unsecure VLAN, werden automatisch in der VLAN-Table ergänzt bzw. entfernt.

Wichtig: Falls Spanning Tree global aktiviert ist, wird das VLAN 1 grundsätzlich nicht gelöscht. Dies ist notwendig da das VLAN 1 für eventuell angeschlossene PVST-Geräte (Per-VLAN Spanning Tree) benötigt wird.

HINWEIS: Diese Funktion sollte ausschließlich verwendet werden, wenn nur ein einzelner Port (z.B. der Uplink) auf Trunking eingestellt ist.

Static - Port based (16 VLANs):

Dieser Mode ist primär für Provider Anwendungen konzipiert worden. Hier werden alle Ports, die dieselbe Default VLAN-ID eingestellt haben, transparent miteinander verbunden. Zwischen diesen verbundenen Ports werden alle Pakete (incl. einen evt. enthaltenem beliebigen 802.1Q VLAN-Tag) unverändert übertragen. Empfangene Pakete ohne VLAN Tag werden dabei ebenfalls ohne VLAN Tag auf den anderen verbundenen Ports rausgesendet.

Möchte man allerdings, dass empfangene ungetaggte Pakete mit einem 802.1Q Tag rausgesendet werden, so muss für diesen Port der Trunking Mode auf "802.1Q Tagging (Tag Default VLAN)" eingestellt werden. Dabei wird die an diesem Trunk-Port eingestellte Default VLAN-ID in das ungetaggte Paket als 802.1Q VLAN-Tag eingefügt. Diese Funktion ist dann hilfreich, wenn man z.B. den Management Port (der per Default ungetaggt ist) auf einem Trunk-Port mit VLAN-Tag versenden möchte. In der Gegenrichtung wird für alle auf dem Trunk-Port empfangenen Pakete, die dann auf den Management-Port weitergeleitet werden, ein evt. enthaltenes VLAN-Tag wieder entfernt.

HINWEIS: Diese Funktion wird z.Z. für die Switchtypen 'GigaSwitch V5', 'GigaSwitch V3' und allen Industrie Switchen unterstützt.

10.31.3. Fabric Attach

Fabric Attach ist eine technologische Erweiterung von Shortest Path Bridging (SPB) und erlaubt die Einbindung von nicht SPB fähigen Geräten und Switches in SPB Netze. Dazu muss für jede in der VLAN Tabelle definierte VLAN-ID eine SPBM I-SID konfiguriert werden. Sofern am Uplink Port ein Core-Switch angeschlossen ist, der Fabric Attach unterstützt, werden die konfigurierten I-SIDs per LLDP an diesen übermittelt. Zur Authentifizierung gegenüber dem Core-Switch kann optional ein „Fabric Attach Authentication Key“ konfiguriert werden. Wird dieser Key leer gelassen so wird per Factory Default der Key ‚nexans‘ verwendet.

10.31.4. Globale VLAN Port Isolation

Bei eingeschalteter VLAN Port Isolation sind alle oder ausgewählte User-Ports und der Management-Port grundsätzlich gegeneinander isoliert und können daher nicht direkt Daten miteinander austauschen. Dies gilt insbesondere, wenn die Ports demselben VLAN zugeordnet sind. Die Ports können in diesem Fall ausschließlich über den Uplink/Downlink-Port Daten austauschen.

Über die Konfigurationseinstellung 'Link type' kann dabei definiert werden, welche Ports User-Ports bzw. Uplink/Downlink-Ports sind. Per Factory Default sind Fiber- und SFP-Ports als Uplink/Downlink-Ports konfiguriert und alle anderen Ports als User-Ports.

Diese Funktion ist sinnvoll, wenn die VLAN-Zuweisung der angeschlossenen Endgeräte durch den Core-Switch anhand der MAC- oder IP-Adresse erfolgen soll. Ein häufiger Einsatzfall ist die Multi-User-Authentication nach IEEE802.1X bzw. MAC-based durch den Core-Switch.

Für die Globale VLAN Port Isolation sind folgende Einstellungen möglich:

- Disabled
- Isolate all User ports and Management port
- Isolate selected User ports and Management port

Disabled:

VLAN Port Isolation ist global deaktiviert.

Isolate all User ports and Management port:

Alle User-Ports und der Management-Port sind global voneinander isoliert.

Isolate selected User ports and Management port:

Nur ausgewählte User-Ports und der Management-Port sind voneinander isoliert. Um zu konfigurieren, welcher User-Port und ob der Management-Port isoliert werden soll, muss die Pro-Port-VLAN-Port-Isolation für den jeweiligen Port aktiviert werden, siehe Kapitel [10.31.5 Pro-Port VLAN Port Isolation](#).

10.31.5. Pro-Port VLAN Port Isolation

Wenn die Globale VLAN Port Isolation auf 'Isolate selected User ports and Management port' eingestellt ist, kann die VLAN Port Isolation separat für jeden User-Port und den Management-Port aktiviert werden.

HINWEIS:

Wenn die Globale VLAN Port Isolation deaktiviert ist, wird diese Funktion für alle einzelnen Ports deaktiviert.

10.31.6. Tagging Ethertype (Q-in-Q)

Der Tagging Ethertype bestimmt, welcher Wert als Ethertype in getaggte Pakete eingefügt wird. Laut IEEE802.1Q Standard ist dies der Wert '8100'. Einige Hersteller von Coreswitchen unterstützen aber auch andere Werte um z.B. IEEE801.Q-VLAN's zu tunneln. Dies ist vor allem für Service-Provider interessant.

Folgende Einstellungen sind möglich:

- 8100 (IEEE802.1Q)
- 9100 (Q-in-Q)
- 9200 (Q-inQ)

WICHTIG:

Die Q-inQ Einstellungen 9100 (Q-inQ) und 9200 (Q-inQ) sollten nur eingestellt werden, wenn der Core-Switch ebenfalls entsprechend konfiguriert ist. Ferner wird bei diesen Einstellungen keine Default-VLAN-ID bei getaggtten Ports unterstützt, d.h., bei getaggtten Ports werden grundsätzlich alle VLAN's getaggt. Eine evtl. eingestellte Default-VLAN-ID wird in diesem Fall ignoriert.

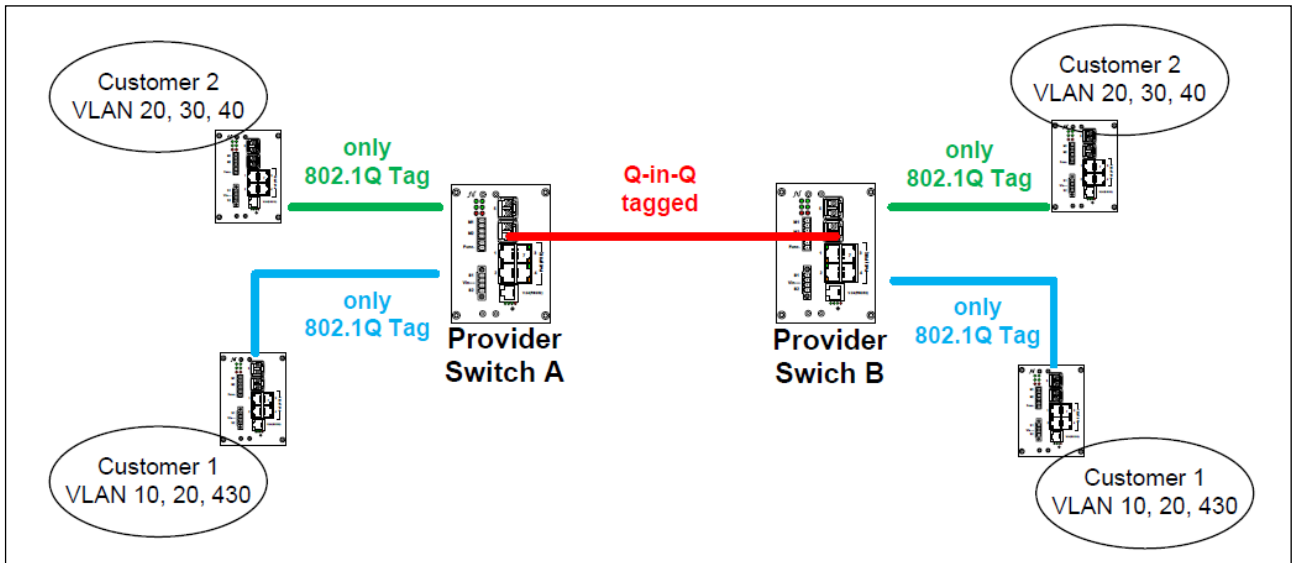
HINWEIS:

Der Tagging Ethertype ist nur bei bestimmten Switchtypen konfigurierbar. Bei allen andern Switchtypen ist er fest auf 8100 eingestellt.

10.31.6.1. Q-in-Q mit zwei Nexans Switchen

Beispiel A zeigt einen Aufbau mit zwei Nexans Switchen, die als Providerswitches dienen. Wichtig bei dieser Topologie ist, dass Customer 1 und Customer 2 ein unterschiedliches Default VLAN am Providerswitch zugeordnet bekommen. Das jeweils zugeordnete VLAN muss auf beiden Providerswitchen identisch sein. Damit Q-in-Q einwandfrei funktioniert, muss neben dem Umstellen des „Tagging Ethertype“ und dem Aktivieren des Trunking, dass Default VLAN zwischen den beiden Nexans Switchen auf „0“ konfiguriert werden.

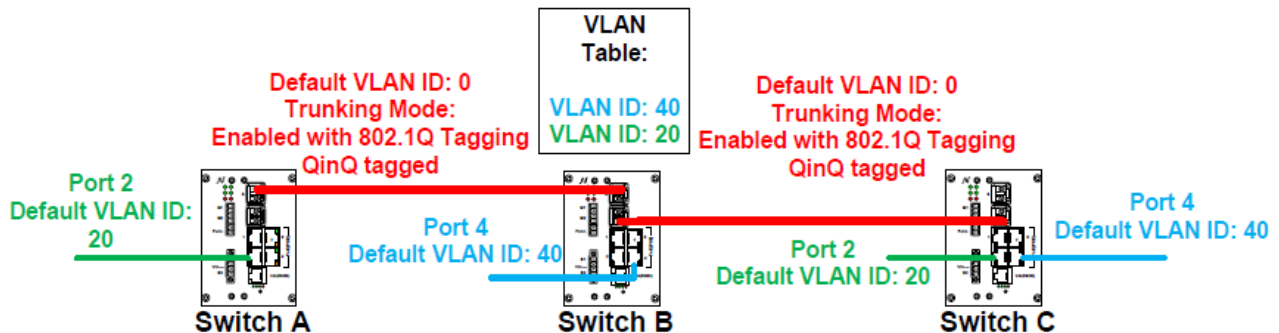
Beispiel A)



10.31.6.2. Q-in-Q mit drei Nexans Switchen

Beispiel B zeigt einen Aufbau mit drei Nexans Switchen, die als Providerswitches dienen. Die Konfiguration der Customer Ports und der Links zwischen den Nexans Switchen ist identisch zu der Konfiguration [10.31.6.1 Q-in-Q mit zwei Nexans Switchen](#). Jeder Customer muss sein eigenes Default VLAN zugewiesen bekommen. Die Links zwischen den Nexans Switchen müssen Trunking aktiviert haben und das Default VLAN "0" besitzen. Wichtig bei dieser Konstellation ist, dass das VLAN 20 in die VLAN Table des Switches B hinzugefügt wird, damit auch dieser die Daten im VLAN 20 Forwarded. Siehe auch Kapitel [10.31.1 VLAN Table](#)

Beispiel B)



Wichtiger HINWEIS:

Die Durchleitung von Q-in-Q Frames wie in Kapitel [10.31.6.2 Q-in-Q mit drei Nexans Switchen](#) beschrieben wird ausschließlich von folgenden Switchtypen unterstützt:

- iGigaSwitch 542
- iSwitch G 1043E+
- iGigaSwitch 1604
- iGigaSwitch 1608
- iGigaSwitch 160C

Bei allen anderen Switchtypen darf nur ein einziger Uplink Port als Trunk Port konfiguriert werden da eine Durchleitung von Q-in-Q Paketen zwischen zwei Trunk Ports nicht unterstützt wird. Siehe auch Kapitel [10.31.6.1 Q-in-Q mit zwei Nexans Switchen](#)

10.31.7. Port Trunking Mode

Der Trunking-Mode bestimmt, ob der betreffende Port alle VLAN-ID's der VLAN-Table transportieren soll.

Beim Trunking-Mode kann zwischen folgenden Einstellungen ausgewählt werden:

- Disable
- Enabled with 802.1Q Tagging
- Hybrid
- Enabled without Tagging

Die Funktionsweise der einzelnen Einstellungen hängt davon ab, ob der VLAN Table Mode auf einen "802.1Q based" oder "Port based" Mode eingestellt ist (siehe Kapitel [10.31.2. VLAN Table Mode](#)).

Disable:

- **802.1Q based:** Bei dieser Einstellung werden auf dem betreffenden Port ausschließlich Pakete gesendet, die dem Default-VLAN oder Voice-VLAN des betreffenden Ports angehören.
- **Port based:** Pakete werden auf diesem Port exakt so gesendet, wie sie auf einem anderen verbundenen Port empfangen wurden. Evt. enthaltene 802.1Q VLAN-Tags werden dabei 1:1 durchgereicht.

Enabled with 802.1Q Tagging:

- **802.1Q based:** Auf dem betreffenden Port werden die Pakete aller VLAN's, die in der VLAN-Table aufgeführt sind, gesendet und mit einem VLAN-Tag gemäß IEEE802.1Q versehen (mit Ausnahme des Default-VLAN).

Empfangene Pakete, die ebenfalls ein IEEE802.1Q Tag beinhalten, werden dem im Tag angegebenen VLAN zugeordnet. Sollte diese VLAN-ID allerdings nicht in der VLAN-Table aufgeführt sein, so wird das Paket verworfen.

Empfangene Pakete, die kein Tag beinhalten, werden grundsätzlich dem Default-VLAN des betreffenden Ports zugeordnet (siehe auch Kapitel [10.31.8. Port Default-VLAN-ID](#)).

Wichtig ist, dass auch die Gegenseite (zentraler Switch) in der Lage ist diese Tags auszuwerten und entsprechend konfiguriert wurde.

- **Port based:** Ungetaggte Pakete, die auf einem anderen verbundenen Port empfangen wurden, werden mit einem 802.1Q Tag gesendet. Dabei wird die auf diesem Port eingestellte Default VLAN-ID als 802.1Q VLAN-Tag eingefügt. Getaggte Pakete, die auf einem anderen verbundenen Port empfangen wurden, werden unverändert gesendet.

Hybrid:

- **802.1Q based:** Für den betreffenden Port kann individuell für jedes VLAN in der VLAN-Table eingestellt werden, ob dieses VLAN zugelassen ist.

Empfangene Pakete, die ein IEEE802.1Q Tag beinhalten, werden dem im Tag angegebenen VLAN zugeordnet, sofern das VLAN für diesen Port zugelassen ist. Anderenfalls wird das Paket verworfen.

Empfangene Pakete, die kein Tag beinhalten, werden grundsätzlich dem Default-VLAN des betreffenden Ports zugeordnet (siehe auch Kapitel [10.31.8. Port Default-VLAN-ID](#)).

Wichtig ist, dass auch die Gegenseite (zentraler Switch) in der Lage ist diese Tags auszuwerten und entsprechend konfiguriert wurde.

- **Port based:** Der Hybrid Mode steht hier nicht zu Verfügung.

Enable without Tagging:

- **802.1Q based:** Auf dem betreffenden Port werden die Pakete aller VLAN's, die in der VLAN-Table aufgeführt sind, gesendet, allerdings grundsätzlich ohne Tag. Wegen des fehlenden Tags erhält der angeschlossene Switch keine VLAN-Informationen zu den einzelnen Paketen. Es ist dann die Aufgabe des eingesetzten Switches die VLAN Zugehörigkeit anderweitig zu ermitteln (z.B. aufgrund der MAC-Source-Adresse).

WICHTIG: In empfangenen Paketen wird auf jeden Fall ein Tag benötigt, damit der Nexans Switch die VLAN Zugehörigkeit ermitteln kann. Empfangene Pakete, die kein Tag beinhalten, werden grundsätzlich der Default-VLAN-ID des betreffenden Ports zugeordnet.

- **Port based:** Pakete, die auf einem anderen verbundenen Port empfangen wurden, werden grundsätzlich ohne VLAN-Tag gesendet.

10.31.8. Port Default-VLAN-ID

Die Port Default-VLAN-ID bestimmt, welche Pakete auf dem betreffenden Port ohne Tag gesendet und empfangen werden. Auch wenn für den betreffenden Port das IEEE802.1Q Tagging eingeschaltet ist, werden die Pakete der Default-VLAN-ID auf diesem Port ohne Tag versendet. In Empfangsrichtung bedeutet dies, dass alle Empfangspakete, die kein Tag aufweisen, dieser Default-VLAN-ID zugeordnet werden.

Möchte man, dass für einen getrunken Port grundsätzlich alle Pakete getaggt gesendet und empfangen werden, so muss die Default-VLAN-ID des betreffenden Ports auf 0 eingestellt werden. In diesem Falle werden alle empfangenen Pakete, die kein Tag beinhalten, verworfen.

WICHTIG:

Bei Verwendung einer Default-VLAN-ID für einen getaggtten Port, sollte auch auf der Gegenseite (zentraler Switch) dieselbe VLAN-ID als Default-VLAN-ID eingestellt sein. Ansonsten laufen die Pakete u.U. in Leere und werden verworfen.

HINWEIS:

Die 'Default-VLAN-ID' wird z.T. bei anderen Herstellern auch als 'Native-VLAN-ID' bezeichnet.

10.31.9. Port Voice-VLAN-ID

Mittels der Port Voice-VLAN-ID kann auf dem betreffenden Port ein einzelnes getaggttes VLAN konfiguriert werden. Wie der Name schon sagt, ist das Einsatzgebiet dieser Funktion speziell auf die Kombination aus IP-Phone und nachgeschaltetem PC zugeschnitten. In den meisten Voice-over-IP Installationen sendet und empfängt der PC ungetaggte Pakete, wogegen das IP-Phone getaggtte Pakete mit entsprechenden 802.1Q Priorisierungsinformationen sendet und empfängt. In diesem Fall müsste die Default-VLAN-ID auf das VLAN des PC's und die Voice-VLAN-ID auf das VLAN des Phones konfiguriert werden.

Möchte man für den Port ausschließlich das Default-VLAN zulassen, so muss die Voice-VLAN-ID des betreffenden Ports auf 0 eingestellt werden (Factory Default).

HINWEIS: Wenn für den betreffenden Port das IEEE802.1Q Tagging eingeschaltet ist, wird eine evtl. konfigurierte Voice-VLAN-ID ignoriert.

10.31.10. Port VLAN-Tagging

Das VLAN-Tagging bestimmt für jeden Port und jedes VLAN, ob Pakete des betreffenden VLANs durchgelassen werden und ob das VLAN der gesendeten Pakete mit einem IEEE802.1Q Tag versehen wird oder nicht. Es ist abhängig von dem eingestellten Trunking-Mode und von der eingestellten Default-VLAN-ID bzw. Voice-VLAN-ID des betreffenden Ports.

Nur im Trunking-Mode "Hybrid" kann das VLAN-Tagging aller VLANs, mit Ausnahme der Default-VLAN-ID und Voice-VLAN-ID, individuell eingestellt werden. Für alle anderen Trunking-Modes ist das Tagging fest vorgegeben. Die entsprechenden Konfigurationparameter sind für den betreffenden Port schreibgeschützt (siehe Kapitel [10.31.7 Port Trunking Mode](#)).

Beim VLAN-Tagging werden folgende Einstellungen für jeden Port und jedes VLAN angezeigt:

- D
- V
- T
- U
- -

D:

Das betreffende VLAN ist für den Port als Default-VLAN-ID eingestellt. Pakete des Default-VLANs werden grundsätzlich ungetaggt über den Port versendet. Empfangene Pakete des Default-VLANs können getaggt oder ungetaggt sein.

V:

Das betreffende VLAN ist für den Port als Voice-VLAN-ID eingestellt. Pakete des Voice-VLANs werden grundsätzlich getaggt über den Port versendet. Empfangene Pakete des Voice-VLANs müssen getaggt ebenfalls sein.

T:

Pakete des betreffenden VLANs werden getaggt über den Port versendet. Empfangene Pakete des VLANs müssen ebenfalls getaggt sein.

U:

Pakete des betreffenden VLANs werden ungetaggt über den Port versendet. Empfangene Pakete des VLANs müssen getaggt sein.

-:

Pakete des betreffenden VLANs sind für den Port nicht erlaubt und werden beim Empfang verworfen.

Im Trunking Mode "Hybrid" können folgende Einstellungen für den betreffenden Port und jedes VLAN, ausgenommen Default-VLAN-ID und Voice VLAN-ID, geändert werden:

- T
- U (abhängig vom Switchtyp)
- -

10.31.11. Port Active Default-VLAN-ID

Die 'Active Default-VLAN-ID' zeigt die aktuell gültige Default-VLAN-ID für den betreffenden Port an. Dies ist normalerweise die für den Port konfigurierte Default-VLAN-ID.

Wenn für den Port eine Portsecurity Funktion mit Authentifizierung per RADIUS Server aktiviert ist, kann die aktive Default-VLAN-ID auch die RADIUS-Unsecure-VLAN-ID, RADIUS-Guest-VLAN-ID, RADIUS-Inaccessible-VLAN-ID oder IEEE802.1X-Authentication-Failure-VLAN-ID sein. Dies hängt davon ab, ob die MAC-Adresse oder der User noch nicht authentifiziert wurden bzw. die Authentifizierung fehlgeschlagen ist. Darüber hinaus kann das aktive Default-VLAN auch per RADIUS Server zugewiesen werden und ist damit völlig losgelöst von den im Switch konfigurierten VLAN-IDs.

Für nähere Informationen siehe Kapitel [10.59. Portsecurity mit Authentifizierung per RADIUS Server](#)

Ferner wird bei aktivierter Portmonitor Funktion der Monitor-Destination-Port auf die Default-VLAN-ID des Source-Ports geschaltet (siehe Kapitel [10.34. Portmonitor](#)).

10.31.12. Port Active Voice-VLAN-ID

Die 'Active Voice-VLAN-ID' zeigt die aktuell gültige Voice-VLAN-ID für den betreffenden Port an. Dies ist normalerweise die für den Port konfigurierte Voice-VLAN-ID.

Wenn für den Port eine Portsecurity Funktion mit Authentifizierung per RADIUS Server aktiviert ist, kann das aktive Voice-VLAN auch per RADIUS Server zugewiesen werden und ist damit völlig losgelöst von der im Switch konfigurierten Voice-VLAN-ID.

Ferner wird bei aktivierter Portmonitor Funktion der Monitor-Destination-Port auf die Voice-VLAN-ID des Source-Ports geschaltet (siehe Kapitel [10.34. Portmonitor](#)).

10.31.13. Port Active Trunking Mode

Der 'Active Trunking Mode' zeigt den aktuell gültigen Trunking-Mode für den betreffenden Port an. Dies ist normalerweise der für den Port konfigurierte Trunking-Mode.

Wenn für den Port eine Portsecurity Funktion mit Authentifizierung per RADIUS Server aktiviert ist, kann der aktive Trunking Mode auch 'Disabled' sein, obwohl der Trunking-Mode laut Konfiguration aktiviert ist. Dies hängt davon ab, ob die MAC-Adresse oder der User noch nicht authentifiziert wurden bzw. die Authentifizierung fehlgeschlagen ist. Für nähere Informationen siehe Kapitel [10.59. Portsecurity mit Authentifizierung per RADIUS Server](#)

Ferner wird bei aktivierter Portmonitor Funktion der Destination-Port auf den Trunking-Mode des Source-Ports eingestellt (siehe Kapitel [10.34. Portmonitor](#)).

10.31.14. Port Active VLAN-Tagging

Das 'Active VLAN-Tagging' zeigt das aktuell gültige VLAN-Tagging für den betreffenden Port und das betreffende VLAN an. Dies ist normalerweise das für den Port konfigurierte VLAN-Tagging.

Wenn für den Port eine Portsecurity Funktion mit Authentifizierung per RADIUS Server aktiviert ist, hängt das VLAN-Tagging von den resultierenden aktiven VLAN-Parametern 'Active Trunking Mode', 'Active Default-VLAN-ID' und 'Active Voice-VLAN-ID' ab. Die Einstellungen für das aktive VLAN-Tagging erfolgen entsprechend Kapitel [10.31.10 Port VLAN-Tagging](#). Jedoch werden die aktiven VLAN-Parameter anstelle der konfigurierten verwendet.

10.31.15. RADIUS Unsecure VLAN-ID

Alle Ports, für die eine RADIUS-MAC-based oder IEEE802.1X Authentifizierung aktiviert ist, werden im 'Nicht-Authentifizierten' Zustand auf dieses globale RADIUS-Unsecure-VLAN geschaltet. Dabei wird die Default-VLAN-ID des betreffenden Ports ignoriert und stattdessen die RADIUS-Unsecure-VLAN-ID verwendet. Bei entsprechender Konfiguration des zentralen Switches, kann somit ein 'Nicht-Authentifizierter' Port auf ein spezielles VLAN geschaltet werden, welches nur eingeschränkte Funktionalität bietet. Möchte man allerdings, dass ein 'Nicht-Authentifizierter' Port keinerlei Zugriff auf das Netz hat, so sollte als RADIUS-Unsecure-VLAN-ID eine ID angegeben werden, die auf dem zentralen Switch nicht verwendet wird. Dadurch laufen alle Pakete dieses VLAN ins Leere.

Für weitere Informationen zur VLAN Zuweisung siehe Ablaufdiagramme in den Kapiteln [10.59.1. Portsecurity Modi {RADIUS allow ...}](#) und [10.59.2. Portsecurity Modus {IEEE802.1X allow one MAC-Address}](#).

10.31.16. RADIUS Guest VLAN-ID

Die 'RADIUS Guest VLAN-ID' ist eine globale VLAN-Einstellung und nur gültig für Ports, für die eine RADIUS-MAC-based oder IEEE802.1X Authentifizierung aktiviert ist. In dieses VLAN wird ein Port verschoben, wenn die Authentifizierung fehlgeschlagen ist.

Soll dieses VLAN nicht zur Anwendung kommen, so muss die VLAN-ID auf 0 eingestellt werden.

Für weitere Informationen zur VLAN Zuweisung siehe Ablaufdiagramme in den Kapiteln [10.59.1. Portsecurity Modi {RADIUS allow ...}](#) und [10.59.2. Portsecurity Modus {IEEE802.1X allow one MAC-Address}](#).

10.31.17. RADIUS Inaccessible VLAN-ID

Die 'RADIUS Inaccessible VLAN-ID' ist eine globale VLAN-Einstellung und nur gültig für Ports, für die eine RADIUS-MAC-based oder IEEE802.1X Authentifizierung aktiviert ist. In dieses VLAN wird ein Port verschoben, wenn alle konfigurierten RADIUS Server Down sind.

Soll dieses VLAN nicht zur Anwendung kommen, so muss die VLAN-ID auf 0 eingestellt werden.

Für weitere Informationen zur VLAN Zuweisung siehe Ablaufdiagramme in den Kapiteln 10.59.1. Portsecurity Modi {RADIUS allow ...} und 10.59.2. Portsecurity Modus {IEEE802.1X allow one MAC-Address}.

10.31.18. IEEE802.1X Authentication Failure VLAN-ID

Die 'IEEE802.1X Authentication Failure VLAN-ID' ist eine globale VLAN-Einstellung und nur gültig für Ports, für die eine IEEE802.1X Authentifizierung aktiviert ist. In dieses VLAN wird ein Port verschoben, wenn der angeschlossene IEEE802.1X Client die maximale Anzahl von Authentifizierungsversuchen überschritten hat.

Soll dieses VLAN nicht zur Anwendung kommen, so muss die VLAN-ID auf 0 eingestellt werden.

Für weitere Informationen zur VLAN Zuweisung siehe Ablaufdiagramme in den Kapiteln 10.59.1. Portsecurity Modi {RADIUS allow ...} und 10.59.2. Portsecurity Modus {IEEE802.1X allow one MAC-Address}.

10.32. VLAN Portmirror

Durch die Auswahl der Funktion 'VLAN Portmirror' wird das Addresslearning im Switch abgeschaltet und der Switch verhält sich innerhalb von jedem VLAN wie ein Hub. D.h., dass auf allen Ports eines VLAN's alle Pakete des betreffenden VLAN's weitergeleitet werden.

Diese Funktion ist z.B. sehr hilfreich, wenn man den Datenverkehr eines bestimmten TP-Ports auf einem anderen TP-Port aufzeichnen möchte. Bei Ports müssen dazu im selben VLAN sein.

WICHTIGER HINWEIS:

Durch Einschalten dieser Funktion ist eine Anzeige der MAC-Adressenliste per Telnet/SSH/V.24-Console und per SNMP nicht mehr möglich. Ferner wird die Portsecurity Funktion und der Bandbreitenlimiter aller Ports deaktiviert.

10.33. Global LED Mode

Mit der Funktion LED Setup ist es möglich, den Anzeigemodus der Switch LEDs zu verändern. Folgende Anzeigemodi können eingestellt werden:

- Standard
- All LEDs Off
- All LEDs Off, except Mgmt LED
- All LEDs On
- All LEDs green blinking
- Right LEDs red/blue blinking

Standard:

Dies ist der Factory Default Wert. Die Anzeige LEDs leuchten entsprechend Ihrer normalen Funktion.

All LEDs Off:

Alle Anzeige LEDs sind permanent ausgeschaltet.

All LEDs Off, except Mgmt LED:

Die Mgmt-LED zeigt ihre normale Funktion an. Alle anderen Anzeige LEDs sind permanent ausgeschaltet.

All LEDs On:

Alle Anzeige LEDs sind permanent eingeschaltet.

All LEDs green blinking:

Alle LEDs blinken grün.

Right LEDs red/blue blinking:

Alle LEDs blinken abwechselnd rot und blau.

10.34. Portmonitor

Die Portmonitor Funktion (auch Portspiegelung genannt) erlaubt es, den Datenverkehr eines einzelnen Switchports auf einen zweiten Port zu duplizieren. Der Source-Port, dessen Verkehr mitgehört werden soll, und der Destination-Port, auf den diese Daten dupliziert werden, können frei gewählt werden.

Dabei können folgende Modi eingestellt werden:

- Disabled
- Rx and Tx
- Rx only
- Tx only

Disabled:

Die Portmonitor Funktion ist deaktiviert

Rx and Tx:

Alle Pakete, die auf den Source-Port empfangen oder gesendet werden, werden auf den Destination-Port dupliziert.

Rx only:

Nur Pakete, die auf den Source-Port empfangen werden, werden auf den Destination-Port dupliziert.

Tx only:

Nur Pakete, die auf den Source-Port gesendet werden, werden auf den Destination-Port dupliziert.

WICHTIG:

Bei aktivierter Portmonitor Funktion, ist der eingestellte Destination-Port für normalen Datenverkehr blockiert und kann ausschließlich zum mithören der Daten des Source-Ports verwendet werden. Ferner wird die 'Active Default-VLAN-ID', die 'Active Voice-VLAN-ID' und der 'Active Trunking Mode' des Destination-Ports automatisch auf die entsprechenden Werte des Source-Ports eingestellt. D.h., dass Pakete den Destination-Port genauso verlassen, wie diese auf dem Source-Port empfangen bzw. gesendet wurden. Steht der Source-Port auf Trunking, so werden getaggte Pakete am Source-Port auch auf dem Destination-Port mit Tag ausgegeben.

HINWEIS:

Gilt nur für Switches deren Tagging Ethertype auf 9100(Q-in-Q) oder 9200(Q-in-Q) eingestellt ist: Werden am Monitor Source Port Pakete mit Q-in-Q Tag 9100 bzw. 9200 gesendet oder empfangen, so wird dieses Q-in-Q Tag vor der Weiterleitung des Paketes am Monitor Destination-Port u.U. entfernt.

10.35. IEEE802.1X Transparenz

Diese Funktion bewirkt, dass alle für die IEEE802.1X Authentifizierung verwendeten Multicast-Pakete '01:80:C2:00:00:03' den Switch transparent durchlaufen. Auch wenn die einzelnen Ports in verschiedenen VLAN's konfiguriert sind, werden diese speziellen Multicasts auf alle Ports verteilt. Alle anderen Multicasts und Broadcasts bleiben allerdings weiterhin innerhalb der definierten VLAN Grenzen.

Diese Funktion wird in Verbindung mit zentralen Switchen verwendet, die das sogenannte 'Multi-User-Authentication-per-Port' mit IEEE802.1X unterstützen. Dadurch ist es möglich die IEEE802.1X Authentifizierung vom zentralen Switch durchführen zu lassen, obwohl die Teilnehmer am Nexans Switch in verschiedenen VLAN's konfiguriert sind.

HINWEIS:

Diese Funktion wird automatisch abgeschaltet, wenn für mindestens einen Port die IEEE802.1X Authentifizierung eingeschaltet ist. In diesem Fall wird nämlich die IEEE802.1X Authentifizierung ausschließlich durch den Nexans Switch durchgeführt.

10.36. Portsecurity

Die folgenden Modi werden unterstützt:

- 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)

Die folgenden Modi, **mit** Authentifizierung über einen RADIUS Server, stehen ausschließlich bei den Firmware-Versionen mit RADIUS bzw. IEEE802.1X Unterstützung zur Verfügung (Beschreibung siehe Kapitel [10.59](#)).

Portsecurity mit Authentifizierung per 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

Diese Einstellung bestimmt, ob bei einem Portsecurity-Failure der betreffende Port abgeschaltet wird oder ob ausschließlich periodische Event Meldungen versendet werden.

Abgeschaltete Ports können optional nach einer einstellbaren "Re-Enable Time for Security-Disabled Ports" automatisch wieder aktiviert werden. Die Zeit ist dabei im Bereich von 1 bis 60000 Sekunden konfigurierbar.

Für 'Portsecurity-Failure Action' sind folgende Einstellungen möglich:

- 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:

Sofort nach Erkennen eines Portsecurity-MAC-Failure (siehe Tabelle unten) wird der betreffende Port abgeschaltet. Als Status wird daraufhin im 'Link State' und 'Security State' der Wert 'SECURITY-DISABLED' angezeigt.

Disable Port after second wrong MAC:

Im Falle eines Portsecurity-MAC-Failure (siehe Tabelle unten) wird zunächst die erste fehlerhafte MAC Adresse geblockt und im NEXMAN in der Spalte 'Allowed MACs Overflow Address' angezeigt. Als Status wird dann im 'Security State' der Wert 'SECURITY-WARNING' angezeigt. Erst nach Erkennen einer zweiten fehlerhaften MAC Adresse wird der betreffende Port abgeschaltet. Als Status wird daraufhin im 'Link State' und 'Security State' der Wert 'SECURITY-DISABLED' angezeigt.

Don't disable Port. Send periodic Events only:

Im Falle eines Portsecurity-MAC-Failure (siehe Tabelle unten) bleibt der betreffende Port einschaltet und im 'Security Status' wird 'SECURITY-WARNING' angezeigt.

Disable Port immediately after wrong MAC or Authentication:

Dieser Mode ist identisch zum Security Mode „Disable Port immediately after first wrong MAC“. Zusätzlich wird der betreffende Port abgeschaltet falls bei den Security Modi 'RADIUS ...' und 'IEEE802.1X ...' die Authentifizierung vom RADIUS Server abgelehnt wurde. Als Status wird daraufhin im 'Link State' und 'Security State' der Wert 'SECURITY-DISABLED' angezeigt.

Folgende Ereignisse führen zu einem Portsecurity-MAC-Failure:

Security Mode	Ereignis
Manual setting three MAC-Addresses	Erkennen einer MAC-Adresse, die nicht manuell konfiguriert wurde
Manual setting three Vendor MAC-Addresses	Erkennen einer Vendor MAC-Adresse, die nicht manuell konfiguriert wurde
Auto allow one MAC-Address	Erkennen von mehr als einer MAC-Adresse seit dem letzten Link Up
Auto allow two MAC-Addresses	Erkennen von mehr als zwei MAC-Adressen seit dem letzten Link Up
Auto allow three MAC-Addresses	Erkennen von mehr als drei MAC-Adressen seit dem letzten Link Up
Learn and fix one MAC-Address	Erkennen einer MAC-Adresse, die nicht zuvor automatisch gelernt wurde. Es kann maximal eine MAC-Adresse gelernt werden
Learn and fix two MAC-Addresses	Erkennen einer MAC-Adresse, die nicht zuvor automatisch gelernt wurde. Es können maximal zwei MAC-Adressen gelernt werden
RADIUS allow one MAC-Address	Erkennen von mehr als einer MAC-Adresse seit dem letzten Link Up
RADIUS allow two MAC-Addresses	Erkennen von mehr als zwei MAC-Adressen seit dem letzten Link Up
RADIUS allow three MAC-Addresses	Erkennen von mehr als drei MAC-Adressen seit dem letzten Link Up

IEEE802.1X allow one MAC-Address	Erkennen von mehr als einer MAC-Adresse seit dem letzten Link Up
IEEE802.1X PC+Voice allow two MAC-Addresses	Erkennen von mehr als zwei MAC-Adressen seit dem letzten Link Up
IEEE802.1X Multi-User allow three MAC-Addresses	Erkennen von mehr als drei MAC-Adressen seit dem letzten Link Up
IEEE802.1X allow all MAC-Addresses	Nicht anwendbar

10.36.2. Portsecurity - Voice VLAN Authentication Mode

Der 'Voice VLAN Authentication Mode' bestimmt, ob für MAC Adressen, die im Voice VLAN erkannt wurden, eine IEEE802.1X oder MAC basierte Authentifizierung durchgeführt wird.

Hier stehen folgende Modi zur Verfügung:

- Enable Authentication
- Bypass Authentication

Enable Authentication (Default):

Im Voice VLAN erkannte MAC Adressen müssen entsprechend dem eingestellten Security Mode authentifiziert werden bevor dieser Zugriff auf das Voice VLAN erhalten.

Bypass Authentication:

Für MAC Adressen, die im Voice VLAN erkannt werden, wird keine Authentifizierung durchgeführt und die betreffenden Endgeräte haben unmittelbaren Zugriff auf das eingestellte Voice VLAN.

HINWEIS:

Diese Einstellung ist ausschließlich für Ports relevant, bei denen

a) ein Voice VLAN konfiguriert ist
und

b) der Security Mode auf eine RADIUS-MAC-based oder IEEE802.1X Authentifizierung eingestellt ist.

10.36.3. Portsecurity - Allowed MACs Overflow Address

Im Falle eines Portsecurity-Failure, wird die fehlerhafte MAC Adresse u.a. im NEXMAN in der Spalte 'Allowed MACs Overflow Address' angezeigt. Als Status wird dann in der Spalte 'Security State' der Wert 'SECURITY-WARNING' bzw. 'SECURITY-DISABLED' ausgegeben, abhängig von der Einstellung des Parameters 'Port Security Failure Action' (siehe Kapitel [10.36.1. Portsecurity - Failure Action](#)).

10.36.4. Portsecurity - Security State

Der 'Security State' wird nur angezeigt, wenn für den betreffenden Port einer der oben genannten Portsecurity Modi eingeschaltet ist. Ansonsten wird dort 'not supported' bzw. '-' angezeigt.

Die folgende Übersicht zeigt die möglichen Status Werte:

Security State	
Bezeichnung	Bedeutung
-	Portsecurity ist disabled
Waiting for Link	Es konnte kein gültiges Linksignal auf dem Port detektiert werden
Waiting for MAC's	Auf dem Port wurde ein gültiges Linksignal erkannt, allerdings wurde noch kein Datenpaket eines angeschlossenen Gerätes empfangen um dessen MAC Adresse zu lernen.
Authenticating	Für mindestens eine MAC Adresse des Ports läuft z.Z. eine nicht abgeschlossene Authentifizierung per IEEE802.1X oder RADIUS-MAC-based.
Port Authenticated	Für keine der gelernten MAC Adressen des Ports liegt ein Portsecurity-Failure oder eine Portsecurity-Warning vor. Ferner sind alle Authentifizierungen per IEEE802.1X oder RADIUS-MAC-based abgeschlossen.
SECURITY-DISABLED	Der Port wurde automatisch abgeschaltet, weil ein Portsecurity-Failure detektiert wurde (Siehe Kapitel 10.36.1. Portsecurity - Failure Action)

Security Warning	Auf dem Port wurde ein Portsecurity-Failure detektiert, aber der Port wurde nicht abgeschaltet (Siehe Kapitel 10.36.1. Portsecurity - Failure Action)
LOOP-DISABLED	Der Port wurde automatisch abgeschaltet, weil die aktivierte 'Active Loop Protection' eine Loop erkannt hat.
Port Admin Disabled	Der Port wurde vom Administrator manuell abgeschaltet
RADIUS Server(s) down	Alle konfigurierten Radius Server sind nicht erreichbar. Es wird ein Alarm in der Device List des Managers angezeigt.
Unsecure VLAN	Dem Port wurde das Unsecure VLAN zugeordnet
Auth.-Failure-VLAN	Dem Port wurde das Auth.-Failure-VLAN zugeordnet
BPDU-DISABLED	Der Port wurde automatisch abgeschaltet, weil eine Spanning-Tree BPDU empfangen wurde.
RING-LOOP-DISABLED	Der Port wurde automatisch abgeschaltet, weil ein Loop-Protection-Paket empfangen wurde.
DHCP-SNOOP-DISABLED	Der Port wurde automatisch abgeschaltet, weil ein DHCP-Server Paket empfangen wurde.

10.36.5. Portsecurity – Renew-Befehl

Möchte man einen Port mit aktivierter Portsecurity Re-Initialisieren oder einen abgeschalteten Port wieder aktivieren, so kann dies über den Befehl 'Renew Portsecurity' erfolgen.

HINWEIS:

Der Renew Befehl kann im CLI sowie im WEB sowohl im User Mode (Read/Only Access) als auch im Admin Mode (Read/Write Access) ausgeführt werden.

Bei Ausführung dieses Befehls werden folgende Aktionen für den betreffenden Port ausgeführt:

- **Portsecurity Modi {Disabled}:**

- Falls der Port abgeschaltet ist, wird dieser wieder eingeschaltet

- **Portsecurity Modi {Manual setting ...}:**

- Falls der Port abgeschaltet ist, wird dieser wieder eingeschaltet

- **Portsecurity Modi {Auto allow ...}:**

- Falls der Port abgeschaltet ist, wird dieser wieder eingeschaltet
- Alle gelernten MAC-Adressen werden gelöscht

- **Portsecurity Modi {Learn and fix ...}:**

- Falls der Port abgeschaltet ist, wird dieser wieder eingeschaltet
- Alle gelernten und im Flash gespeicherten MAC-Adressen werden gelöscht

- **Portsecurity Modi {RADIUS allow ...}:**

- Falls der Port abgeschaltet ist, wird dieser wieder eingeschaltet
- Alle gelernten MAC-Adressen werden gelöscht und müssen erneut über Radius authentifiziert werden
- Der Port wird auf das Startup-VLAN eingestellt (Default-VLAN bzw. RADIUS-Unsecure-VLAN)

- **Portsecurity Modus {IEEE802.1X allow one MAC-Address}:**

- Falls der Port abgeschaltet ist, wird dieser wieder eingeschaltet
- Die gelernte MAC-Adresse wird gelöscht
- Der Port wird auf das Startup-VLAN eingestellt (Default-VLAN bzw. RADIUS-Unsecure-VLAN)
- Die Authentifizierung des Endgerätes per IEEE802.1X wird neu gestartet

- **Portsecurity Modus {PC+Voice allow two MAC-Addresses}:**

- Falls der Port abgeschaltet ist, wird dieser wieder eingeschaltet
- Die gelernten MAC-Adressen werden gelöscht
- Der Port wird auf das Startup-VLAN eingestellt (Default-VLAN bzw. RADIUS-Unsecure-VLAN)
- Die Authentifizierung der Endgeräte per IEEE802.1X wird neu gestartet

- **Portsecurity Modus {Multi-User allow three MAC-Addresses}:**

- Falls der Port abgeschaltet ist, wird dieser wieder eingeschaltet
- Alle gelernten MAC-Adressen werden gelöscht
- Der Port wird auf das Default-VLAN eingestellt, neue MAC Adressen werden zunächst geblockt.
- Die Authentifizierung der Endgeräte per IEEE802.1X wird neu gestartet

•Portsecurity Modus {IEEE802.1X allow all MAC-Addresses}:

- Falls der Port abgeschaltet ist, wird dieser wieder eingeschaltet
- Der Port wird auf das Startup-VLAN eingestellt (Default-VLAN bzw. RADIUS-Unsecure-VLAN)
- Die Authentifizierung per IEEE802.1X wird neu gestartet

• Portsecurity Modus {Supplicant with MD5 Challenge}:

- Nicht anwendbar, da Authentifizierung und Freischaltung durch den Core Switch erfolgen muss.

10.36.6. Portsecurity - Modus {Auto allow one, two or three MAC-Address(es)}

Die Security Modi {Auto allow one MAC-Address}, {Auto allow two MAC-Addresses} bzw. {Auto allow three MAC-Addresses} ermöglichen, dass der Switch den Zugriff über den betreffenden Ports auf eine, zwei bzw. drei MAC-Adressen dynamisch begrenzt, und alle Adressen darüber hinaus als Portsecurity-Failure meldet und der Port ggf. abgeschaltet wird (siehe Kapitel [10.36.1. Portsecurity - Failure Action](#)). Dies verhindert z.B., dass der Benutzer hinter einem TP-Port einen weiteren Switch anschließt. Die gelernten MAC-Adressen werden automatisch gelöscht, wenn der Link des betreffenden Ports ausfällt (z.B. wenn ein anderer PC aufgesteckt wird) oder wenn der Port manuell abgeschaltet wurde.

Möchte man die Portsecurity Funktion eines bestimmten Ports Re-Initialisieren oder einen automatisch abgeschalteten Port wieder aktivieren, so kann dies über den 'Renew-Befehl' erzwungen werden (siehe Kapitel [10.36.5. Portsecurity – Renew-Befehl](#)).

10.36.7. Portsecurity - Modus {Manual setting three MAC-Addresses}

Bei diesem Modus können bis zu drei MAC-Adressen pro Port fest konfiguriert werden. Wird dann an dem betreffenden Port eine unbekannte MAC-Adresse empfangen, wird der Port ggf. abgeschaltet (siehe Kapitel [10.36.1. Portsecurity - Failure Action](#)).

Möchte man die Portsecurity Funktion eines bestimmten Ports Re-Initialisieren oder einen automatisch abgeschalteten Port wieder aktivieren, so kann dies über den 'Renew-Befehl' erzwungen werden (siehe Kapitel [10.36.5. Portsecurity – Renew-Befehl](#)).

10.36.8. Portsecurity - Modus {Manual setting three Vendor MAC-Addresses}

Bei diesem Modus können bis zu drei Vendor MAC-Adressen pro Port fest konfiguriert werden. Diese Funktion ist identisch mit der Einstellung {Manual setting three MAC-Addresses}, allerdings wird von den konfigurierten MAC-Adressen nur der Vendor-Teil (die ersten drei Bytes) überprüft.

10.36.9. Portsecurity - Modus {Learn and fix one or two MAC-Address(es)}

Bei der Security Funktion {Learn and fix one MAC-Address} und {Learn and fix two MAC-Addresses}, lernt der Switch automatisch eine bzw. zwei MAC-Adressen und übernimmt diese als fixe Vorgabe ins Flash. Alle Adressen darüber hinaus werden als Portsecurity-Failure gemeldet und der Port ggf. abgeschaltet (siehe Kapitel [10.36.1. Portsecurity - Failure Action](#)). Da die gelernten MAC-Adressen im Flash abgespeichert werden, sind diese auch nach einem Reboot des Switches aktiv.

Möchte man die Portsecurity Funktion eines bestimmten Ports Re-Initialisieren oder einen automatisch abgeschalteten Port wieder aktivieren, so kann dies über den 'Renew-Befehl' erzwungen werden (siehe Kapitel [10.36.5. Portsecurity – Renew-Befehl](#)).

10.36.10. Portsecurity - MAC Adressen

Im NEXMAN, WEB, Telnet und SNMP werden pro Port bis zu drei MAC Adressen angezeigt, die für die Portsecurity relevant sind. Dies sind entweder die fest vorgegebenen oder die automatisch gelernten MAC Adressen. Bei ausgeschalteter Portsecurity werden hier ebenfalls die gelernten MAC Adressen angezeigt, allerdings werden diese für keinerlei Securityfunktionen herangezogen. Werden in diesem Fall mehr als drei MAC Adressen pro Port erkannt, so wird statt der MAC Adressen der Hinweis 'More than three MACs' angezeigt. Zur Anzeige aller Adressen kann dann z.B. im NEXMAN die Funktion 'Show MAC Table' verwendet werden.

10.36.11. Portsecurity - MAC State

Der Security MAC State gibt zu jeder Security MAC Adresse den aktuellen Status der Authentifizierung an.

Die folgende Übersicht zeigt die möglichen Status Werte:

Security MAC State	
Bezeichnung	Bedeutung
Fixed	Die MAC Adresse ist fest vorgegeben. Für diesen Port ist entweder ist eine Security Mode mit manueller Vorgabe oder mit automatischem Fixen der MAC Adresse eingestellt.
Learned	Die MAC Adresse wurde gelernt aber keine Authentifizierung durchgeführt.
MAC:Authen. via RADIUS	Der Port ist auf einen Mode mit MAC basierender Authentifizierung eingestellt {RADIUS allow ...} und die Anfrage an den RADIUS Server zwecks Authentifizierung dieser MAC Adresse wird gerade ausgeführt.
MAC:REJECTED BY RADIUS	Die Anfrage an den RADIUS Server zwecks Authentifizierung dieser MAC Adresse wurde vom Server mit einem Access Reject abgelehnt. Es wird ein Alarm in der Device List des Managers angezeigt.
MAC:OK	Die Anfrage an den RADIUS Server zwecks Authentifizierung dieser MAC Adresse wurde vom Server mit einem Access Accept bestätigt. Die MAC Adresse wurde dem Default VLAN des betreffenden Ports zugeordnet.
MAC:OK:Voice-VLAN	Die Anfrage an den RADIUS Server zwecks Authentifizierung dieser MAC Adresse wurde vom Server mit einem Access Accept bestätigt. Die MAC Adresse wurde dem Voice VLAN des betreffenden Ports zugeordnet.
BYPASS:OK:Voice-VLAN	Die MAC Adresse wurde dem Voice VLAN des betreffenden Ports zugeordnet und kann dort produktiv arbeiten. Eine Authentifizierung wurde nicht durchgeführt, weil der 'Voice VLAN Authentication Mode' auf 'Bypass Authentication' eingestellt ist.
DOT1X:Requesting Identity	Der Port ist auf einen Mode mit IEEE802.1X basierender Authentifizierung eingestellt und der Switch versucht gerade, per EAP-Request-Identity Paketen, einen Kontakt zum IEEE802.1X Supplicanten des angeschlossenen Endgerätes aufzubauen.
DOT1X:Authen. via RADIUS	Der Port ist auf einen Mode mit IEEE802.1X basierender Authentifizierung eingestellt und die Anfrage an den RADIUS Server zwecks Authentifizierung des IEEE802.1X Gerätes gerade ausgeführt.
DOT1X:REJECTED BY RADIUS	Die Anfrage an den RADIUS Server zwecks Authentifizierung des IEEE802.1X Gerätes wurde vom Server mit einem Access Reject abgelehnt. Es wird ein Alarm in der Device List des Managers angezeigt.
DOT1X:OK	Die Anfrage an den RADIUS Server zwecks Authentifizierung dieses IEEE802.1X Gerätes wurde vom Server mit einem Access Accept bestätigt. Die MAC Adresse wurde dem Default VLAN des betreffenden Ports zugeordnet.
DOT1X:OK:Voice-VLAN	Die Anfrage an den RADIUS Server zwecks Authentifizierung dieses IEEE802.1X Gerätes wurde vom Server mit einem Access Accept bestätigt. Die MAC Adresse wurde dem Voice VLAN des betreffenden Ports zugeordnet.

10.36.12. Portsecurity - MAC Adressen Ageing

Die per Portsecurity gelernten MAC Adressen werden in einer separaten Tabelle geführt die unabhängig von der Switch Forwarding Tabelle ist (siehe Kapitel [10.37. MAC Adressen Tabelle](#)). Die per Portsecurity gelernten MAC Adressen werden z.B. im Manager auf dem Reiter 'MAC+Security State' angezeigt und normalerweise durch einen Link Down oder Renew Befehl gelöscht.

Über das Portsecurity Adressen Ageing Setup kann alternativ eine Ageing Zeit zwischen 1 und 255 Minuten für diese Portsecurity MAC Adressen eingestellt werden. Diese Zeit kann allerdings nicht kürzer als die Ageing Zeit der Switch Forwarding Tabelle eingestellt werden (siehe Kapitel [10.39. Address Ageing Time der Forwarding Tabelle](#)).

Hierbei wird zwischen zwei separat konfigurierbaren Zeiten unterschieden:

- Portsecurity ageing time
- Portsecurity ageing time for PC behind IP-Phone

Portsecurity ageing time:

Diese Zeit greift für folgende Portsecurity Modi:

- 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

Die eingestellte Zeit gilt für alle gelernten MAC in den oben aufgeführten Modi. Eine Ausnahme bilden jedoch MAC Adressen von Endgeräten, die in Verbindung mit einem Voice-VLAN gelernt wurden, d.h. PCs, die hinter einem IP Phone angeschlossen sind. Für diese Endgeräte lässt sich eine separate Ageing Zeit konfigurieren, siehe unten. Wird die Ageing Zeit auf 0 eingestellt so ist das Ageing abgeschaltet (Werkseinstellung) und die Portsecurity MAC Adressen können ausschließlich per Link Down des Switchports oder Renew Befehl gelöscht werden.

Portsecurity ageing time for PC behind IP-Phone:

Diese Ageing Time greift nur für Endgeräte, die hinter einem IP-Phone angeschlossen sind. Bedingung ist, dass der Portsecurity Mode auf **IEEE802.1X PC+Voice allow two MAC addresses** eingestellt ist und auf dem Port eine MAC Adresse im Voice-VLAN erkannt wurde.

Dies ist insbesondere für Installationen interessant, bei denen an einen Port des Switches ein IP Phone und ein kaskadierter Notebook angeschlossen ist (z.B. flexible Arbeitsplätze). Wird das angeschlossene Notebook dann entfernt, so wird nach Ablauf der Ageing Zeit die MAC Adresse des Notebooks gelöscht und es kann ein Notebook mit einer anderen MAC Adresse angeschlossen werden. Wird diese Ageing Zeit auf 0 eingestellt so gilt für diese Endgeräte ebenfalls die oben einstellbare Standard Portsecurity ageing time.

Portsecurity ageing time for Allowed MACs Overflow Address:

Diese Zeit greift für folgende Portsecurity Modi:

- Auto allow one/two/three MAC address(es)
- IEEE802.1X PC+Voice allow two MAC addresses
- IEEE802.1X Multi-User allow three MAC addresses

Bei einem Portsecurity Fehler wird die erste fehlerhafte MAC-Adresse geblockt und als " Allowed MACs Overflow Address " gemeldet. Wenn eine Ageing Zeit konfiguriert ist und diese MAC-Adresse für die konfigurierte Ageing Zeit auf dem betreffenden Port nicht empfangen wird, wird diese MAC-Adresse gelöscht. Wird die Ageing Zeit auf 0 eingestellt so ist das Ageing abgeschaltet (Werkseinstellung) und die 'Allowed MACs Overflow Address' kann ausschließlich per Link Down des Switchports oder per Renew Befehl gelöscht werden.

10.37. MAC Adressen Tabelle

Über NEXMAN, Telnet/SSH/V.24-Console und SNMP kann eine Liste aller gelernten MAC Adressen und der zugehörigen VLANs und Ports abgerufen werden.

Im NEXMAN erfolgt dies über die Funktion 'Show MAC Table'.

Das entsprechende Telnet Kommando lautet: ' sh:ow ma:c-address-table d:ynamic [<if-no>|a:ll]'

Per SNMP sind die MAC-Adressen über folgende Standard-MIB abrufbar:

- BRIDGE-MIB: dot1dTpFdbTable

Für eine Übersicht aller SNMP-MIBs siehe Kapitel [10.53.7. SNMP MIB Übersicht](#).

10.38. Quality of Service (QoS) / Priorisierung

Es gibt zwei QoS-Verfahren, die auf heutigen Industriestandards basieren und uneingeschränkt vom Switch unterstützt werden:

- IEEE802.1p (Layer-2)
- IPv4 / IPv6 (Layer-3)

Ferner wird eine portbasierende Default-Priorisierung unterstützt:

- Default 802.1p Priorityvalue / Default Queue (Portbasierend)

Jeder Switchport besitzt vier Ausgangsqueues. Die Pakete der Queue 0 haben dabei die niedrigste und die der Queue 3 die höchste Priorität.

10.38.1. Priorisierungsschema

Bei der Abarbeitung der einzelnen Queues kann zwischen zwei bzw. vier Priorisierungsschemas ausgewählt werden:

- Strict
- Weighted

Die folgenden beiden Schemas sind nur für neuere Switchtypen verfügbar:

- Strict for Queue 3 / Weighted for Queues 2,1,0
- Strict for Queues 3,2 / Weighted for Queues 1,0

Gemeinsam für alle Schemen ist, dass bei der Abarbeitung der Queues immer mit der höchsten Queue (3) begonnen wird.

Strict:

Hierbei müssen alle Pakete einer Queue versendet sein, bevor Pakete der nächst niedrigeren Queue verarbeitet werden.

Weighted:

Beim Weighted Schema wird nach zwei versandten Paketen einer Queue jeweils ein Paket der nächst niedrigeren Queue versendet. Vergleicht man z.B. die Queue 3 mit der Queue 0, so heißt dies, dass nach acht Paketen der Queue 3 ein Paket der Queue 0 versendet wird. Dieses Verfahren wird auch als 8-4-2-1 Weighted Round Robin bezeichnet.

Strict for Queue 3 / Weighted for Queues 2,1,0:

Hier werden zunächst alle Pakete der Queue 3 versendet, bevor die Pakete der Queues 0, 1 und 2 nach dem Weighted Schema verarbeitet werden.

Strict for Queues 3,2 / Weighted for Queues 1,0:

Hier werden zunächst alle Pakete der Queues 3 und 2 versendet, bevor die Pakete der Queues 0 und 1 nach dem Weighted Schema verarbeitet werden.

10.38.2. Priorisierung nach IEEE802.1p

Die Priorisierung nach IEEE802.1p kann für jeden Port separat aktiviert werden und wertet den IEEE802.1p Priorityvalue in getaggten Empfangspaketen aus um eine der vier internen Queues zuzuweisen.

Hier sind zwei Sonderfälle zu beachten:

- Bei ungetaggte Paketen wird als Priorityvalue der pro Port konfigurierte 'Default 802.1p Priorityvalue' herangezogen und für die Zuweisung der Queue verwendet.
- Falls durch die Funktion „IEEE802.1p VLAN based priority override“ der Priorityvalue gemäß Einstellung in der VLAN Table überschrieben bzw. zugewiesen wurde, so wird dieser Priorityvalue für die Zuweisung der Queue verwendet.

Im IEEE802.1p Standard sind insgesamt acht Priorityvalues für den Tag definiert:

- 0 = Best effort
- 1 = Background
- 2 = Reserved
- 3 = Excellent effort
- 4 = Controlled load
- 5 = Video
- 6 = Voice
- 7 = Network control

Im globalen 'Priority Setup: 802.1p' des Switches kann nun jedem Priorityvalue die gewünschte Queue zugeordnet werden. Möchte man z.B. alle Empfangspakete mit dem Priorityvalue 6:voice vorrangig weiterleiten (weil z.B. IP-Telefone mit IEEE802.1Q/p Unterstützung angeschlossen werden sollen), so muss im 'Priority Setup: 802.1p' die Queue für 6:voice auf einen Wert größer 0 eingestellt werden.

Die Factory Default Einstellung für die oben genannten Priorityvalues ist der Norm IEEE802.1D Kapitel 7.7.3 Tabelle 7-2 entnommen:

Table 7-2—Recommended user priority to traffic class mappings

		Number of available traffic classes							
		1	2	3	4	5	6	7	8
User Priority	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.									

WICHTIG:

Ist für den betreffenden Port die Priorisierung nach IEEE802.1p ausgeschaltet, so wird gemäß dem eingestellten 'Default 802.1p Priorityvalue' die Queue zugewiesen (siehe Kapitel [10.38.5 Port Default 802.1p Priorityvalue](#)).

10.38.3. IEEE802.1p VLAN based Priority Override

Über die Funktion „IEEE802.1p VLAN based Priority Override“ kann der IEEE802.1p Priorityvalue abhängig von der VLAN-ID des empfangenen Paketes überschrieben werden.

Diese Funktion kann pro Port und pro VLAN-ID separat aktiviert werden.

Der grundsätzliche Ablauf ist wie folgt:

- Ein Priority Override findet nur statt, wenn für den Port, auf den das Paket empfangen wurde, die „IEEE802.1p VLAN based Override“ Funktion eingeschaltet ist
- Wird ein ungetaggttes Paket empfangen, so wird dieses dem Default VLAN des betreffenden Ports zugewiesen. Ist für dieses Default VLAN in der VLAN-Table ein „IEEE802.1p VLAN based override value“ eingestellt, so wird der Priorityvalue aus der VLAN-Table übernommen. Ist allerdings in der VLAN-Table der „IEEE802.1p VLAN based override value“ abgeschaltet, so wird der 'Default 802.1p Priorityvalue' des betreffenden Ports verwendet.
- Wird ein getaggttes Paket empfangen, so wird dieses dem VLAN gemäß Tag zugewiesen und überprüft, ob dieses VLAN für den betreffenden Port erlaubt ist und das Paket ggf. weitergeleitet. Ist für dieses VLAN in der

VLAN-Table ein „IEEE802.1p VLAN based Override value“ eingestellt, so wird der empfangene Priorityvalue durch den Priorityvalue aus der VLAN-Table überschrieben. Ist dagegen in der VLAN-Table der „IEEE802.1p VLAN based override value“ abgeschaltet, so sind wiederum zwei Fälle zu unterscheiden:

- Ist für den betreffenden Port die Priorisierung nach IEEE802.1p eingeschaltet, so wird der Priorityvalue gemäß dem empfangenen Tag verwendet
- Ist für den betreffenden Port die Priorisierungen nach IEEE802.1p ausgeschaltet, so wird der 'Default 802.1p Priorityvalue' des betreffenden Ports verwendet.

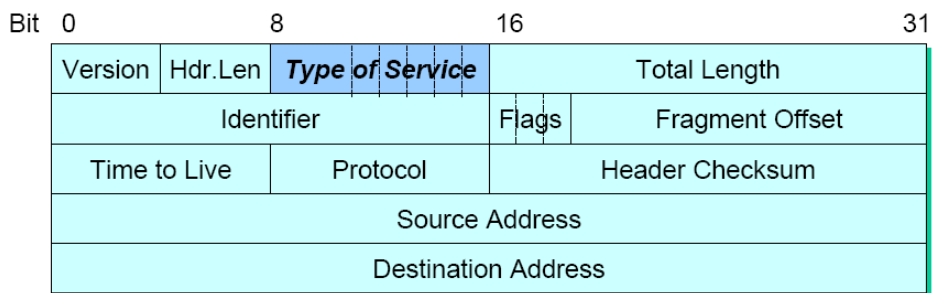
10.38.4. Priorisierung nach IPv4/IPv6

Die Priorisierung nach IPv4/IPv6 kann für jeden Port separat aktiviert werden und wertet das Typ-of-Service Feld (IPv4) bzw. das Traffic-Class Feld (IPv6) der Empfangspakete aus.

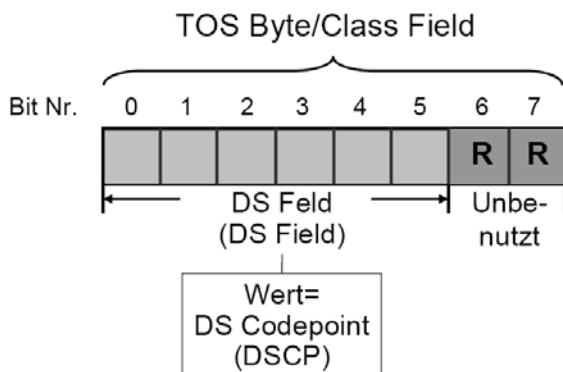
Für beide Protokolle sind jeweils 64 verschiedene Priorityvalues möglich. Im 'Priority Setup: IPv4/IPv6' kann dabei jedem dieser Werte die gewünschte Queue zugeordnet werden.

Wird auf dem betreffenden Port ein IP-Paket empfangen und dieses Paket auf einem anderen Port getaggt gesendet (z.B. ein Uplink mit eingeschaltetem IEEE802.1Q Tagging), so wird die im 'Priority Setup: IPv4/IPv6' eingestellte Queue mit 2 multipliziert und als IEEE802.1p Wert in den Tag eingefügt.

Nachfolgend der Aufbau eines IPv4 Paketheaders:



HINWEIS: Vom Type-of-Service Feld werden nur die ersten sechs Bits ausgewertet, die je nach RFC Standard unterschiedliche Bedeutung haben. Laut den aktuellen Standards RFC2474 und RFC3168 werden diese als DSCP (Differentiated Services Code Point) bezeichnet. Die Zuordnung zwischen Type-of-Service und DSCP zeigt die folgende Abbildung:



HINWEIS:

Das Management Interface sendet alle IPv4 Pakete mit dem DSCP Wert 60. Dadurch lässt sich eine eindeutige IPv4 Priorisierung der Management Pakete im Core Switch konfigurieren.

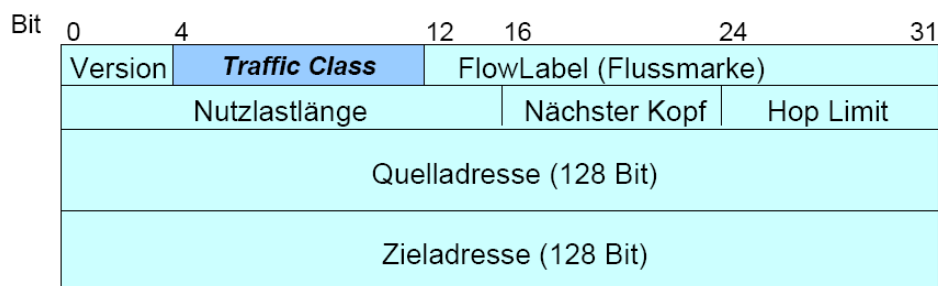
Ein Umrechnung zwischen den alten Bezeichnungen im RFC791 zeigt die folgende Tabelle:

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

Nachfolgend der Aufbau eines IPv6 Paketheaders:



HINWEIS:

Das ' Priority Setup: IPv4/IPv6' ist eine globale Einstellung des Switches und wird für alle Ports mit eingeschalteter IPv4/IPv6 Priorisierung angewendet.

10.38.5. Port Default 802.1p Priorityvalue

Die Default Priorisierung, die auch als portbasierende Priorisierung bezeichnet wird, ist unabhängig vom Inhalt des Empfangspaketes und wird immer dann verwendet, wenn keine der oben aufgeführten Priorisierungsmethoden für das betreffende Empfangspaket zutrifft.

Folgende Einstellungen sind hier möglich:

Default 802.1p Priorityvalue
0 = Best effort
1 = Background
2 = Reserved
3 = Excellent effort
4 = Controlled load
5 = Video
6 = Voice
7 = Network control

Default 802.1p Priorityvalue:

Sind beim betreffenden Port die Priorisierungen nach IEEE802.1p und IPv4/IPv6 ausgeschaltet, so wird ausschließlich gemäß dem eingestellten Default Priorityvalue priorisiert. Als Defaultwert für alle Ports ist „0 = Best effort“ eingestellt, d.h., dass kein Port bevorzugt priorisiert wird (die Pakete werden in der Reihenfolge ihres Eintreffens weitergesendet).

Wird auf dem betreffenden Port ein ungetaggtetes Paket empfangen und dieses Paket auf einem anderen Port getaggt gesendet (z.B. ein Uplink mit eingeschaltetem IEEE802.1Q Tagging) , so wird der eingestellte 'Default 802.1p Priorityvalue' in das Tag eingefügt.

Wichtiger HINWEIS:

Wird auf dem betreffenden Port ein Paket **mit** Tag empfangen, und ist für den betreffenden Port die Priorisierungen nach IEEE802.1p ausgeschaltet, so wird der im Tag enthaltene IEEE802.1p Priorityvalue durch den eingestellten 'Default 802.1p Priorityvalue' überschrieben.

WICHTIG:

Ist für einen bestimmten Port die Priorisierung nach IEEE802.1p oder IPv4/IPv6 eingeschaltet, so wird normalerweise der eingestellte 'Default 802.1p Priorityvalue' ignoriert. Wird allerdings ein Paket empfangen, auf das keine der eingeschalteten Priorisierungsmethoden zutrifft (z.B. IPX-Paket ohne IEEE802.1p-Tag), so wird als Rückfallwert wiederum der 'Default 802.1p Priorityvalue' herangezogen.

Ist die Priorisierung nach IEEE802.1p **und** IPv4/IPv6 eingeschaltet, und ein Paket mit IEEE802.1p-Tag **und** IP-Header empfangen, so wird vorrangig die Priorisierung nach IEEE802.1p durchgeführt.

10.39. Address Ageing Time der Fowarding Tabelle

Über diese Funktion kann eingestellt werden, nach welcher Zeit, die in der Forwarding Tabelle gelernten MAC Adressen, automatisch gelöscht werden.

HINWEIS:

Das Address Ageing der Forwarding Tabelle ist unabhängig von der Portsecurity Ageing Zeit (siehe auch Kapitel [10.36.12. Portsecurity - MAC Adressen Ageing](#)).

10.40. Port Name

Pro Port kann ein beliebiger 'Port Name' mit max. 64 Zeichen eingetragen werden. Dieser Name wird dann in den entsprechenden Tabellen zusätzlich angezeigt und kann z.B. für Hinweise auf das angeschlossene Endgerät verwendet werden.

10.41. Port Typ

Der Port Typ zeigt den physikalischen Schnittstellentyp des betreffenden Ports an.

Folgende Typen sind hier möglich:

- Internal Management Port
- 10/100 Mbit/s Twisted Pair
- 10/100/1000 Mbit/s Twisted Pair
- 100 Mbit/s Fiber Optic
- 1000 Mbit/s Fiber Optic

10.42. Programmierung der Port Status-LEDs

Bei den Teilnehmerports kann die Funktion der Port-LED's programmiert werden. Die Einstellung der LEDs hat dabei keinerlei Einfluss auf die Funktion des Ports.

Für die grüne Port Status-LED können folgende Einstellungen konfiguriert werden:

- Show Link/Activity
 - Permanent aus, falls kein Link-Signal empfangen wird
 - Permanent an, falls ein gültiges Link-Signal empfangen wird
 - Blinkt, falls Daten empfangen bzw. gesendet werden
- Blink (1)
 - Permanentes blinken
- Off
 - Permanent aus
- On
 - Permanent an
- Show Link/Speed-Duplex (1)
 - Permanent aus, falls kein Link-Signal empfangen wird
 - 1x kurzes blinken + Pause, falls 1000-FDX Link-Signal empfangen wird
 - 2x kurzes blinken + Pause, falls 100-FDX Link-Signal empfangen wird
 - 3x kurzes blinken + Pause, falls ein anderes Link-Signal empfangen wird

Für die gelbe Port Status-LED können folgende Einstellungen konfiguriert werden (2):

- Show Full-Duplex
 - Permanent an, falls ein Voll-Duplex Link-Signal empfangen wird
- Show Speed (1)
 - Permanent aus, falls kein Link-Signal empfangen wird
 - 1x kurzes blinken + Pause, falls 10Mbit/s Link-Signal empfangen wird
 - 2x kurzes blinken + Pause, falls 100Mbit/s Link-Signal empfangen wird
 - 3x kurzes blinken + Pause, falls 1000Mbit/s Link-Signal empfangen wird
- Blink (1)
 - Permanentes blinken
- Off
 - Permanent aus
- On
 - Permanent an
- Show PoE-Setup (1)
steht
 - Permanent an, falls das PoE-Setup auf 'Auto 802.3af' oder 'On (Forced)' steht

(1) Diese Funktionen sind nicht für alle Switchtypen bzw. Firmware-Versionen verfügbar.

(2) Die gelbe Port Status-LED ist ausschließlich für Desk und Industrieswitche verfügbar

10.43. Bandwidth-Limiter

Pro Port kann ein 'Bandwidth-Limiter' aktiviert werden.

Konfigurationseinstellungen des Bandwidth-Limiters sind:

- 1) RX Bitrate
- 2) TX Bitrate
- 3) Packet Type

WICHTIG:

Durch Einschalten von VLAN-Port-Mirror wird der Bandwidth-Limiter für alle Ports disabled.

10.43.1. Limiter RX/TX Bitrate

Der Grenzwert für die Bitrate kann für RX und TX getrennt eingestellt werden und ist jeweils in den folgenden Stufen konfigurierbar:

- disable (Factory Default), keine Begrenzung der Datenrate
- 128kbit/s
- 256 kbit/s
- 512 kbit/s
- 1Mbit/s
- 2Mbit/s
- 4Mbit/s
- 8Mbit/s

Für Switche mit Gigabit Ports können außerdem folgende Stufen eingestellt werden:

- 16Mbit/s
- 32Mbit/s
- 64Mbit/s
- 128Mbit/s
- 256Mbit/s

Die Verfahren, nach denen die Limiter für die RX bzw. TX arbeiten, sind teilweise unterschiedlich und sollten beim Einsatz der Limiter berücksichtigt werden:

• RX-Limiter

Das Verfahren hängt von der Einstellung des 'Limiter Paket Type' ab:

a) Bei Einstellung '**Limit all Packet Types (TCP/IP burst compatible)**' kommt das 'Leaky Bucket' Verfahren zum Einsatz. Dabei werden die Pakete in einen Buffer geschrieben und entsprechende der RX Bitrate kontinuierlich weitergeleitet. Die Gesamtgröße des RX Buffers beträgt dabei 112 kByte und wird zwischen allen aktiven Ports dynamisch verteilt.

b) Bei der Einstellung '**Limit all Packet Types**' kommt, im Gegensatz zum Verfahren unter a), pro Port ein Buffer mit einer festen Größe von 1,5 bis 12 kByte zum Einsatz. Die Empfangspakete werden in diesen FIFO-Buffer geschrieben und entsprechend der RX Bitrate weitergeleitet. Durch die geringere Buffergröße als beim Verfahren unter a), ist die Wahrscheinlichkeit, dass Pakete verworfen werden, größer. Dies ist primär vom verwendeten Übertragungsprotokoll und dem damit verbundenen Burst-Traffic abhängig. Dieses Verfahren ist daher primär für kontinuierliche Datenströme wie Video- und Audio-Streams geeignet.

• TX-Limiter

Dieses Verfahren ist unabhängig von der Einstellung des 'Limiter Packet Type'.

Für den TX-Limiter kommt grundsätzlich das 'Leaky Bucket' Verfahren zum Einsatz. Dabei werden die Pakete in einen Buffer geschrieben und entsprechende der TX Bitrate gesendet. Die Gesamtgröße des Buffer beträgt 112 kByte und wird zwischen allen aktiven Ports dynamisch verteilt.

10.43.2. Limiter Packet Type

Der Packet Type bestimmt, auf welche Art von Paketen der Limiter angewendet werden soll.

Hier sind folgende Konfigurationseinstellungen möglich:

- Limit all Packets
- Limit Loop and Broadcast Packets

Limit all Packet Types:

Bei dieser Einstellung werden alle Pakete bei der Berechnung der Datenrate einbezogen. Es können unterschiedliche Grenzwerte für gesendete und empfangene Pakete eingestellt werden.

Limit all Packet Types (TCP/IP burst compatible):

Diese Einstellung ist identisch zur obigen Konfiguration 'Limit all Paket Types', allerdings wird zusätzlich für den RX-Limiter das Traffic-Shaping von burstartigen TCP/IP Datenströmen unterstützt. WICHTIG: Dieses Verfahren benötigt zur optimalen Funktionsweise, dass auf dem betreffenden Port der 'Flow Control State' aktiv ist. Ferner wird dieser Mode nur von bestimmten neueren Switchtypen unterstützt (z.B. GigaSwitch V3, GigaSwitch 54x und iGigaSwitch 54x).

Limit RX Flood-/Broadcast/Multicast Packets Only:

Hier wird der eingestellte Grenzwert ausschließlich auf 'gefloodete' Empfangspakete angewendet. Dies sind entweder Broadcasts/Multicasts oder Unicast-Pakete dessen Ziel-MAC-Adresse unbekannt ist und deshalb auf alle Ports gefloodet werden. HINWEIS: Bei dieser Einstellung kann nur der RX-Limiter aktiviert werden. Der TX-Limiter wird hier automatisch disabled.

10.44. Flow Control

Die Flow-Control Funktion hat die Aufgabe, ein Überlaufen der Paketbuffer im Switch zu verhindern indem er den angeschlossenen Geräten signalisiert, dass sie das Senden einstellen. Dies erfolgt im Halb Duplex-Betrieb durch Simulation einer Kollision oder im Voll Duplex-Betrieb durch Senden spezieller 'Pause'-Pakete.

Die Flow Control Funktion ist Standardmäßig deaktiviert da der Switch genügend Paketbuffer hat um Lastspitzen verlustfrei abzufangen. Die Flow Control Funktion kann bei Bedarf eingeschaltet werden (wird aber nicht empfohlen da es ansonsten zu Netzwerkblockaden durch fehlerhafte Endgeräte kommen kann).

Weiterhin wird der aktuelle Flow-Control Status im WEB, Telnet und NEXMAN angezeigt:

Flow Control State

Bezeichnung	Bedeutung
NOT ACTIVE	Flow Control ist nicht aktiv
ACTIVE	Flow Control ist aktiv

HINWEIS:

Bei Ports im Full-Duplex Betrieb wird die Flow Control Funktion nur dann aktiviert, wenn der Switch und das angeschlossene Endgerät auf {Autoneg} eingestellt sind. Dies gilt auch für **Gigabit** Fiber-Optik Ports, da hier ebenfalls Autonegotiation verwendet wird.

10.45. Layer-2 Discovery Funktionen

10.45.1. Periodisches Senden von Life und Autodiscover Paketen

Die Life-Packet Funktion sendet in periodischen Abständen IP-Broadcastpakete in das Management-VLAN. Das Senden der Pakete wird aktiviert, sobald der Switch eine gültige IP-Adresse per DHCP bezogen hat oder wenn die IP-Adresse fest eingestellt wurde.

Diese Funktion ist z.B. sehr hilfreich, wenn der zentrale Switch eine automatische IP-basierte VLAN-Konfiguration eingestellt hat. Durch das periodische Senden der Life-Pakete wird nämlich verhindert, dass der zentrale Switch das Management-VLAN verlernt weil er die IP-Adresse des Nexans-Switches zu lange nicht mehr sieht.

Der Zeitabstand zwischen den Life-Paketen kann wie folgt eingestellt werden:

- 1 Minute (Factory Default)
- 10 Minuten
- 1 Stunde
- 10 Stunden
- Disable Life Packets
- Disable Life and Autodiscover Packets

Bei der Einstellung 'Disable Life Packets' werden keine Life-Pakete gesendet. Wird die Einstellung 'Disable Life and Autodiscover Packets' verwendet, so werden weder Life noch Autodiscover Pakete versendet. Dies hat zur Folge, dass der Switch nicht über Layer-2, sondern nur noch über Layer-3 Autodiscover gefunden werden kann.

10.45.2. Basic Configurator abschalten

Durch das deaktivieren der Basic Configurator Funktion auf dem Switch, wird sowohl das Lesen, als auch das Schreiben via Basic Configurator unterbunden.

10.46. Funktionseingänge bei Industrie und Office Switchen

Industrie Switches besitzen einen oder mehrere Funktionseingänge. Office Switches der Familie Gigaswitch haben je nach Ausführung einen einzelnen Funktionseingang neben dem Stromversorgungseingang.

Je nach Switchtyp, besitzen die Funktionseingänge eine interne oder externe Hilfsspannung.

Interne Hilfsspannung:

Hier genügt es, die beiden Klemmen des Funktionseingangs über einen externen Schalter (z.B. Türkontakt) kurzzuschließen. Der kurzgeschlossene Zustand wird dann als "aktiv", und der offene Zustand als "inaktiv" angesehen.

Externe Hilfsspannung:

In diesem Fall muss der Eingang mit einer Spannung beaufschlagt werden damit dieser als "aktiv" angesehen wird. Hierfür kann entweder die vom Switch bereitgestellte Hilfsspannung verwendet werden oder eine kundenseitige Spannungsquelle.

Durch die Funktionseingänge können u.a. folgenden Aktionen auszulösen:

- Schalten der lokalen Alarmausgänge (via Alarm Output Mode)
- Schalten der Alarmausgänge eines anderen Switches (via Function Input Alarm Mode / Alarm Output Mode)
- Löschen aller lokalen inaktiven Alarmer der Alarmausgänge (via Function Input Alarm Mode)

- Senden eines Alarms per SNMP-Trap, Remote-Syslog oder Local-Logging (via Alarm Destination Table)

10.46.1. Funktionseingang Alarm Mode

Das Schalten der Alarmausgänge eines anderen Switches kann über den "Function Input Alarm Mode" konfiguriert und erfordert auf der Gegenseite einen Nexans Industrie Switch mit entsprechenden Alarmausgängen. Voraussetzung ist, dass für den Remote Switch der gewünschte Alarmausgang auf den Mode "Function Input from Remote Switch" konfiguriert ist. Weiterhin muss auf beiden Seiten dieselbe "Remote Alarm Group" eingetragen sein und beide Switches müssen sich im selben VLAN bzw. LAN-Segment befinden da der Datenaustausch auf Layer-2 Ebene geschieht.

HINWEIS: Durch einen Funktionseingang können mehrere Alarmausgänge verschiedener Remote Switches gleichzeitig ausgelöst werden, vorausgesetzt, dass alle Alarmausgänge derselben "Remote Alarm Group" zugewiesen sind.

Ferner können über die Funktionseingänge aktive Alarmer der lokalen Alarmausgänge gelöscht werden.

Für den Remote Alarm Mode können folgenden Modi eingestellt werden:

- 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-shortened
- Clear all active Output Alarm when Function Input opened
- Clear all active Output Alarm when Function Input shorted

Disabled:

Funktionseingang abgeschaltet.

Send Alarm when Function Input shorted:

Der Alarmkontakt des Remote Switches wird ausgelöst, wenn der lokale Eingang aktiv wird. Nachdem der Eingang wieder inaktiv wird, bleibt der Alarmkontakt am Remote Switch im Alarmzustand, wird jedoch als inaktiv im Management gekennzeichnet. Dieser muss dann am Remote Switch manuell über den Management Befehl "Clear Alarm" oder einen Funktionseingang des Remote Switches gelöscht werden (siehe unten).

Send Alarm when Function Input shorted / Clear Alarm when re-opened:

Der Alarmkontakt des Remote Switches wird ausgelöst sobald der lokale Eingang aktiv ist. Wird der Eingang wieder inaktiv, wird ebenfalls der Alarm am Remote Switch gelöscht.

Send Alarm when Function Input open:

Hier wird davon ausgegangen, dass der Funktionseingang im Normalzustand aktiv ist. Der Alarmkontakt des Remote Switches wird hier ausgelöst sobald der Eingang inaktiv wird. Nachdem der Eingang wieder aktiv wird, bleibt der Alarmkontakt am Remote Switch im Alarmzustand, wird jedoch als inaktiv im Management gekennzeichnet. Dieser muss dann am Remote Switch manuell über den Management Befehl "Clear Alarm" oder einen Funktionseingang des Remote Switches gelöscht werden (siehe unten).

Send Alarm when Function Input open / Clear Alarm when re-shortened:

Hier wird davon ausgegangen, dass der Funktionseingang im Normalzustand aktiv ist. Der Alarmkontakt des Remote Switches wird hier ausgelöst sobald der Eingang inaktiv wird. Wird der Eingang wieder aktiv, wird ebenfalls der Alarm am Remote Switch gelöscht.

Clear all active Output Alarm when Function Input opened:

Wenn der Funktionseingang inaktiv wird, werden alle inaktiven Alarmer der lokalen Alarmkontakte gelöscht.

Clear all active Output Alarm when Function Input shorted:

Wenn der Funktionseingang aktiv wird, werden alle inaktiven Alarmer der lokalen Alarmkontakte gelöscht.

10.47. Alarmausgänge bei Industrie Switchen

Die Nexans Industrieswitches besitzen zwei potentialfreie Alarmausgänge die mit M1 und M2 bezeichnet sind.

Für jeden Ausgang kann separat einer der folgenden Modi eingestellt werden:

- Link Down
- Forced On
- Forced Off
- Function Input from Remote Switch
- Alarm Destination from Remote Switch
- Alarm Destination from Local Switch

Die folgenden Modi werden nur von Industrie Switches unterstützt:

- Power Input S1 failed
- Power Input S2 failed
- Power Input S1 or S2 failed
- Function Input shorted
- Function Input open

Link Down:

Hierbei wird der Alarmausgang geschaltet, wenn der Link eines oder mehrerer Ports ausgefallen ist. Dabei kann über die Parameter 'Link Down Alarm M1' bzw. 'Link Down Alarm M2' für jeden Port separat eingestellt werden, ob ein Linkausfall auf dem betreffenden Port zu einem Alarm an Ausgang M1 und/oder M2 führen soll.

Forced On:

Hier wird der Alarmausgang permanent eingeschaltet {On}.

Forced Off:

Hier wird der Alarmausgang permanent ausgeschaltet {Off}.

Die Funktionen **Forced On** und **Forced Off** können z.B. zur gezielten Ansteuerung von Aktoren verwendet werden.

Function Input from Remote Switch:

Hier wird der Alarmausgang in Abhängigkeit vom Funktionseingang eines anderen Nexans Industrie Switches gesteuert. Voraussetzung ist, dass der Funktionseingang entsprechend konfiguriert wurde und derselben Remote Group zugewiesen ist. Ferner müssen sich beide Switches im selben VLAN bzw. Segment befinden da der Datenaustausch auf Layer-2 Ebene geschieht.

Alarm Destination from Remote Switch:

Hier wird der Alarmausgang in Abhängigkeit von der Alarm Destination Table eines anderen Nexans Switches gesteuert (dies kann auch ein Office Switch sein). Voraussetzung ist, dass der "Destination Type" in der Alarm Destination Table auf "Remote Alarm Output M1/M2" konfiguriert wurde und dort die korrekte IP Adresse eingestellt ist. Die beiden Switches dürfen dabei in verschiedenen VLANs sein weil der Datenaustausch auf Layer-3 Ebene geschieht.

Alarm Destination from Local Switch:

Hier wird der Alarmausgang in Abhängigkeit von der eigenen Alarm Destination Table gesteuert. Voraussetzung ist, dass der "Destination Type" in der Alarm Destination Table auf "Local Alarm Output M1/M2" konfiguriert wurde. Die dort eingestellte IP Adresse wird dabei ignoriert.

Power Input S1 failed:

Hier wird der betreffende Alarmausgang geschaltet, wenn die Spannung an Power Input S1 ausfällt.

Power Input S2 failed:

Hier wird der betreffende Alarmausgang geschaltet, wenn die Spannung an Power Input S2 ausfällt.

Power Input S1 or S2 failed:

Hier wird der betreffende Alarmausgang geschaltet, wenn die Spannung an Power Input S1 oder S2 ausfällt.

Function Input shorted:

Der betreffende Alarmausgang wird geschaltet, wenn der Funktionseingang aktiv ist.

Function Input open:

Der betreffende Alarmausgang wird geschaltet, wenn der Funktionseingang inaktiv ist.

10.48. Telnet Console Authentication Mode

Für Telnet können sechs verschiedene Authentifizierungs-Modi eingestellt werden:

- Local: Lokale Authentifizierung
- Disabled: Telnet Interface disabled
- Radius only: Authentifizierung ausschließlich durch den RADIUS Server
- Radius first, then local: Authentifizierung durch RADIUS, nur falls kein Server antwortet: lokale Authentifizierung
- TACACS+ only: Authentifizierung ausschließlich durch den TACACS+ Server
- TACACS+ first, then local: Authentifizierung durch TACACS+, nur falls kein Server antwortet: lokale Authentifizierung

Local (Factory-Default):

Im Switch ist je ein Name und ein Passwort für den Admin- und User-Access gespeichert (siehe Kapitel [10.5. Admin / User Accounts beim Management Zugriff](#)). Diese Daten werden per Factory-Default beim Telnet

Login zur Authentifizierung herangezogen und mit dem eingegebenen Login-Namen und Login-Passwort verglichen.

Disabled:

Das Telnet Interface ist abgeschaltet. Jeder Verbindungsaufbau auf dem Telnet TCP Port wird vom Switch abgelehnt.

Radius only:**Radius first, then local:**

Diese Modi sind ausschließlich bei Firmware-Versionen mit RADIUS Unterstützung auswählbar.

Siehe Kapitel [10.56. RADIUS Console Authentication Modes](#).

TACACS+ only:**TACACS+ first, then local:**

Diese Modi sind ausschließlich bei Firmware-Versionen mit TACACS+ Unterstützung auswählbar.

Siehe Kapitel [10.64 TACACS+ Console Authentication Modes](#).

HINWEIS:

Nach dreimaliger falscher Eingabe von Name oder Passwort, werden alle Console Interfaces (SSH, TELNET und ggf. V.24) für 60 Sekunden gesperrt.

10.49. SSHv2 Console Authentication Mode

Für SSHv2 können sechs verschiedene Authentifizierungs-Modi eingestellt werden:

- Local: Lokale Authentifizierung
- Disabled: SSHv2 Interface disabled
- Radius only: Authentifizierung ausschließlich durch den RADIUS Server
- Radius first, then local: Authentifizierung durch RADIUS, nur falls kein Server antwortet: lokale Authentifizierung
- TACACS+ only: Authentifizierung ausschließlich durch den TACACS+ Server
- TACACS+ first, then local: Authentifizierung durch TACACS+, nur falls kein Server antwortet: lokale Authentifizierung

Local (Factory-Default):

Im Switch ist je ein Name und ein Passwort für den Admin- und User-Access gespeichert (siehe Kapitel [10.5. Admin / User Accounts beim Management](#) Zugriff). Diese Daten werden per Factory-Default beim SSH Login zur Authentifizierung herangezogen und mit dem eingegebenen Login-Namen und Login-Passwort verglichen.

Disabled:

Das SSHv2 Interface ist abgeschaltet. Jeder Verbindungsaufbau auf dem SSH TCP Port wird vom Switch abgelehnt.

Radius only:**Radius first, then local:**

Diese Modi sind ausschließlich bei Firmware-Versionen mit RADIUS Unterstützung auswählbar.

Siehe Kapitel [10.56. RADIUS Console Authentication Modes](#).

TACACS+ only:**TACACS+ first, then local:**

Diese Modi sind ausschließlich bei Firmware-Versionen mit TACACS+ Unterstützung auswählbar.

Siehe Kapitel [10.64 TACACS+ Console Authentication Modes](#).

HINWEIS:

Nach dreimaliger falscher Eingabe von Name oder Passwort, werden alle Console Interfaces (SSH, TELNET und ggf. V.24) für 60 Sekunden gesperrt.

10.50. SCP Authentication Mode

Für die SCP können sieben verschiedene Authentifizierungs-Modi eingestellt werden:

- Local Lokale Authentifizierung
- Radius only Authentifizierung ausschließlich durch den RADIUS Server

- Radius first, then local Authentifizierung durch RADIUS, nur falls kein Server antwortet: lokale Authentifizierung
- TACACS+ only Authentifizierung ausschließlich durch den TACACS+ Server
- TACACS+ first, then local Authentifizierung durch TACACS+, nur falls kein Server antwortet: lokale Authentifizierung
- Use SSHv2 mode Es wird der SSHv2 authentication mode benutzt
- Disabled SCP Interface deaktiviert

Local:

Im Switch ist je ein Name und ein Passwort für den Admin- und User-Access gespeichert (siehe Kapitel [10.5. Admin / User Accounts beim Management Zugriff](#)). Diese Daten werden per Factory-Default beim SCP Login zur Authentifizierung herangezogen und mit dem eingegebenen Login-Namen und Login-Passwort verglichen.

Disabled:

Das SCP Interface ist abgeschaltet. Jeder Verbindungsaufbau auf dem SCP TCP Port wird vom Switch abgelehnt.

Radius only:**Radius first, then local:**

Diese Modi sind ausschließlich bei Firmware-Versionen mit RADIUS Unterstützung auswählbar. Siehe Kapitel [10.58 RADIUS SCP Authentication Modes](#).

TACACS+ only:**TACACS+ first, then local:**

Diese Modi sind ausschließlich bei Firmware-Versionen mit TACACS+ Unterstützung auswählbar. Siehe Kapitel [10.66 TACACS+ SCP Authentication Modes](#).

Use SSHv2 mode (Factory-Default):

Hier wird der unter SSHv2 Console Authentication Mode eingetragene Authentication Mode benutzt.

10.51. Console Password Mode

Über den 'Console Password Mode' kann eingestellt werden, ob das Passwort während der Telnet und V.24 Eingabe angezeigt wird oder nicht. Dies ist z.B. bei Verwendung eines RADIUS Servers sinnvoll, wenn One-Time-Passwörter verwendet werden und das eingegebene Passwort nur einmal verwendet werden kann.

Mögliche Einstellungen sind:

- Invisible (Default)
- Visible

10.52. Statistic- / RMON-Counter

Mittels NEXMAN, Telnet/SSH/V.24-Console und SNMP können umfangreiche Statistic Counter pro Port abgerufen werden.

Folgende Counter werden unterstützt:

- 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

Die oben mit einen (*) gekennzeichneten Counter sind in 64 Bit ausgeführt. Ein Überlaufen dieser Counter ist praktisch ausgeschlossen. Die Ausgabe als 64 Bit Wert erfolgt auf allen Management-Interfaces, incl. der SNMP High-Capacity-Counter.

Per SNMP sind die Counter über folgende Standard-MIBs abrufbar:

- MIB-II: interfaces
- IF-MIB: ifXTable
- BRIDGE-MIB: dot1dTpPortTable
- EtherLike-MIB: dot3StatsTable
- RMON-MIB: statistics

Für eine Übersicht aller SNMP-MIBs siehe Kapitel [10.53.7. SNMP MIB Übersicht](#).

10.53. SNMP Unterstützung

10.53.1. SNMP Protocol Version

Hierüber wird eingestellt, über welche SNMP Protokolle auf die SNMP-MIB des Switches zugegriffen werden darf.

Für die SNMP Protocol Version kann zwischen folgenden Einstellungen ausgewählt werden:

- 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:

Der Zugriff auf die SNMP-MIB ist ausschließlich per SNMP Version1 erlaubt. Für die Authentifizierung wird die Community des Paketes ausgewertet und überprüft.

SNMPv2c:

Der Zugriff auf die SNMP-MIB ist ausschließlich per SNMP Version 2c erlaubt. Für die Authentifizierung wird die Community des Paketes ausgewertet und überprüft.

SNMPv1 and SNMPv2c:

Der Zugriff auf die SNMP-MIB ist per SNMP Version 1 und Version 2c erlaubt. Für die Authentifizierung wird die Community des Paketes ausgewertet und überprüft.

SNMPv3[Auth.-MD5][No Priv.]:

Der Zugriff auf die SNMP-MIB ist ausschließlich per SNMP Version 3 erlaubt. Für die Authentifizierung werden der Username und der MD5-Passwort-Hash des Paketes ausgewertet und überprüft. Eine Verschlüsselung der Daten findet nicht statt.

SNMPv3[Auth.-MD5][Priv.-DES]:**SNMPv3[Auth.-MD5][Priv.-AES-128]:**

Der Zugriff auf die SNMP-MIB ist ausschließlich per SNMP Version 3 erlaubt. Für die Authentifizierung werden der Username und MD5-Passwort-Hash des Paketes ausgewertet und überprüft. Eine Verschlüsselung der Daten findet mit dem Verschlüsselungsalgorithmus DES bzw. AES statt.

SNMPv3[Auth.-SHA][No Priv.]:

Der Zugriff auf die SNMP-MIB ist ausschließlich per SNMP Version 3 erlaubt. Für die Authentifizierung werden der Username und SHA-Passwort-Hash des Paketes ausgewertet und überprüft. Eine Verschlüsselung der Daten findet nicht statt.

SNMPv3[Auth.-SHA][Priv.-DES]:**SNMPv3[Auth.-SHA][Priv.-AES-128]:**

Der Zugriff auf die SNMP-MIB ist ausschließlich per SNMP Version 3 erlaubt. Für die Authentifizierung werden der Username und SHA-Passwort-Hash des Paketes ausgewertet und überprüft. Eine Verschlüsselung der Daten findet mit dem Verschlüsselungsalgorithmus DES bzw. AES statt.

SNMPv3[Auth.-SHA][No Priv.] with SNMPv1/SNMPv2c read/only access:**SNMPv3[Auth.-SHA][Priv.-AES-128] with SNMPv1/SNMPv2c read/only access:**

Diese Einstellungen erlaubt für SNMPv3 einen Lese- und Schreibzugriff und gleichzeitig für SNMPv1 und SNMPv2c einen ausschließlichen Lesezugriff. Dies ermöglicht z.B. die Änderung von Parametern über das sichere SNMPv3 Protokoll während die Abfrage von Parametern über das weniger komplexe Protokoll SNMPv1 oder SNMPv2c ausgeführt werden kann.

10.53.2. SNMP Access Mode

Für den SNMP Zugriff können folgende Modi eingestellt werden:

- Read/Write: Read/Write Zugriff erlaubt
- Read/Only Read/Only Zugriff erlaubt
- SNMP disabled: SNMP Interface disabled

Read/Write (Factory-Default):

Bei dieser Einstellung ist Read und Write Access per SNMP erlaubt.

Read/Only:

Hierbei ist ausschließlich Read Access per SNMP erlaubt.

SNMP disabled:

Das SNMP Interface ist abgeschaltet.

10.53.3. SNMPv1/v2c Communities

Bei SNMPv1 und SNMPv2c werden die Read/Only- und Read/Write-Community entsprechend ausgewertet und müssen in der SNMP Management Station korrekt eingestellt sein. Bei falscher Angabe der Community liefert der Switch den Fehler 'No Such Name' bzw. 'Read/Only'.

Die Standardvorgaben für die Communities sind:

- Read/Only Community: public
- Read/Write Community: nexans
- Trap Community: public (falls diese leer ist, wird die Read/Only Community verwendet)

Folgende ASCII Zeichen sind für die Community Namen zulässig und werden in den Eingabemasken von WEB, CLI und Manager überprüft:

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

Die einzigen Ausnahmen sind die folgenden ASCII Zeichen:

? (ASCII 63) Wird im CLI Interface grundsätzlich als Hilfe-Kommando interpretiert

` (ASCII 96) Hier muss der Benutzer die Tastenfuge <shift + `> + <space> drücken, was nicht praktikabel ist

10.53.4. SNMPv1 MAC Table Mode

Für den SNMP MAC Table Mode können folgende Modi eingestellt werden:

- List MAC's of all port: MACs aller Ports werden gelistet
- List only MAC's of user ports: Nur MACs der User-Ports werden gelistet

Dieser Parameter steht per Factory Default auf 'List MAC's of all port'. Wenn diese Einstellung auf 'List only MAC's of user ports' konfiguriert wird, so listet die SNMP MAC Table nur noch solche MAC Adressen, die sich auf den User Ports befinden. Über die Einstellung 'Link type' kann definiert werden, welche Ports 'User Ports' bzw. 'Uplink Ports' sind. Per Factory Default sind Fiber Ports als Uplink Port konfiguriert und die anderen Ports als User Ports.

HINWEIS: Diese Einstellung ist nur für den SNMPv1 Zugriffe relevant. Bei SNMPv2c und SNMPv3 wird grundsätzlich der Mode "List MAC's of all port" verwendet.

10.53.5. SNMPv3 Engine ID

Die SNMPv3 Engine ID ist Teil des SNMPv3 Netzwerk Protokolls und dient der Identifizierung des Switch SNMP Agents gegenüber dem SNMP Manager. Diese ID kann manuell mittels Parameter "Engine ID" konfiguriert werden. Die Eingabe muss dabei in HEX Notation erfolgen.

Falls keine Engine ID manuell konfiguriert ist, verwendet der Switch eine automatisch generierte und eindeutige MAC basierte ID mit der folgenden Syntax (in HEX Notation):

8000010A03xxxxxxxxxx

Mit den folgenden Bestandteilen:

8000 (SNMPv3 Protokoll Identifikation)

010A (Nexans Enterprise ID)

03 (MAC Adressen Schema)

xxxxxxxxxx (Switch MAC Adresse, sechs HEX Bytes)

10.53.6. SNMPv3 User Setup

Über das SNMPv3 User Setup können die Usernamen und Passwörter für die SNMP Authentifizierung konfiguriert werden.

Hier stehen vier User Accounts zur Verfügung:

- Read/Write User Account: voller Read/Write Access auf die MIB
- Read/Only User Account: Read/Only Access auf die MIB
- Flexible User Account: Wahlweise Read/Write oder Read/Only Access auf die MIB
- Trap User Account: Wird zum versenden von SNMPv3 Traps verwendet

Für jeden Account keine jeweils ein Username und Passwort eingestellt werden. Diese sind im Auslieferungszustand leer, d.h., ein Zugriff per SNMPv3 ist mit Werkseinstellungen nicht möglich.

Folgende ASCII Zeichen sind für Usernamen und Passwörter zulässig und werden in den Eingabemasken von WEB, CLI und Manager überprüft:

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

Die einzigen Ausnahmen sind die folgenden ASCII Zeichen:

? (ASCII 63) Wird im CLI Interface grundsätzlich als Hilfe-Kommando interpretiert

` (ASCII 96) Hier muss der Benutzer die Tastenfolge <shift + `> + <space> drücken, was nicht praktikabel ist

10.53.7. SNMP MIB Übersicht

Die nachfolgende Übersicht zeigt alle implementierten MIBs und die jeweils unterstützten Gruppen. Die einzelnen Variablen der MIBs sind nicht einzeln aufgeführt, können aber den jeweiligen MIB Dateien entnommen werden.

HINWEIS:

Die unten aufgeführten MIBs sind z.T. im ZIP-Archiv des Update-Files enthalten (siehe Spalte 1).

Für die Nexans Switches sind zwei MIB-Dateien relevant:

- **NEXANS-MIB.mib** - Globale MIB für alle Nexans Produkte
- **NEXANS-BM-MIB.mib** - Produktspezifische MIB für Nexans Office und Industrie Switches

a) Bezeichnung b) Dateiname	RFC	MIB OID
a) NEXANS-MIB NEXANS-BM-MIB b) NEXANS-MIB.mib NEXANS-BM-MIB.mib		<pre> 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) </pre>

		<pre> 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) </pre>
--	--	--

		<pre> 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) sfpInfoWavelength(9) sfpInfoLength9um(10) sfpInfoLength50um(11) sfpInfoLength62um(12) sfpInfoConnectorDescr(13) sfpDiagTemperature(14) sfpDiagSupplyVoltage(15) sfpDiagTxBiasCurrent(16) sfpDiagTxOutputPower(17) sfpDiagTxOutputPowerDbm(18) sfpDiagRxInputPower(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) </pre>
--	--	--

		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	..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)

		<pre> 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) </pre>
a) Q-BRIDGE-MIB b) Q-BRIDGE.mib	4188	<pre> 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) </pre>
a) RSTP-MIB b) RSTP.mib	4318	<pre> iso(1).org(3).dod(6).internet(1).. ..mgmt(2) mib-2(1) dot1dBridge(17) dot1dStp(1) </pre>

		<pre> dot1dStpVersion(16) dot1dStpTxHoldCount(18) dot1dStpExtPortTable(19) dot1dStpExtPortEntry(1) dot1dStpPortProtocolMigration(1) dot1dStpPortAdminEdgePort(2) dot1dStpPortOperEdgePort(3) dot1dStpPortAdminPointToPoint(4) dot1dStpPortOperPointToPoint(5) dot1dStpPortAdminPathCost(6) </pre>
a) EtherLike-MIB b) ETHERLIKE.mib	2665	<pre> 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) </pre>
a) RMON-MIB b) RMON.mib	2819	<pre> 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) </pre>
a) ENTITY-MIB b) ENTITY-MIB.mib	6933	<pre> 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) </pre>

		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)

		<pre> lldpRemPortDesc(8) lldpRemSysName(9) lldpRemSysDesc(10) lldpRemSysCapSupported(11) lldpRemSysCapEnabled(12) lldpRemManAddrTable(2) lldpRemManAddrEntry(1) lldpRemManAddrSubtype(1) lldpRemManAddr(2) lldpRemManAddrIfSubtype(3) lldpRemManAddrIfId(4) lldpRemManAddrOID(5) </pre>
a) LLDP-EXT-MED-MIB b) LLDP-MED.mib		<pre> 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) </pre>

10.54. Alarm Destination Table

In der Alarm Destination Table können bis zu acht Empfänger für Alarime eingetragen werden. Für jeden Empfänger kann dabei separat ausgewählt werden, welche Alarmtypen relevant sind.

Für jeden Empfänger kann separat eingestellt werden, welcher der folgenden Destination-Typen versendet werden soll:

- SNMPv1 Trap
- SNMPv2 Trap
- SNMPv3 Trap
- SYSLOG Server
- Local Logging
- Remote Alarm Output M1
- Remote Alarm Output M2

Die folgenden Destination-Typen sind ausschließlich bei Industrie Switchen verfügbar:

- Local Alarm Output M1
- Local Alarm Output M2

SNMPv1 Trap:

SNMPv2 Trap:

Versendet einen SNMPv1 bzw. SNMPv2 Trap an die konfigurierte IP-Adresse.

SNMPv3 Trap:

Versendet einen SNMPv3 Trap an die konfigurierte IP-Adresse. Voraussetzung dafür ist, dass die SNMP Protocol Version auf SNMPv3 konfiguriert ist und ein passender Trap Account (Username und Password) eingestellt ist.

Wichtiger HINWEIS: Bei reinen SNMPv3 Trap Receivern kann es u.U. erforderlich sein, die sogenannte SNMPv3 Engine ID des Switches im Trap Receiver einzugeben damit die empfangenen Traps decrypted werden können. Falls die SNMP Protocol Version auf SNMPv3 konfiguriert ist, kann die SNMPv3 Engine ID über das CLI Kommando "show configuration access" bzw. "show run" angezeigt werden (siehe Abschnitt "ACCESS SNMP" in der CLI Ausgabe).

SYSLOG Server:

Versendet eine SYSLOG Meldung an die konfigurierte IP-Adresse. Die SYSLOG Severity kann dabei für jeden

Alarmtyp separat eingestellt werden. Desweiteren kann die Syslog Facility auf einen Wert zwischen 1 und 31 geändert werden. Die folgenden Werte sind laut RFC 3164 vordefiniert:

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:

Hier werden die Alarme im lokalen Logbuch gespeichert. Dieses kann, abhängig von der Länge der jeweiligen Alarmtexte, ca. 500-1000 Alarme speichern. Über den **Local Logging Mode** kann eingestellt werden, ob bei Überlauf die ältesten Einträge überschrieben oder das logging gestoppt werden soll. Ferner kann das lokale Logging global abgeschaltet werden.

Das Logbuch kann per WEB, Telnet/SSH/V.24-Console und Manager angezeigt werden. Weiterhin kann es via SCP gelesen werden. Hier gilt folgende 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:

Hier wird der Alarmausgang M1 bzw. M2 eines Remote Nexans Industrie Switches gesteuert. Voraussetzung ist, dass die korrekte IP Adresse des Remote Switches eingestellt ist und der Alarm Output des betreffenden Remote Switches auf "Alarm Destination from Remote Switch" konfiguriert wurde.

Local Alarm Output M1:

Local Alarm Output M2:

Hier wird der eigene Alarmausgang M1 bzw. M2 gesteuert. Voraussetzung ist, dass der Alarm Output auf "Alarm Destination from Local Switch" konfiguriert wurde. Eine evt. eingestellte IP Adresse wird ignoriert.

HINWEIS:

Zum Testen der SNMP-Traps, der Syslog-Meldungen und des Local Logging kann im NEXMAN auf dem Reiter "Alarms > Alarm Destinations" die Funktion "Test Traps/Syslog" oder das Console Kommando 'test - traps - sys log' verwendet werden. Der Switch sendet daraufhin von jedem Event-Typ einen Trap bzw. eine Syslog Meldung an alle IP-Adressen der Destination Table, oder im Fall des Local Logging zum internen Logbuch. Dies ermöglicht die Kontrolle der Darstellung im SNMP-Manager, im Syslog-Server bzw. im lokalen Logbuch. Es werden dabei nur die Event-Typen versendet, die vom jeweiligen Switchtyp und von der installierten Firmware unterstützt werden.

Die nachfolgende Tabelle enthält eine Übersicht aller Event-Typen:

Event-Typ	Trap-Art	Trap wird gesendet ...
Cold Start	Standard Trap	Bei Einschalten oder reboot des Switches Mit jedem "Cold Start" Event wird eine "Source" im Local Log und im Remote-Syslog angegeben

		(nicht für SNMP-Traps). Beispiele: Cold Start: Source= Software reboot via config buttons Cold Start: Source= Power up or Power interruption Wenn die "Source" mit "Unkown" markiert ist, wurde der Reset durch eine Software- oder Hardwarefehlfunktion verursacht. In diesem Fall zeigt "Reset Reason" eine Nummer an, die nur für den Herstellersupport von Nutzen ist. Beispiel: Cold Start: Source=Unknown [Reset reason=0x02000] Wenn ein solcher Reset häufig auftritt, aktualisieren Sie bitte zuerst die Switch-Firmware auf die neueste Firmware-Version. Wenn das Problem dadurch nicht behoben wird, muss das Managementmodul im Werk überprüft werden.
Link Up	Standard Trap	Bei Link-Änderung eines Ports von Down nach Up
Link Down	Standard Trap	Bei Link-Änderung eines Ports von Up nach Down
RSTP New Root	Standard Trap	Wenn sich dieser Switch als neue Root Bridge selektiert hat. Dies geschieht direkt nach dem booten und wenn der Switch für eine bestimmte Zeit keine BPDU Pakete von einem benachbarten Switch (mit einer höheren Bridge-Priorität) empfangen hat.
RSTP Topology Change	Standard Trap	Bei einer Topologieänderung bei eingeschaltetem Rapid Spanning Tree
Temperature Failure	Enterprise Trap 1	Bei Über- bzw. Unterschreitung der konfigurierten Temperaturgrenzen. HINWEIS: Solange eine Verletzung der Grenzen besteht, wird dieses Event in Abständen von fünf Minuten gesendet.
Link Change	Enterprise Trap 2	Bei Link-Änderung eines Ports mit Angabe von Datenrate und Duplex-Mode
New MAC Address	Enterprise Trap 3	Bei Lernen einer neuen MAC-Adresse auf einem Port mit eingeschalteter Portsecurity. Gilt nicht für die Modi {Manual setting ...} und {IEEE802.1X allow multiple MAC-Addresses}
Portsecurity-Failure	Enterprise Trap 4	Bei Erkennen einer unzulässigen Mac-Adresse auf einen Port mit eingeschalteter Portsecurity (siehe auch Kapitel 10.36.1. Portsecurity - Failure Action)
Port Error Counter Failure	Enterprise Trap 5	Bei Inkrementierung des Port-Error-Counters um 2 oder mehr innerhalb eines Zeitfensters von 2 Sekunden. HINWEIS: Wird nur in Abständen von fünf Minuten gesendet um bei massiven Fehlern einen Sturm von SNMP Traps zu vermeiden.
Management Authentication Info	Enterprise Trap 6	Beim Versuch eines IP Gerätes auf das Switch Management zuzugreifen. Diese Info enthält die IP-Adresse, den authentifizierten Benutzernamen, den Authentifizierungsstatus (OK, FAILURE) und das Interface über das der Zugriff erfolgte (SSH, TELNET, V.24, WEB, SNMP, SCP oder Manager). Im Falle eines Authentifizierungsfehlers ist auch der Grund (falscher Benutzer / Passwort für Telnet / ssh / V.24, falsche Community für SNMP-Lese- / Schreibzugriff oder falsche Zugriffsrechte gemäß IPv4/IPv6 Accesslist) enthalten.

Radius Management Authentication Reject	Enterprise Trap 7	Bei Abweisung des Telnet/SSH/V.24-Console oder NEXMAN Login durch den RADIUS Server
Radius Portsecurity Reject	Enterprise Trap 8	Bei Abweisung eines Portsecurity Access-Request durch den RADIUS Server
Port Broadcast Failure	Enterprise Trap 9	Bei unzulässig hohem Broad-/Multicast Empfang auf einem TP-Teilnehmerport. (> 25 Pakete / Sekunde für länger als 10 Sekunden). WICHTIG: Dieser Trap wird nicht für Ports versendet, dessen Link-Typ auf {Uplink/Downlink} eingestellt ist.
Switch PoE Voltage Failure	Enterprise Trap 10	Bei Unterschreitung bzw. Überschreitung der konfigurierten zulässigen PoE Eingangsspannungsgrenzen. HINWEIS: Dieser Trap wird ausschließlich für Switches mit installierter PoE-Option unterstützt
Switch PoE Overload Failure	Enterprise Trap 11	Bei Überschreitung des PoE Powerlimits für die Gesamtleistungsaufnahme HINWEIS: Dieser Trap wird ausschließlich für Switches mit installierter PoE-Option unterstützt
Port PoE Overload Failure	Enterprise Trap 12	Bei Überschreitung des PoE Powerlimits für einen einzelnen Port HINWEIS: Dieser Trap wird ausschließlich für Switches mit installierter PoE-Option unterstützt
Port Loop Detected	Enterprise Trap 13	Bei Erkennen einer Loop zwischen zwei Ports durch die 'Active Loop Protection'. Bei diesem Fehler wird der betreffende Port sofort abgeschaltet.
Industrial Alarm M1	Enterprise Trap 14	Bei Änderung des M1 Alarmstatus mit Angabe des aktuellen Status (on bzw. off)
Industrial Alarm M2	Enterprise Trap 15	Bei Änderung des M2 Alarmstatus mit Angabe des aktuellen Status (on bzw. off)
Internal Voltage Failure	Enterprise Trap 16	Bei Über- bzw. Unterschreitung der zulässigen Grenzen für die beiden internen Versorgungsspannungen 2,5V und 3,3V. HINWEIS: Solange eine Verletzung der Grenzen besteht, wird dieser Event in Abständen von fünf Minuten gesendet.
TFTP Message	Enterprise Trap 17	Bei erfolgreichem oder fehlgeschlagenem TFTP Transfers einer Konfigurationsdatei. Dies gilt nicht für TFTP Transfers, die direkt durch den Nexans Switch Manager ausgeführt werden, da diese im Logbuch des Managers dokumentiert werden.
SFP Event	Enterprise Trap 18	Bei Entfernen oder Stecken eines SFP Moduls und bei Verletzung der SFP Alarmlimits für RX-Power, TX-Power oder Laser-Bias-Current. HINWEIS: Solange eine Verletzung von mindestens einem Alarmlimits besteht, wird dieses Event in Abständen von fünf Minuten gesendet.
Client Remove Alarm	Enterprise Trap 19	Bei dauerhaftem entfernen eines Endgerätes vom Port (Diebstahlschutz).
Internal Management Warning	Enterprise Trap 20	Bei internen Unregelmäßigkeiten (z.B. verfügbarer RAM Speicher zu gering, Probleme beim Zugriff

		auf die Switchengine etc.). Die Warning besteht dabei aus einem Code und einem Value. Der Code beinhaltet dabei den Typ der Warning und der Value den zugehörigen internen Wert. HINWEIS: Diese Warning wird für bestimmte kritische Zustände, unabhängig von der Aktivierung in der Destination Table, grundsätzlich gesendet. Im nachfolgenden werden einige Warningcodes erläutert. Ist der gemeldete Warningcode nicht aufgeführt sein, so sollte der Support des Herstellers kontaktiert werden. Code=101: Die Empfangs Paketpuffer des Management Prozessors sind für einen Zeitraum von ca. 100 Sekunden permanent ausgeschöpft. Falls diese Warning nur sporadisch auftaucht, deutet dies auf eine temporär hohe Broadcast- oder Multicast-Netzlast im Management VLAN hin. Hier sollte geklärt werden, wer der Verursacher für diese hohe Broadcast-/Multicast Netzlast ist. Code=104: Erkennung von Fehlern in der Ethernetanbindung des Prozessors an den Switching Chip. Falls diese Anbindung gestört ist, kann dies zu schweren Fehlern in redundanten Netzwerktopologien führen. Insbesondere besteht die Gefahr von Loops weil geblockte Ports fälschlicherweise auf Forwarding geschaltet werden. Hier sollte unbedingt Kontakt mit dem Support des Herstellers aufgenommen werden. Code=105: Ein Firmwareupdate ist fehlgeschlagen. Der angegebene Wert gibt dabei die Ursache an: 1 oder 2: Die übertragene Firmware ist korrupt oder nicht passend für den Switchtyp. 3: Die übertragene Firmware ist zu alt für den Switchtyp.
Function Input Alarm	Enterprise Trap 21	Bei Statusänderung des Funktionseingangs von Open nach Shorted bzw. von Shorted nach Open
Configuration Changed Info	Enterprise Trap 22	Bei Änderung der Switch Configuration. Diese Info enthält die IP-Adresse, den authentifizierten Benutzernamen und das Interface über das die Änderung ausgelöst wurde (SSH, TELNET, V.24, WEB, SNMP, SCP oder Manager).
Port Error Disabled	Enterprise Trap 23	Bei Abschaltung des Ports aufgrund eines Fehlers, Die Ursache der Abschaltung wird in der Alarmmeldung übermittelt.
Port State Changed	Enterprise Trap 24	Bei Änderung des Port Status von Blocking nach Forwarding oder umgekehrt.

10.55. RADIUS Authentication

Der Switch unterstützt das RADIUS Authentifizierungs-Protokoll gemäß RFC2865.

Dieses Protokoll wird für folgende Authentifizierungsaufgaben im Switch verwendet:

- Telnet Authentifizierung von Name/Passwort
- SSHv2 Authentifizierung von Name/Passwort

- V.24 Authentifizierung von Name/Passwort
- Manager Authentifizierung von Name/Passwort
- MAC basierte Portsecurity Modi {RADIUS allow...}
- User basierte Portsecurity Modi {IEEE802.1X ...}

Die Funktionsweise der einzelnen Modi wird in den nachfolgenden Kapiteln detailliert beschrieben.

WICHTIG:

Für die Authentifizierung von Name/Passwort (Telnet, SSHv2, V24, Manager) können separate RADIUS Einstellungen konfiguriert werden. Sofern der "RADIUS Management Authentication Mode" auf "Use Global Authentication Setup" eingestellt ist (dies ist die Werkseinstellung), werden allerdings für alle RADIUS Anfragen die globalen Einstellungen verwendet.

10.55.1. RADIUS Global Authentication-Einstellungen

Die folgende Tabelle zeigt eine Übersicht der RADIUS Global Authentication-Einstellungen:

Bez. im NEXMAN	Default Wert	Funktion
Server 1 Address		Es können vier RADIUS Server IP-Adressen angegeben, wobei die erste IP-Adresse immer den primären RADIUS Server angibt. Abhängig vom eingestellten Algorithmus für Server-Anfragen sind die anderen IP-Adressen für die Backup RADIUS Server reserviert, oder sie werden abwechselnd oder parallel abgefragt (siehe Feld 'Server request algorithm' unten). Per NEXMAN (Reiter 'Radius State' und 'MAC+Security State') und per Console Kommando 'sh:ow ra:dus' kann der Status der RADIUS Server kontrolliert werden.
Server 2 Address		
Server 3 Address		
Server 4 Address		
Authentication UDP Port	1812	Die UDP Port-Nummer, auf der der RADIUS Servers Authentication Requests empfängt. Die offizielle Nummer ist 1812, nach einer älteren Spezifikation ist aber auch 1645 möglich.
Shared secret	<leer>	Das sogenannte 'Shared Secret' dient als Passwort gegenüber dem RADIUS Server. Dieses muss im Switch und im RADIUS Server identisch eingetragen werden.
Request timeout	5	Die maximale Zeit in Sekunden, die der Switch nach einem Radius-Request auf die Antwort des RADIUS Servers wartet.
Request retries	2	Gibt an, wie oft der Switch einen Radius-Request wiederholt, bevor der Request als fehlgeschlagen angesehen wird. Der entsprechende RADIUS Server wird in der Statusanzeige als 'down' gekennzeichnet.
Portsecurity password	<leer>	Dieses Passwort wird ausschließlich für die MAC-basierten Authentifizierung verwendet und wird im Radius-Attribut 'User-Password' übermittelt. Wird dieses Feld leer gelassen, so wird stattdessen die MAC Adresse des zu authentifizierenden Endgerätes verwendet. Das Format ist dabei identisch zum Attribut 'User-Name', jedoch wird das 'User-Password' als verschlüsselter Wert übermittelt. Für weitere Informationen siehe Kapitel 10.59.1. Portsecurity Modi {RADIUS allow ...} .
Portsecurity realm	<leer>	Dieser Realm-String wird nur für die MAC-basierten Authentifizierung verwendet. Die MAC Adresse im Radius-Attribut 'User-Name', wird dabei um diesen Portsecurity-Realm-String ergänzt. Wird in der Konfiguration ein leerer String angegeben, so wird kein Portsecurity-Realm eingefügt und die Einstellungen unter 'Realm location' und 'Realm separator' werden ignoriert. Für weitere Informationen siehe Kapitel 10.59.1. Portsecurity Modi {RADIUS allow ...} bzw. 10.59.2. Portsecurity Modus {IEEE802.1X allow one MAC-Address} .
Management realm	<leer>	Dieser Realm-String gilt nur für Telnet/SSH/V.24-Console und NEXMAN Radius-Requests. Der Login Name im Radius-Attribut 'User-Name' wird dabei um diesen Management-Realm-String ergänzt. Wird in der Konfiguration ein leerer String angegeben, so wird kein Management-Realm eingefügt und die Einstellungen unter 'Realm location' und 'Realm separator' werden ignoriert. Für weitere Informationen siehe Kapitel 10.56. RADIUS

		<u>Console Authentication Modes</u> bzw. <u>10.57. RADIUS Manager Authentication Modes</u> .
Realm location	Suffix	Gibt an, ob der Realm-String vor (prefix) oder hinter (suffix) dem eigentlichen 'User-Namen' angefügt wird.
Realm separator	<leer>	Bestimmt das Trennzeichen, das zwischen dem eigentlichen 'User-Namen' und den Realm-String eingefügt wird. Wird in der Konfiguration ein leerer String angegeben, so wird kein Realm-Separator eingefügt.
MAC address separator	<leer>	Bei den MAC-basierten Portsecurity Radius-Requests wird im Attribut User-Name und ggf. im Attribut User-Password die MAC-Adresse eingetragen. Die einzelnen Bytes dieser MAC-Adresse können dabei durch diesen Separator-String voneinander getrennt werden. Wird in der Konfiguration ein leerer String angegeben, so wird kein MAC-Separator eingefügt.
Startup VLAN-ID	Unsecure-VLAN (Allow RX traffic to VLAN for unauthorized MACs)	Diese Einstellung gilt ausschließlich für Ports, bei denen eine RADIUS-basierte (IEEE802.1X oder MAC based) Authentifizierung aktiviert ist. Folgende Einstellungen sind möglich: • 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) Bestimmt, welche VLAN-ID nach einem Link-Up oder Portsecurity-Renew-Befehl als Port-Default-VLAN-ID aktiviert wird: Unsecure VLAN-ID: Bei dieser Einstellung wird das global konfigurierte Unsecure VLAN aktiviert. Port Default VLAN-ID: Hier wird die pro Port konfigurierte Port Default VLAN-ID verwendet. Ist für den Port die Port Default VLAN-ID auf 0 eingestellt ist, so wird für diesen Port stattdessen die Unsecure VLAN-ID verwendet. Ferner kann bestimmt werden, ob RX Daten vom Endgerät an das aktivierte VLAN durchgeleitet oder geblockt werden: Allow RX traffic to VLAN for unauthorized MACs: Bei dieser Einstellung werden ungetaggte RX Pakete ungefiltert an das betreffende VLAN weitergeleitet. Dagegen werden getaggte RX Pakete im eingestellten Voice-VLAN nach einer kurzen Verzögerung geblockt, d.h., dass für einige Sekunden RX Pakete in das Voice VLAN durchgeleitet werden. Diese Blockierung wird wieder aufgehoben sobald das betreffende Endgerät per RADIUS authentifiziert wurden. Block RX traffic to VLAN for unauthorized MACs: Hier werden sofort RX Pakete vom Endgerät geblockt. Diese RX Blockierung bleibt bestehen, bis das Endgerät per RADIUS authentifiziert wurde (über IEEE802.1X oder über MAC-basierte Authentifizierung) oder bis das Endgerät in das 'Guest VLAN', 'Inaccessible VLAN' or 'IEEE802.1x Authentication Failure VLAN' verschoben wurde. Außerdem werden getaggte RX Pakete im eingestellten Voice-VLAN sofort geblockt, d.h., dass keine Pakete ins Voice VLAN weitergeleitet werden bis das betreffende Endgerät per RADIUS authentifiziert wurden. Achtung: Bei dieser Einstellung ist die „Portsecurity ageing time for PC behind IP-Phone“ ohne Funktion. WICHTIG: Trotz Blockierung der RX Daten, werden Broad- und Multicast Pakete im Default und Voice VLAN an die Endgeräte weitergeleitet. Dies ermöglicht z.B. Wake-On-LAN während das Endgerät ausgeschaltet oder noch nicht authentifiziert ist.
VLAN Attribute	IETF Tunnel-Private-Group-ID with VLAN-ID	Legt fest, welches RADIUS-Attribut in einem Access-Accept für die Konfiguration der Port Default-VLAN_ID und der Voice-VLAN-ID ausgewertet wird. Folgende Einstellungen sind möglich: • 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

		WICHTIG: Es wird nur das eingestellte Attribut akzeptiert. Fehlt dieses Attribut im Access-Accept, so wird der Port auf die Default-VLAN-ID des betreffenden Ports eingestellt. Wird zwar das korrekte Attribut empfangen, aber die VLAN-ID ist außerhalb des zulässigen Bereichs von 1 ... 4095, so wird der Access-Accept verworfen und der Port bleibt im RADIUS-Unsecure-VLAN. Nexans Vendor Specific VLAN-ID: Hier wird das sogenannte Nexans Enterprise Attribut 'Nexans-Port-Default-VLAN-ID' und 'Nexans-Port-Voice-VLAN-ID' ausgewertet, welche im Radius-Dictionary wie folgt deklariert werden müssen: <pre> VENDOR Nexans 266 ietf ATTRIBUTE Nexans-Port-Default-VLAN-ID 1 integer Nexans ATTRIBUTE Nexans-Port-Voice-VLAN-ID 2 integer Nexans </pre> Der Wert des Attributes muss die VLAN-ID beinhalten und muss im Bereich 1...4095 liegen. Die übermittelte VLAN-ID wird automatisch der VLAN-Table hinzugefügt. Es wird empfohlen den 'VLAN Table Mode' auf {dynamic} einzustellen, um ein Überlaufen der Table zu verhindern. Ist der 'VLAN Table Mode' auf {static} eingestellt und sollte dann die VLAN-Table voll sein, so wird die übermittelte VLAN-ID ignoriert und stattdessen die im Switch gespeicherte Default-VLAN-ID des betreffenden Ports verwendet. IETF Tunnel-Private-Group-ID with VLAN-ID: Hier wird das IETF Standard Attribut 'Tunnel-Private-Group-ID' erwartet (siehe RFC2868). Der Wert des Attributes muss die VLAN-ID beinhalten und muss im Bereich 1...4095 liegen. Die übermittelte VLAN-ID wird automatisch der VLAN-Table hinzugefügt. Es wird empfohlen den 'VLAN Table Mode' auf {dynamic} einzustellen, um ein Überlaufen der Table zu verhindern. Ist der 'VLAN Table Mode' auf {static} eingestellt und sollte dann die VLAN-Table voll sein, so wird die übermittelte VLAN-ID ignoriert und stattdessen die im Switch gespeicherte Default-VLAN-ID des betreffenden Ports verwendet. Wird lediglich ein Zahlenwert vom RADIUS Server übermittelt, so wird dieser als Default-VLAN-ID eingestellt. Möchte man dagegen das Voice-VLAN zuweisen, so muss dem Zahlenwert der Text 'v:' oder 'V:' vorangestellt werden. Beispiel: 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 Wird zusätzlich zur Tunnel-Private-Group-ID das Cisco Attribut "device-traffic-class=voice" empfangen, so wird die VLAN-ID grundsätzlich als Voice-VLAN interpretiert (siehe auch Parameter „Cisco device-traffic-class mode“). IETF Tunnel-Private-Group-ID with VLAN-Description: Hier wird ebenfalls das IETF Standard Attribut 'Tunnel-Private-Group-ID' erwartet (siehe RFC2868). Der Wert des Attributes muss allerdings die VLAN-Description laut VLAN-Table beinhalten. Wird die übermittelte VLAN-Description nicht in der VLAN-Table gefunden, so wird der Access-Accept verworfen und der Port bleibt im RADIUS-Unsecure-VLAN. Hierbei muss der 'VLAN Table Mode' auf {static} eingestellt werden, um ein Löschen unbenutzter VLAN-ID's zu verhindern. HINWEIS: Möchte man das Voice-VLAN zuweisen, so muss der VLAN Description der Text 'v:' oder 'V:' vorangestellt werden. Wird zusätzlich zur Tunnel-Private-Group-ID das Cisco Attribut "device-traffic-class=voice" empfangen, so wird die VLAN-ID grundsätzlich als Voice-VLAN interpretiert (siehe auch Parameter „Cisco device-traffic-class mode“). Ignore VLAN attributes: Hier werden alle VLAN-Attribute des RADIUS Servers ignoriert und der Port
--	--	--

		nach einen Access-Accept auf die Default-VLAN-ID des betreffenden Ports eingestellt.
Cisco device-traffic-class mode		Legt fest, wie das CISCO proprietäre RADIUS-Attribut „device-traffic-class=voice“ in einem Access-Accept für die Konfiguration der Port Voice-VLAN-ID ausgewertet wird. Folgende Einstellungen sind möglich: • 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: Dies ist die Standardeinstellung und sollte immer dann verwendet falls: • das Attribut ‚device-traffic-class=voice‘ im RADIUS Access-Accept grundsätzlich nicht zum Einsatz kommt. • auf den Switchports keine Voice-VLAN-IDs konfiguriert sind und die Voice-VLAN-IDs vom RADIUS Server via Attribut ‚Tunnel-Private-Group-ID‘ und ‚device-traffic-class=voice‘ vergeben werden. Hier wird bei einem RADIUS Access-Accept überprüft, ob zusätzlich zur übermittelten VLAN-ID im Attribut ‚Tunnel-Private-Group-ID‘, das Attribut ‚device-traffic-class=voice‘ enthalten ist. Falls dies zutrifft, so wird diese VLAN-ID als Voice-VLAN-ID für den betreffenden Port übernommen. Use device-traffic-class=voice to allow access to Voice-VLAN: Diese Einstellung sollte verwendet werden falls die Voice-VLAN-IDs auf den Switchports fest konfiguriert sind und der RADIUS Server diese lediglich aktivieren soll. Hierbei werden die pro Port eingestellten Voice-VLAN-IDs zunächst deaktiviert und das Voice-VLAN abgeschaltet. Bei einem RADIUS Access-Accept wird nun überprüft, ob das Attribut ‚device-traffic-class=voice‘ enthalten ist. Falls dies zutrifft, so wird die konfigurierte Voice-VLAN-ID auf dem betreffenden Port aktiviert. HINWEIS: Sollte der RADIUS Access-Accept zusätzlich eine VLAN-ID im Attribut ‚Tunnel-Private-Group-ID‘ enthalten, so wird diese VLAN-ID vorzugsweise als Voice-VLAN-ID für den betreffenden Port übernommen.
Server request algorithm	Strict-Priority	Hier kann konfiguriert werden, mit welchem Algorithmus die Radius Server abgefragt werden: Strict-Priority: Die Radius Server werden strikt in Reihenfolge unabhängig vom Status abgefragt. Es wird immer von dem als erstes eingetragenen Radius Server angefangen. Round-Robin: Im Gegensatz zur Strict-Priority wird beim Round-Robin die Reihenfolge der eingetragenen Radius Server fortgesetzt. Ist beispielsweise eine Authentifizierung bei Server 1 erfolgt, wird die nächste Anfrage bei Server 2 gestartet. Nach abarbeiten des letzten Servers in der Liste beginnt die Anfrage erneut beim ersten. Durch diesen Algorithmus wird die Verbindung und Verwendung aller eingetragenen Radius-Server gewährleistet. Parallel: Alle eingetragenen Radius-Server werden bei einer Anfrage parallel abgefragt. Die erste Antwort, die vom Server zurückkommt, wird vom Switch akzeptiert.

10.55.2. RADIUS Management Authentication-Einstellungen

Die folgende Tabelle zeigt eine Übersicht der RADIUS Management Authentication-Einstellungen:

Bez. im NEXMAN	Default Wert	Funktion
Management Authentication Mode	Use Global Setup	Gibt an, ob die globalen RADIUS Authentication Einstellungen oder der folgende separate Parametersatz für die Authentifizierung von Name und Passwort (Telnet, SSHv2, V24, Manager) verwendet werden sollen.
Server 1 Address		

Server 2 Address		Funktionsweise identisch zu den entsprechenden Einstellungen bei den globalen RADIUS Parametern.
Server 3 Address		
Server 4 Address		
Authentication UDP Port	1812	
Shared secret	<leer>	
Request timeout	5	
Request retries	2	

10.56. RADIUS Console Authentication Modes

Für die Telnet-, SSHv2- und V.24-Console können jeweils vier verschiedene Authentifizierungs-Modi eingestellt werden:

- Local: Lokale Authentifizierung
- Disabled: Telnet Interface disabled
- Radius only: Authentifizierung ausschließlich durch den RADIUS Server
- Radius first, then local: Authentifizierung durch RADIUS, nur falls kein Server antwortet: lokale Authentifizierung
- TACACS+ only: Authentifizierung ausschließlich durch den TACACS+ Server
- TACACS+ first, then local: Authentifizierung durch TACACS+, nur falls kein Server antwortet: lokale Authentifizierung

Local (Factory-Default):

Disabled:

Siehe Kapitel [10.14. V.24 Console Authentication Mode](#), [10.48 Telnet Console Authentication Mode](#) bzw. [10.49. SSHv2 Console Authentication Mode](#)

TACACS+ Only:

TACACS+ first, then local:

Siehe Kapitel [10.64 TACACS+ Console Authentication Modes](#)

Radius only:

Statt die lokal gespeicherten Authentifizierungsdaten zu verwenden, wird die Authentifizierung durch einen zentralen RADIUS Server durchgeführt.

Radius first, then local:

In diesem Modus wird zunächst eine Authentifizierung über RADIUS Server versucht. Nur wenn keiner der eingestellten RADIUS Server abhängig vom gesetzten Server-Anfragealgorithmus antwortet, wird der eingegebene Login-Name und das Passwort mit den lokal gespeicherten Daten verglichen.

Die RADIUS Authentifizierung läuft wie folgt ab:

- Der User gibt beim Console Login seinen Namen und Passwort ein
- Der Switch sendet Name und Passwort per Radius Access-Request an den RADIUS Server
- Der RADIUS Server überprüft, ob der User in der Datenbank bekannt ist und die notwendigen Rechte besitzt und antwortet mit Access-Accept oder Access-Reject.
- Wird ein Access-Accept empfangen, so werden die Rechte gemäß dem enthaltenen Attribut 'Service-Typ' gewährt. Wird ein Access-Accept ohne dieses Attribut oder mit einem unzulässigen Service-Typ empfangen, so wird bei V.24- oder Telnet-Consolen die Fehlermeldung 'Wrong authentication' am Console-Prompt ausgegeben und ein 'Radius-Mgmt-Auth-Reject' Event versendet.
- Wird ein Access-Reject empfangen, so wird bei V.24- oder Telnet-Consolen ebenfalls die Fehlermeldung 'Wrong authentication' am Console-Prompt ausgegeben und ein 'Radius-Mgmt-Auth-Reject' Event versendet.
- Antwortet kein RADIUS Server (Timeout), so wird bei V.24- oder Telnet-Consolen die Fehlermeldung 'No response from RADIUS Server' am Console-Prompt ausgegeben. Außerdem wird ein Alarm in der Device List des Managers angezeigt.

10.56.1. RADIUS Attribute zur Consolen-Authentifizierung

Folgende RADIUS Attribute werden vom Switch an den RADIUS Server gesendet:

Attribut	Attribut enthält ...
NAS-IP-Address	IP-Adresse des Nexans Switches
NAS-Identifizier	Switch Name
NAS-Port	0
NAS-Port-Type	Virtual (5)
Calling-Station-ID	IP-Adresse der Station, die den Zugriff per Telnet ausführt HINWEIS: Bei Zugriff per V.24 Console ist dieser Wert 0.0.0.0
Service-Type	Administrative (6)
User-Name	Vom Benutzer eingegebener Login Name Das Attribut kann optional um einen festen Realm-String ergänzt werden. Dieser Management-Realm wird dann vor (prefix) oder hinter (suffix) den eigentlichen Login Namen angefügt und durch einen Realm-Separator getrennt. Beispiel: Console Login Name: MeierF Management-Realm: nexans-port Realm-Separator: @ Realm-Position: suffix → User-Name: MeierF@nexans-port
User-Password	Vom Benutzer eingegebenes Login Passwort. HINWEIS: Das Passwort wird vor der Übertragung gemäß PAP Verfahren nach RFC 2865 Kapitel 5.2 verschlüsselt und ist somit nicht im Klartext via Wireshark mitlesbar.

Folgende Radius Attribute werden vom Switch ausgewertet:

Attribut	Attribut enthält ...
Service-Type	Im Access-Accept muss dieses Attribut enthalten sein. Es teilt dem Switch mit, ob der Benutzer als Admin Account (R/W) oder als User Account (R/O) angemeldet werden soll. Dabei sind folgende Werte für den Service-Typ zulässig: • Service-Typ = Login (1) → User-Mode (R/O) • Service-Typ = Administrative (6) → Admin-Mode (R/W)

10.57. RADIUS Manager Authentication Modes

Für den NEXMAN Zugriff können im Switch sieben Authentifizierungs-Modi eingestellt werden:

- SCP – Use SCP authentication mode setting: Authentifizierung via SCP
- UDP/TFTP – No authentication (Ignores Username and Password) Keine Authentifizierung
- UDP/TFTP – Local Accounts Lokale Authentifizierung
- UDP/TFTP – Radius Only Authentifizierung ausschließlich durch den RADIUS Server
- UDP/TFTP – Radius first, then Local Accounts Authentifizierung durch RADIUS, nur falls kein Server antwortet: lokale Authentifizierung
- SNMPv3 – Local Accounts Lokale Authentifizierung
- Disable Manager access Manager Zugriff per UDP, TFTP und SNMPv3 abgeschaltet

SCP – Use SCP authentication mode setting (Factory-Default)

UDP/TFTP – No authentication (Ignores Username and Password)

SNMPv3 – Local Accounts

Disable Manager access:

Siehe Kapitel [10.10. Manager Authentication Mode](#)

UDP/TFTP – Radius Only

UDP/TFTP – Radius first, then Local Accounts:

Der Ablauf der Authentifizierung ist prinzipiell identisch zur Consolen-Authentifizierung per RADIUS Server (siehe Kapitel [10.56. RADIUS Console Authentication Modes](#)).

10.58. RADIUS SCP Authentication Modes

Für SCP können im Switch sieben verschiedene Authentifizierungs-Modi eingestellt werden:

- Local: Lokale Authentifizierung
- Radius only: Authentifizierung ausschließlich durch den RADIUS Server
- Radius first, then local: Authentifizierung durch RADIUS, nur falls kein Server antwortet: lokale Authentifizierung
- TACACS+ only: Authentifizierung ausschließlich durch den TACACS+ Server
- TACACS+ first, then local: Authentifizierung durch TACACS+, nur falls kein Server antwortet: lokale Authentifizierung
- Use SSHv2 mode Es wird der SSHv2 authentication mode benutzt
- Disabled: SCP Interface deaktiviert

Use SSHv2 mode (Factory-Default):

Local:

Disabled:

Siehe Kapitel [10.50 SCP Authentication Mode](#)

TACACS+ Only:

TACACS+ first, then local:

Siehe Kapitel [10.66 TACACS+ SCP Authentication Modes](#)

Radius only:

Radius first, then local:

Der Ablauf der Authentifizierung ist prinzipiell identisch zur Consolen-Authentifizierung per RADIUS Server (siehe Kapitel [10.56. RADIUS Console Authentication Modes](#)).

10.59. Portsecurity mit Authentifizierung per RADIUS Server

Folgende Portsecuritymodi, mit Authentifizierung über einen RADIUS Server, werden unterstützt:

- 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

Die folgenden Modi (**ohne** Authentifizierung über einen RADIUS Server) werden ebenfalls unterstützt (Beschreibung siehe Kapitel [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 Modi {RADIUS allow ...}

Die Einstellungen {RADIUS allow one MAC-Address}, {RADIUS allow two MAC-Addresses} bzw. {RADIUS allow three MAC-Addresses} ermöglichen, dass der Switch eine, zwei bzw. drei MAC-Adressen automatisch lernt und diese zusätzlich von einem RADIUS Server authentifizieren lässt. Hierbei können maximal zwei

VLANs zugewiesen werden, nämlich ein "ungetaggttes" Default-VLAN (z.B. für einen PC oder Drucker) und zusätzlich ein "getaggttes" Voice-VLAN (z.B. für ein IP-Phone).

Solange keine positive Antwort von RADIUS Server empfangen wurde, bleibt der Port im sogenannten 'RADIUS-Unsecure-VLAN' (siehe Kapitel 10.31.15. RADIUS Unsecure VLAN-ID). Erst nach Erhalt eines Access-Accept wird der Port auf die Default- bzw. Voice-VLAN-ID gemäß dem empfangenen VLAN-Attribut geschaltet (siehe 'VLAN Attribut' im Kapitel 10.55. RADIUS Authentication). Wird für eine zweite oder dritte MAC Adresse ein weiterer Access-Accept empfangen, welcher ebenfalls eine Default- bzw. Voice-VLAN-ID enthält, so wird die aktuell eingestellte Default- bzw. Voice-VLAN-ID ggf. überschrieben. Dies heißt, dass der zuletzt empfangene Access-Accept die Default- bzw. Voice-VLAN-ID des Ports bestimmt.

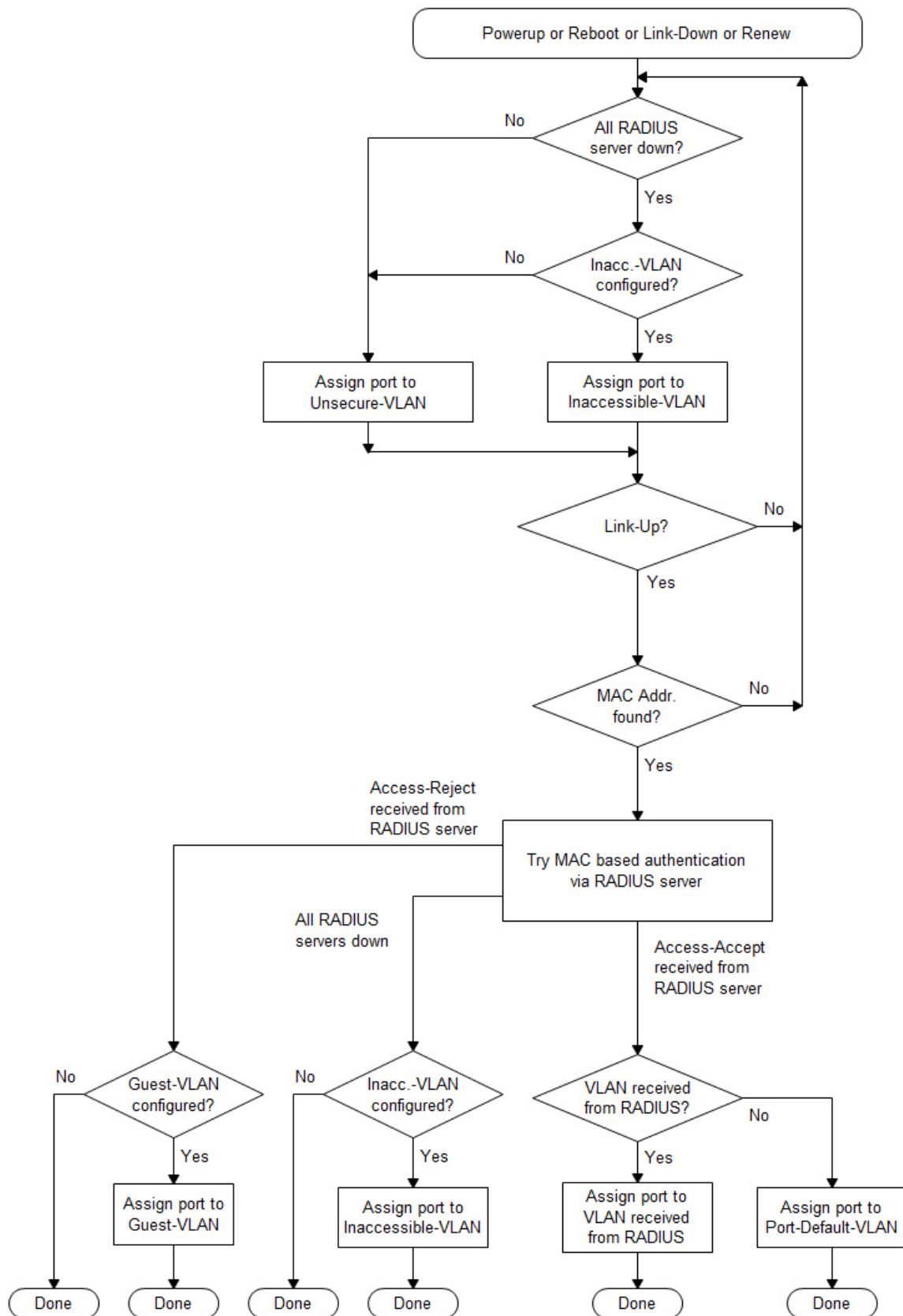
Wird eine negative Antwort vom RADIUS Server empfangen, so wird außerdem ein 'Radius Portsecurity Reject' Event versendet und ein Alarm in der Device List des Managers angezeigt.

Falls kein RADIUS Server antwortet (Timeout), wird ebenfalls ein Alarm in der Device List des Managers angezeigt.

Erkennt der Switch mehr als die zugelassenen ein, zwei bzw. drei MAC Adressen, so wird der Port ggf. abgeschaltet (siehe Kapitel 10.36.1. Portsecurity - Failure Action). Dies verhindert z.B., dass der Benutzer hinter einem TP-Port einen weiteren Switch anschließt. Außerdem wird ein 'Portsecurity-Failure' Event versendet, der die unzulässige MAC Adresse beinhaltet. Die gelernten MAC-Adressen werden automatisch wieder gelöscht, wenn der Link des betreffenden Ports auf Down geht (z. B. wenn ein anderer PC aufgesteckt wird) oder wenn der Port abgeschaltet wurde. Ferner wird unmittelbar nachdem eine neue MAC-Adresse gelernt wurde ein 'New-MAC-Address' Event versendet.

Möchte man die Portsecurity Funktion eines bestimmten Ports Re-Initialisieren oder einen automatisch abgeschalteten Port wieder aktivieren, so kann dies auf einfache Weise über den 'Renew-Befehl' erfolgen (siehe Kapitel 10.36.5. Portsecurity – Renew-Befehl).

Das nachfolgende Ablaufdiagramm zeigt den grundsätzlichen Ablauf der MAC based RADIUS Authentifizierung und die entsprechende Zuweisung der VLAN's:



Folgende Radius Attribute werden vom Switch and den RADIUS Server gesendet:

Attribut	Attribut enthält ...
NAS-IP-Address	IP-Adresse des Nexans Switches
NAS-Identifizier	Switch Name
NAS-Port	Nummer des Ports auf dem die neue MAC-Adresse empfangen wurde.
NAS-Port-ID	Bezeichnung des Ports auf dem die neue MAC-Adresse empfangen wurde.
NAS-Port-Type	Ethernet(15)
Calling-Station-ID	Die Calling-Station-ID besteht aus einem Textstring, der die zu authentifizierende MAC-Adresse enthält. Das Format ist in RFC3580 definiert und lautet wie folgt: XX-XX-XX-XX-XX-XX Beispiel: MAC-Adresse: 00c02900000f → Calling-Station-ID: 00-C0-29-00-00-0F
Service-Type	Call Check(10)
User-Name	Der User-Name besteht aus einem Textstring, der die zu authentifizierende MAC-Adresse enthält. Das Format ist wie folgt: xx<sep>xx<sep>xx<sep>xx<sep>xx<sep>xx Dabei sind xx die einzelnen Bytes der MAC-Adresse und <sep> ein frei wählbarer MAC-Separator. Der User-Name kann optional um einen festen Realm-String ergänzt werden. Dieser Portsecurity-REALM wird dann vor (prefix) oder hinter (suffix) die eigentliche MAC-Adresse angefügt und durch einen Realm-Separator getrennt. Beispiel: MAC-Adresse: 00c02900000f MAC-Separator : : Portsecurity-REALM: nexans-port Realm-Separator: @ Realm-Position: suffix → User-Name: 00:c0:29:00:00:0f@nexans-port
User-Password	Defaultwert = MAC-Adresse Im Prinzip ist beim Portsecurity-Request kein User-Passwort notwendig, jedoch wird ein leeres Passwort nicht von allen RADIUS Servern akzeptiert. Der Switch setzt deshalb die MAC-Adresse (identisch zum Attribut User-Name) oder ein festes Passwort ein, dass vom Benutzer frei konfiguriert werden kann (siehe Einstellung 'Portsecurity-Password' im Kapitel <u>10.55. RADIUS Authentication</u>). HINWEIS: Das Passwort wird vor der Übertragung gemäß PAP Verfahren nach RFC 2865 Kapitel 5.2 verschlüsselt.
Tunnel-Private-Group-ID	Dieses Attribut dient ausschließlich zu Diagnose-Zwecken und muss vom RADIUS ignoriert werden. Es beinhaltet die VLAN-ID der MAC Adresse des zu authentifizierenden Endgerätes, den Authentifizierungsstatus des Endgerätes und die aktuellen Port Default- und Voice VLAN-IDs des Switchports.

Folgende Radius Attribute werden vom Switch ausgewertet:

Attribut	Attribut enthält ...
Tunnel-Private-Group-ID Nexans-Port-Default-VLAN-ID Nexans-Port-Voice-VLAN-ID device-traffic-class	Diese Attribute werden nur in einem Access-Accept ausgewertet und bestimmen, auf welche VLAN-ID der betreffende Port eingestellt werden soll. Detaillierte Informationen siehe Konfigurationseinstellung 'VLAN Attribut' im Kapitel 10.55. RADIUS Authentication .

10.59.2. Portsecurity Modus {IEEE802.1X allow one MAC-Address}

Diese Einstellung erzwingt eine Authentifizierung nach IEEE802.1X und setzt voraus, dass das angeschlossene Endgerät und der RADIUS Server ebenfalls IEEE802.1X unterstützen. Ferner wird vom Switch überprüft, ob nur eine einzige MAC-Adressen auf dem betreffenden Port empfangen wird. Erkennt der Switch mehr als eine MAC Adresse, so wird der Port ggf. abgeschaltet (siehe Kapitel [10.36.1. Portsecurity - Failure Action](#)). Dies verhindert z.B., dass der Benutzer hinter einem authentifizierten TP-Port ein weiteres Endgerät anschließt. Außerdem wird ein 'Portsecurity-Failure' Event versendet, der die unzulässige MAC Adresse beinhaltet. Die gelernte MAC-Adresse wird automatisch wieder gelöscht, wenn der Link des betreffenden Ports ausfällt (z. B. wenn ein anderer PC aufgesteckt wird) oder wenn der Port manuell abgeschaltet wurde. Ferner wird unmittelbar nachdem eine neue MAC-Adresse gelernt wurde ein 'New-MAC-Address' Event versendet.

Solange keine positive Antwort von RADIUS Server empfangen wurde, bleibt der Port im sogenannten 'RADIUS-Unsecure-VLAN' (siehe Kapitel [10.31.15. RADIUS Unsecure VLAN-ID](#)). Erst nach Erhalt eines Access-Accept wird der Port auf die VLAN-ID gemäß dem empfangenen VLAN-Attribut eingestellt (siehe 'VLAN Attribut' im Kapitel [10.55. RADIUS Authentication](#)).

Wird eine negative Quittung vom RADIUS Server empfangen (Access-Reject), so wird der Port nach einer maximalen Anzahl von Authentication Retries in das sogenannte 'Authentication Failure VLAN' verschoben. Dies ermöglicht, dass 802.1X Clients, die ein oder mehrmals das falsche Passwort eingeben, in ein spezielles VLAN geschaltet werden. Möchte man dieses zusätzliche VLAN nicht nutzen, so muss die 'Authentication Failure VLAN-ID' auf 0 eingestellt werden. In diesem Fall wird ausschließlich das 'Unsecure VLAN' verwendet. Nach der letzten negativen Quittung wird ein Alarm in der Device List des Managers angezeigt.

Falls kein RADIUS Server antwortet (Timeout), wird ebenfalls ein Alarm in der Device List des Managers angezeigt.

Möchte man die Portsecurity Funktion eines bestimmten Ports Re-Initialisieren oder einen automatisch abgeschalteten Port wieder aktivieren, so kann dies auf einfache Weise über den 'Renew-Befehl' erfolgen (siehe Kapitel [10.36.5. Portsecurity – Renew-Befehl](#)).

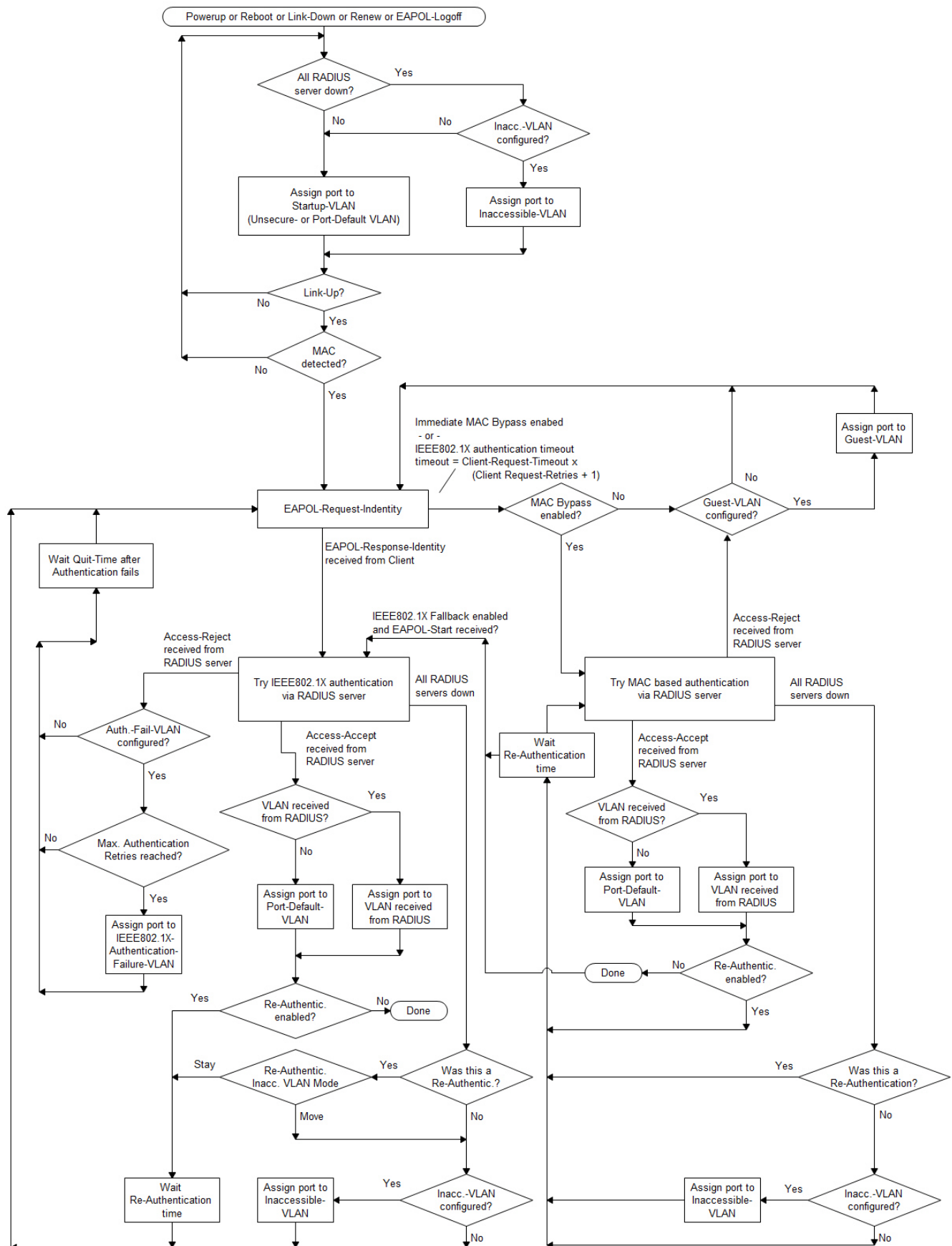
Die folgende Tabelle zeigt eine Übersicht aller IEEE802.1X Einstellungen:

Bezeichnung im NEXMAN	Default Wert	Funktion
IEEE 802.1X Global Setup		
IEEE 802.1X transparency enable	Disabled	Siehe Kapitel 10.35. IEEE802.1X Transparenz
IEEE 802.1X Authenticator Setup		
Re-Authentication enable	Disabled	Wenn eingeschaltet, wird eine periodische Re-Authentifizierung des Endgerätes erzwungen

Re-Authentication initial delay	0	Greift nur falls die Re-Authentifizierung Global enabled ist: Definiert die Zeit bis zur ersten Re-Authentifizierung in Sekunden. Nach dieser ersten Re-Authentifizierung wird das 'Re-Authentication interval' für alle für weiteren Re-Authentifizierungen verwendet. Falls der Wert mit 0 konfiguriert ist, wird für die erste Re-Authentifizierung ebenfalls das 'Re-Authentication interval' angewendet. Dies ist insbesondere hilfreich, falls kurze Zeit nach der initialen Authentifizierung eine erneute Authentifizierung stattfinden soll. Dies z.B. dann der Fall, wenn nach der initialen Authentifizierung eine Prüfung der Endgeräteparameter stattfindet (aktueller Virusscanner installiert? etc.) und dann erneut festgelegt wird, ob das Endgerät im initial zugewiesenen VLAN bleiben darf oder in ein spezielles VLAN verschoben werden soll. Dies kann als ein Bestandteil der CoA (Change of Authorisation) Strategie Anwendung finden.
Re-Authentication interval	3600	Greift nur falls die Re-Authentifizierung Global enabled ist: Bestimmt das Zeitintervall in Sekunden für die periodische Re-Authentifizierung
Re-Authentication Inaccessible VLAN Mode	Stay	Greift nur falls die Re-Authentifizierung Global enabled und ein Inaccessible VLAN konfiguriert ist: Bestimmt das Verhalten des Port VLANs falls bei einer IEEE802.1X Re-Authentifizierung alle RADIUS nicht erreichbar sind. Folgende Einstellung sind verfügbar: • Stay: Der Port verbleibt im aktuell aktivierten Port VLAN • Move: Der Port wird in das "Inaccessible VLAN" verschoben und die IEEE802.1X Authentifizierung des Ports neu angestoßen. Der detaillierte Ablauf der Authentifizierung kann dem Ablaufdiagramm unten entnommen werden.
Quiet-Time after Auth. fails	30	Ruhezeit in Sekunden nach einer abgelehnten Authentifizierung durch den RADIUS Server. Während dieser Zeit ist keine erneute Authentifizierung möglich.
Client request timeout	30	Zeit in Sekunden, die der Switch nach einem EAP-Request an das Endgerät auf dessen Antwort wartet.
Client request retries	2	Anzahl der Wiederholungen eines EAP-Requests bevor die Authentifizierung abgebrochen und neu gestartet wird.
Max. Authentication Retries	0	Die maximale Anzahl von fehlerhaften Authentifizierungsversuchen durch den Client. Wird diese Anzahl überschritten, so wird der betreffende Port in das 'Authentication Failure VLAN' geschaltet. Eine Einstellung von 0 bedeutet z.B., dass nach der ersten Eingabe eines falschen Passwortes durch den User, der Port in das 'Authentication Failure VLAN' verschoben wird. Eine Einstellung von 2 heißt z.B., dass der User nach dreimaliger Eingabe eines falschen Passwortes in das 'Authentication Failure VLAN' verschoben wird.
RADIUS MAC Bypass enable	Disabled	Siehe Kapitel <u>10.59.6. Portsecurity Option {IEEE802.1X Radius MAC Bypass}</u>

MAC bypass Quiet Time	0	Nach dem Empfang eines „Radius Reject“ wird ein erneuter Authentifizierungsversuch per MAC Bypass frühestens nach Ablauf der „MAC bypass Quiet Time“ durchgeführt. Der genaue Zeitpunkt richtet sich nach dem konfigurierten „Client request timeout“ und den „Client request retries“. Ist die „MAC bypass Quiet Time“ auf „0“ eingestellt, so wird nach jedem 802.1x Timeout eine MAC Bypass Authentifizierung angestoßen.
IEEE 802.1X Supplicant Setup		
MD5 Name	<none>	Der Name, der bei der IEEE802.1X Authentifizierung zum Authenticator übermittelt wird. Siehe Kapitel <u>10.59.9. Portsecurity Modus {IEEE802.1X Supplicant mit MD5}</u> .
M5 Password	<none>	Das Passwort, das bei der IEEE802.1X Authentifizierung zum Authenticator übermittelt wird. Siehe Kapitel <u>10.59.9. Portsecurity Modus {IEEE802.1X Supplicant mit MD5}</u> .

Das nachfolgende Ablaufdiagramm zeigt den grundsätzlichen Ablauf der IEEE802.1X Authentifizierung und die entsprechende Zuweisung der VLAN's:



Folgende Radius Attribute werden vom Switch an den RADIUS Server gesendet:

Attribut	Attribut enthält ...
NAS-IP-Address	IP-Adresse des Nexans Switches
NAS-Identifizier	Switch Name
NAS-Port	Nummer des Switch-Ports für den die Authentifizierung durchgeführt wird
NAS-Port-ID	Bezeichnung des Switch-Ports für den die Authentifizierung durchgeführt wird
NAS-Port-Type	Ethernet(15)
Calling-Station-ID	Die Calling-Station-ID besteht aus einem Textstring, der die MAC-Adresse des Endgerätes enthält. Das Format ist in RFC3580 definiert und lautet wie folgt: XX-XX-XX-XX-XX-XX Beispiel: MAC-Adresse: 00c02900000f → Calling-Station-ID: 00-C0-29-00-00-0F
Service-Type	Framed(2)
Framed-MTU	Zulässige Framelänge (1300)
User-Name	Hier wird der Identity String aus dem EAP-Response/Identity Paket des Endgerätes eingesetzt. HINWEIS: Der User-Name wird grundsätzlich unverändert aus dem EAP Paket übernommen. Ein evtl. konfigurierter Portsecurity-Realm String, wie dies z.B. beim Modi {RADIUS allow ...} möglich ist, wird bei 802.1X ignoriert. Aufgrund der Limitierung im RADIUS Protokoll, ist die maximale Länge des User-Name auf 253 Zeichen begrenzt. Sollte im EAP Paket ein längerer Name enthalten sein, so wird dieser auf 253 Zeichen gekürzt bevor er in das RADIUS Attribut 'User-Name' eingesetzt wird. Das EAP Paket wird allerdings mit der kompl. Länge des User-Name in das RADIUS Attribut 'EAP-Message' eingesetzt und ggf. fragmentiert. Die maximale Länge des Usernamen im EAP Paket darf dabei 1400 Zeichen nicht überschreiten.
Chargeable-User-Identity	Dieses Attribut wird nur eingefügt, wenn beim Radius Accounting der Parameter 'User-Name for 802.1X' auf 'Chargeable-User-Identity' eingestellt ist. Für eine detaillierte Erläuterung der Funktionsweise siehe RFC4372.
EAP-Message	EAP-Message des Endgerätes
State	Dieses Attribut wird nur dann gesendet, wenn dieses vom RADIUS Server im vorausgehenden Access-Challenge oder Access-Accept mitgeliefert wurde. Der im Access-Challenge angegebene Inhalt des Attributes wird dabei unverändert im Access-Request eingesetzt. Im Falle eines Access-Accept muss zusätzlich zum Attribut 'State' das Attribut 'Termination-Action' mit dem Wert 'RADIUS-Request(1)' enthalten sein, damit das State Attribut bei der nächsten Re-Authentifizierung mitgeliefert wird.
Message-Authenticator	Signatur, MD5 Hash Wert
Tunnel-Private-Group-ID	Dieses Attribut dient nur zu DEBUG-Zwecken und muss vom RADIUS ignoriert werden. Es beinhaltet die aktuelle VLAN-ID des Endgerätes und die aktuellen Port VLAN-IDs. Ferner wird der Status der IEEE802.1X Authentifizierung angegeben übermittelt.

Folgende Radius Attribute werden vom Switch ausgewertet:

Attribut	Attribut enthält ...
----------	----------------------

Tunnel-Private-Group-ID Nexans-Port-Default-VLAN-ID Nexans-Port-Voice-VLAN-ID device-traffic-class	Diese Attribute werden nur in einem Access-Accept ausgewertet und bestimmen, auf welche VLAN-ID der betreffende Port eingestellt werden soll. Detaillierte Informationen siehe Konfigurationseinstellung 'VLAN Attribut' im Kapitel <u>10.55. RADIUS Authentication</u> .
State	Wird dieses Attribut in einem Access-Challenge mitgeliefert, so wird der angegebene Inhalt unverändert im nächsten Access-Request eingesetzt. Wird dieses Attribut in einem Access-Accept mitgeliefert, so muss zusätzlich das Attribut 'Termination-Action' mit dem Wert 'RADIUS-Request(1)' enthalten sein, damit das State Attribut bei der nächsten Re-Authentifizierung mitgeliefert wird.
User-Name	Dieses Attribut wird nur ausgewertet, wenn beim Radius Accounting der Parameter 'User-Name for 802.1X' auf 'User-Name' eingestellt ist. Für eine detaillierte Erläuterung der Funktionsweise siehe RFC4372.
Chargeable-User-Identity	Dieses Attribut wird nur ausgewertet, wenn beim Radius Accounting der Parameter 'User-Name for 802.1X' auf 'Chargeable-User-Identity' eingestellt ist. Für eine detaillierte Erläuterung der Funktionsweise siehe RFC4372.
Termination-Action	Dieses Attribut wird nur in einem Access-Accept ausgewertet. Falls vorhanden, muss es den Wert 'RADIUS-Request(1)' haben (siehe Attribute 'State').
Message-Authenticator	Signatur, MD5 Hash Wert

10.59.3. Portsecurity Modus {IEEE802.1X PC+Voice allow two MAC-Addresses}

In diesem Modus können zwei MAC Adressen in zwei verschiedenen VLANs per IEEE802.1X authentifiziert werden. Dabei sendet der Switch auf dem Default-VLAN ungetaggte und auf dem Voice-VLAN getaggte EAP-Pakete. Wie der Name schon aussagt, ist das Einsatzgebiet dieser Funktion speziell auf die Kombination aus IP-Phone und nachgeschaltetem PC zugeschnitten. In den meisten Voice-over-IP Installationen sendet und empfängt der PC ungetaggte Pakete, wogegen das IP-Phone getaggte Paket mit entsprechen 802.1Q Priorisierungsinformationen sendet und empfängt.

In Installationen bei denen Cisco IP-Phones zum Einsatz kommen, kann zusätzlich per CDP das Voice-VLAN an das IP-Phone übermittelt werden. Hier wird die am jeweiligen Port des Nexans Switches konfigurierte Voice-VLAN-ID herangezogen. Somit ist eine automatische Konfiguration des Cisco IP-Phones per CDP möglich. Weitere Informationen zur Konfiguration von Nexans Switches in einer Cisco Umgebung, können auf Anfrage bei Nexans angefordert werden (Stichwort 'Cisco Evaluierung').

10.59.4. Portsecurity Modus {IEEE802.1X Multi-User allow three MAC-Addresses}

Wird ein Port in diesen Securitymode geschaltet, so können auf diesem Port bis zu drei MAC-Adressen per IEEE802.1X gleichzeitig authentifiziert werden. Alle erkannten MAC Adressen werden dabei zunächst geblockt. Nur für MAC-Adressen, deren Supplicant per IEEE802.1X authentifiziert werden konnte, wird das blocking wieder aufgehoben.

Solange kein Client authentifiziert ist, wird der Port in das Unsecure-VLAN geschaltet.

Falls ein Default-VLAN konfiguriert ist (VLAN-ID = 1...4095), wird grundsätzlich, nach erfolgreicher Authentifizierung von mindestens einem Client, auf das konfigurierte Default-VLAN geschaltet.

Ist kein Default-VLAN konfiguriert (VLAN-ID = 0), so erwartet der Switch die Zuweisung der VLAN-ID durch den RADIUS Server. Dabei wird die erste empfangene VLAN-ID verwendet, die für einen erfolgreich per IEEE802.1X bzw. MAC-Bypass authentifizierten Client vom RADIUS Server übermittelt wurde.

Über diese Funktionen können z.B. PCs authentifiziert werden, auf denen zusätzlich zur MAC Adresse des PCs selber, weitere MAC Adressen von Virtual Machines verwendet werden.

Clients, die bei der IEEE802.1X Re-Authentication auf EAP-Request-Identity nicht mehr antworten (z.B. PC abgezogen bzw. ausgeschaltet) oder vom RADIUS Server bei der IEEE802.1X bzw. MAC-Bypass Re-Authentication abgelehnt wurden (Benutzer wurde gesperrt), werden erneut geblockt.

Zusätzlich können Clients über das Portsecurity Address Ageing nach einer einstellbaren Zeit automatisch aus der MAC Liste des Ports entfernt werden. Dies ist dann sinnvoll, wenn hinter dem Switchport ein weiterer Switch folgt und deshalb ein Link-Down des Clients nicht erkannt werden kann.

Falls das IEEE802.1X Radius Accounting eingeschaltet ist, werden für alle MAC-Adressen getrennte Datensätze erzeugt. Allerdings enthalten diese keine Counter, da der Switch nur Counter per Port und nicht per MAC-Adresse unterstützt.

10.59.5. Portsecurity Modus {IEEE802.1X allow all MAC-Addresses}

Die Funktionsweise dieses Modus ist weitgehend identisch zum Modus {IEEE802.1X allow one MAC-Address}.

Im Gegensatz zum Modus {IEEE802.1X allow one MAC-Address}, dürfen hier beliebig viele MAC-Adressen auf dem Port empfangen werden. Mindestens eines der angeschlossenen Endgeräte (z.B. Access-Point, der seinerseits IEEE802.1X Authenticator ist) muss IEEE802.1X unterstützen. Der Port wird erst durchgeschaltet, wenn das IEEE802.1X Endgeräte korrekt authentifiziert wurde.

Falls die Option 'IEEE802.1X Radius MAC Bypass' aktiviert ist, wird nach einem IEEE802.1X Timeout ausschließlich die erste detektierte MAC Adresse authentifiziert. Falls der RADIUS Server die MAC Adresse bestätigt, wird der Port durchgeschaltet.

Wichtig: Alle nachfolgenden MAC Adressen werden für eine Authentifizierung ignoriert, auch für den Fall, dass die zuerst detektierte Adresse vom RADIUS Server abgelehnt wurde.

Ein weiterer Unterschied zum Modus {IEEE802.1X allow one MAC-Address} ist, dass hier keine 'New-MAC-Address' Events versendet werden.

10.59.6. Portsecurity Option {IEEE802.1X Radius MAC Bypass}

Diese Option ist nur für Ports relevant, die auf einen IEEE802.1X basierten Securitymode eingestellt sind.

Abhängig von der konfigurierten Einstellung des MAC Bypass, wird vor oder nach einem Authentifizierungsversuch nach IEEE802.1X ein Authentifizierungsversuch der MAC Adresse durchgeführt.

Nach erfolgreicher Authentifizierung der MAC Adresse und eingeschalteter IEEE802.1X 'Re-Authentication', wird eine periodische Re-Authentifizierung der MAC Adresse ausgeführt. Das Zeitintervall dieser Re-Authentifizierung entspricht dabei dem IEEE802.1X 'Re-Authentication intervall'.

Für den RADIUS MAC Bypass kann zwischen folgenden Modi ausgewählt werden:

- Disable
- Send MAC bypass after each IEEE802.1X timeout
- Send single MAC bypass 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 ist deaktiviert.

Send MAC bypass after each IEEE802.1X timeout:

Hier wird zunächst versucht eine Authentifizierung des Ports nach IEEE802.1X durchzuführen. Meldet sich, nach Ablauf der IEEE802.1X Timeouts und Retries das angeschlossene Endgerät nicht mit seiner IEEE802.1X Identity, so wird anschließend versucht die MAC Adresse beim RADIUS Server zu authentifizieren.

- Wird die MAC-Adresse vom RADIUS Server abgelehnt, so werden wechselweise Authentifizierungsversuche nach IEEE802.1X und der MAC Adresse wiederholt, bis eine der beiden Methoden zum Erfolg führt.

- Bei erfolgreicher MAC Authentifizierung werden keine weiteren Authentifizierungsversuche gemäß IEEE802.1X durchgeführt. Eine Rückkehr zu IEEE802.1X kann nur nach Ablauf des IEEE802.1X Re-Authentication Intervalls und einer damit verbundenen Ablehnung der MAC Adresse durch den RADIUS Server erfolgen. Alternativ kann jederzeit eine IEEE802.1X Authentifizierung durch einen Link-Down oder über den Portsecurity Renew-Befehl am betreffenden Port angestoßen werden.

Send single MAC bypass after first IEEE802.1X timeout:

Hier wird zunächst versucht eine Authentifizierung des Ports nach IEEE802.1X durchzuführen. Meldet sich, nach Ablauf der IEEE802.1X Timeouts und Retries das angeschlossene Endgerät nicht mit seiner IEEE802.1X Identity, so wird anschließend ein einziger Versuch durchgeführt die MAC Adresse beim RADIUS Server zu authentifizieren.

- Wird die MAC-Adresse vom RADIUS Server abgelehnt, so werden nur noch Authentifizierungsversuche gemäß IEEE802.1X ausgeführt. Möchte man jedoch eine erneute Authentifizierung der MAC Adresse anstoßen, so muss dies über einen kurzen Link-Down oder über den Portsecurity 'Renew-Befehl' erfolgen.
- Bei erfolgreicher MAC Authentifizierung werden keine weiteren Authentifizierungsversuche gemäß IEEE802.1X durchgeführt bzw. akzeptiert. Eine Rückkehr zu IEEE802.1X kann nur nach Ablauf des IEEE802.1X Re-Authentication Intervalls und einer damit verbundenen Ablehnung der MAC Adresse durch den RADIUS Server erfolgen. Alternativ kann jederzeit eine IEEE802.1X Authentifizierung durch einen Link-Down oder über den Portsecurity Renew-Befehl am betreffenden Port angestoßen werden.

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:**

Diese Modi sind identisch zu den obigen Modi **Send MAC bypass after each IEEE802.1X timeout** bzw.

Send single MAC bypass after first IEEE802.1X timeout, jedoch kann nach erfolgreicher MAC Authentifizierung jederzeit eine erneute IEEE802.1X Authentifizierung durch das angeschlossene Endgerät angestoßen werden. Dies erfolgt, indem das Endgerät ein beliebiges EAP Paket an den Switch sendet (üblicherweise einen EAP-Start Request). Diese Funktion ist insbesondere dann interessant, wenn das angeschlossene Endgerät erst nach erfolgreicher MAC Authentifizierung seine IEEE802.1X Funktion aktiviert (z.B. während der Erstbetankung von PCs).

Send MAC bypass immediately and after each IEEE802.1X timeout:

Hier wird sofort nach erkennen der MAC Adresse versucht, diese beim RADIUS Server zu authentifizieren.

- Wird die MAC-Adresse vom RADIUS Server abgelehnt, so werden wechselweise Authentifizierungsversuche nach IEEE802.1X und der MAC Adresse wiederholt, bis eine der beiden Methoden zum Erfolg führt.
- Bei erfolgreicher MAC Authentifizierung werden keine weiteren Authentifizierungsversuche gemäß IEEE802.1X durchgeführt. Eine Rückkehr zu IEEE802.1X kann nur nach Ablauf des IEEE802.1X Re-Authentication Intervalls und einer damit verbundenen Ablehnung der MAC Adresse durch den RADIUS Server erfolgen. Alternativ kann jederzeit eine IEEE802.1X Authentifizierung durch einen Link-Down oder über den Portsecurity Renew-Befehl am betreffenden Port angestoßen werden.

Send single MAC bypass immediately:

Hier wird sofort nach erkennen der MAC Adresse versucht, diese beim RADIUS Server zu authentifizieren.

- Wird die MAC-Adresse vom RADIUS Server abgelehnt, so werden nur noch Authentifizierungsversuche gemäß IEEE802.1X ausgeführt. Möchte man jedoch eine erneute Authentifizierung der MAC Adresse anstoßen, so muss dies über einen kurzen Link-Down oder über den Portsecurity 'Renew-Befehl' erfolgen.
- Bei erfolgreicher MAC Authentifizierung werden keine weiteren Authentifizierungsversuche gemäß IEEE802.1X durchgeführt bzw. akzeptiert. Eine Rückkehr zu IEEE802.1X kann nur nach Ablauf des IEEE802.1X Re-Authentication Intervalls und einer damit verbundenen Ablehnung der MAC Adresse durch den RADIUS Server erfolgen. Alternativ kann jederzeit eine IEEE802.1X Authentifizierung durch einen Link-Down oder über den Portsecurity Renew-Befehl am betreffenden Port angestoßen werden.

Send MAC bypass immediately and after each IEEE802.1X timeout, with IEEE802.1X fallback:**Send single MAC bypass immediately, with IEEE802.1X fallback:**

Diese Modi sind identisch zu den obigen Modi **Send MAC bypass immediately and after each IEEE802.1X timeout** bzw. **Send single MAC bypass immediately**, jedoch kann nach erfolgreicher MAC Authentifizierung jederzeit eine erneute IEEE802.1X Authentifizierung durch das angeschlossene Endgerät angestoßen werden. Dies erfolgt, indem das Endgerät ein beliebiges EAP Paket an den Switch sendet (üblicherweise einen EAP-Start Request). Diese Funktion ist insbesondere dann interessant, wenn das angeschlossene Endgerät erst nach erfolgreicher MAC Authentifizierung seine IEEE802.1X Funktion aktiviert (z.B. während der Erstbetankung von PCs).

10.59.7. Portsecurity Option {Toggle Link}

Ist diese Funktion aktiviert, so wird nach einer erfolgreichen RADIUS MAC Authentifizierung (z.B. per IEEE802.1X MAC Bypass) der Link des betreffenden Ports für eine Sekunde unterbrochen. Dadurch wird erzwungen, dass das angeschlossene Endgerät eine neue IP Adresse per DHCP anfordert. Dabei bleiben die bereits gelernten MAC Adressen des Switchports erhalten.

Diese Funktion ist hilfreich, wenn das Endgerät zunächst im Unsecure-VLAN eine IP Adresse erhalten hat und nach erfolgter MAC Authentifizierung in ein anderes VLAN mit einem anderen IP-Range verschoben werden soll.

10.59.8. Portsecurity Option {EAP Packets within Voice-VLAN}

Hier kann konfiguriert werden, ob IEEE802.1X EAP Pakete, die als Zieladresse die MAC-Adresse eines Telefons im Voice-VLAN enthalten, mit oder ohne VLAN-Tag gesendet werden. Die korrekte Einstellung ist abhängig von der Vorgabe des jeweiligen Telefonherstellers.

10.59.9. Portsecurity Modus {IEEE802.1X Supplicant mit MD5}

Durch diese Funktion, kann der Switch zum Uplink hin als IEEE802.1X Supplicant arbeiten und sich gegenüber dem Core-Switch per EAP MD5-Challenge authentifizieren. Dies schützt vor Ausbau des Switches um über die Uplink-Faser Zugriff auf das Netzwerk zu erhalten.

HINWEIS:

Der Core-Switch muss einen IEEE802.1X Modus unterstützen, der nach Authentifizierung des Nexans Switches alle weiteren MAC Adressen ohne Authentifizierung durchlässt. Der entsprechende Modus bei Nexans Switches heißt {IEEE802.1X allow all MAC-Addresses}.

10.60. RADIUS Accounting

Der Switch unterstützt das RADIUS Accounting-Protokoll gemäß RFC2866. Dieses Protokoll kann für die MAC und IEEE802.1X basierte Authentifizierung separat aktiviert werden. Für das Radius Accounting steht, neben der Radius Authentication, ein kompl. eigener Parametersatz für die RADIUS Server Konfiguration zur Verfügung.

Radius Accounting kann z.B. für folgenden Aufgaben eingesetzt werden:

- Aufzeichnung der genauen Zeiträume, die eine MAC-Adresse bzw. ein IEEE802.1X User aktiv war
- Aufzeichnung der zugehörigen IP-Adressen (nur beim GigaSwitch BM+ / GigaSwitch V2+ möglich)
- Aufzeichnung der Byte und Paket-Zähler für jeden Port zwecks Abrechnung oder Kontrolle des Datenvolumen

HINWEIS:

Alle Counter werden mit 64-Bit übermittelt. Dabei werden die erweiterten Radius Attribute 'Acct-Input-Gigawords' und 'Acct-Output-Gigawords' verwendet. Ein Überlaufen der Counter ist dadurch praktisch ausgeschlossen. Sollte ein Portsecurity Mode eingestellt sein, der mehr als eine MAC Adresse pro Port erlaubt, so werden keine Counter übermittelt da der Switch nur Counter per Port und nicht per MAC-Adresse unterstützt.

10.60.1. RADIUS Accounting-Einstellungen

Die folgende Tabelle zeigt eine Übersicht aller RADIUS Accounting-Einstellungen:

Bez. im NEXMAN	Default Wert	Funktion
IEEE802.1X Accounting enable	disabled	Wenn ausgewählt, wird für die IEEE802.1X Authentifizierung das Accounting eingeschaltet. Dies gilt für alle Ports auf denen ein IEEE802.1X basierter Security Mode aktiviert ist.
MAC based Accounting enable	disabled	Wenn ausgewählt, wird für die MAC basierte Authentifizierung das Accounting eingeschaltet. Dies gilt für alle Ports auf denen eine MAC basierte Authentifizierung durchgeführt wird. Sofern ein IEEE802.1X basierter Security Mode aktiviert und gleichzeitig der 'IEEE802.1X Radius MAC Bypass'

		eingeschaltet ist, so wird bei Ausführung des MAC Bypass ebenfalls das Accounting ausgeführt.
Server 1 Address		Es können vier RADIUS Server IP-Adressen angegeben, wobei die erste IP-Adresse immer den primären RADIUS Server angibt. Abhängig vom eingestellten Algorithmus für Server-Anfragen sind die anderen IP-Adressen für die Backup-RADIUS Server reserviert, oder sie werden abwechselnd oder parallel abgefragt (siehe Feld 'Server request algorithm' unten). Per NEXMAN (Reiter 'Radius State' und 'MAC+Security State') und per Console Kommando 'sh:ow ra:d:ius ac:counting' kann der Status der RADIUS Server kontrolliert werden.
Server 2 Address		
Server 3 Address		
Server 4 Address		
Accounting UDP Port	1813	Die UDP Port-Nummer, auf der der RADIUS Servers Accounting Requests empfängt. Die offizielle Nummer ist 1813, nach einer älteren Spezifikation ist aber auch 1646 möglich.
Request timeout	5	Die maximale Zeit in Sekunden, die der Switch nach einem Radius-Request auf die Antwort des RADIUS Servers wartet.
Request retries	2	Gibt an, wie oft der Switch einen Radius-Request wiederholt, bevor der Request als fehlgeschlagen angesehen wird. Der entsprechende RADIUS Server wird in der Statusanzeige als 'down' gekennzeichnet.
Shared secret	<leer>	Das sogenannte 'Shared Secret' dient als Passwort gegenüber dem RADIUS Server. Dieses muss im Switch und im RADIUS Server identisch eingetragen werden.
Alive packets enable	disabled	Wenn ausgewählt, werden in periodischen Abständen sogenannte Alive oder Interrim Pakete zum RADIUS Server gesendet.
Alive packets intervall	10 min	Bestimmt das Intervall für das Versenden der oben genannten Alive Pakete
User-Name for 802.1X	EAP only	Bestimmt, welcher Name für das Radius Accounting Attribut 'User-Name' herangezogen wird. Folgende Einstellungen sind möglich: • EAP-Identity only • User-Name from Access-Accept • Chargeable-User-Identity from Access-Accept EAP-Identity only: Bei dieser Einstellung wird ausschließlich der beim EAP-Response-Identity vom Endgerät übermittelte Name verwendet. User-Name from Access-Accept: Diese Einstellung ist vor allem bei Verwendung von EAP-TTLS sinnvoll, weil in diesem Fall das EAP-Response-Identity Paket nur einen anonymen Namen enthält. Sofern der RADIUS Server die Übermittlung des tatsächlichen Namens per User-Name Attribut unterstützt, sollte diese Einstellung ausgewählt werden. Wird allerdings kein User-Name Attribut vom Server geliefert, so wird wiederum der Name aus dem EAP-Response-Identity Paket verwendet. Chargeable-User-Identity from Access-Accept: Diese Einstellung ist vor allem bei Verwendung von EAP-TTLS sinnvoll, weil in diesem Fall das EAP-Response-Identity Paket nur einen anonymen Namen enthält. Sofern der RADIUS Server die Übermittlung des tatsächlichen Namens per Chargeable-User-Identity Attribut gemäß RFC4372 unterstützt, sollte diese Einstellung ausgewählt werden. Wird allerdings kein Chargeable-User-Identity Attribut vom Server geliefert, so wird wiederum der Name aus dem EAP-Response-Identity Paket verwendet.
Discover IP Address	disabled	Wenn dieser Parameter auf 'Discover to Framed-IP-Address' eingestellt wird, so wird nach erfolgreicher MAC oder IEEE802.1X basierter Authentifizierung die IP Adresse des Endgerätes ermittelt. Die IP Adresse wird dann in allen Alive Paketen und im Stop Paket als Framed-IP-Address Attribut übermittelt.

10.60.2. RADIUS Attribute zum Accounting

Folgende Radius Attribute werden vom Switch and den Radius Accounting Server gesendet:

Attribut	Attribut enthält ...
Acct-Status-Type	Der Typ des Accounting Paketes. Dies ist entweder 'Start', 'Alive' oder 'Stop'
Acct-Session-ID	Dient dem RADIUS Server zur eindeutigen Zuordnung der einzelnen Accounting Pakete. Sie wird vom Switch für jede neue erfolgreiche Authentifizierung hochgezählt. Ferner wird die Anzahl der Switch Reboots als Teil der ID mit einbezogen, so dass sich die ID's auch nach einem Reboot nicht wiederholen können.
Acct-Session-Time	Zeit in Sekunden, die seit der erfolgreichen Authentifizierung vergangen ist. Dieses Attribut ist nicht im Start Paket enthalten, da beim Start die Zeit bei 0 beginnt.
NAS-IP-Address	IP-Adresse des Nexans Switches
NAS-Identifizier	Switch Name
NAS-Port	Nummer des Switchports
NAS-Port_ID	Bezeichnung des Switchports
NAS-Port-Type	Ethernet (15)
Calling-Station-ID	Die Calling-Station-ID besteht aus einem Textstring, der die MAC-Adresse des Endgerätes enthält. Das Format ist in RFC3580 definiert und lautet wie folgt: XX-XX-XX-XX-XX-XX Beispiel: MAC-Adresse: 00c02900000f → Calling-Station-ID: 00-C0-29-00-00-0F
Framed-IP-Address	IP-Adresse des Endgerätes. Siehe obige Erläuterungen zu Parameter 'Discover IP Address'.
User-Name	Bei IEEE802.1X basierter Authentifizierung wird hier üblicherweise der beim EAP-Response-Identity vom Endgerät übermittelte Name eingesetzt. Dies ist jedoch abhängig von der oben erläuterten Einstellung 'User-Name for 802.1X'. Im Falle der MAC basierten Authentifizierung besteht der User-Name aus einem Textstring, der die MAC-Adresse enthält. Das Format ist wie folgt: xx<sep>xx<sep>xx<sep>xx<sep>xx<sep>xx Dabei sind xx die einzelnen Bytes der MAC-Adresse und <sep> ein frei wählbarer MAC-Separator. Dieses Attribut kann außerdem optional um einen festen Realm-String ergänzt werden. Dieser Portsecurity-REALM wird dann vor (prefix) oder hinter (suffix) die eigentliche MAC-Adresse angefügt und durch einen Realm-Separator getrennt. Beispiel: MAC-Adresse: 00c02900000f MAC-Separator : : Portsecurity-REALM: nexans-port Realm-Separator: @ Realm-Position: suffix → User-Name: 00:c0:29:00:00:0f@nexans-port
Chargeable-User-Identity	
Acct-Input-Octets Acct-Input-Gigawords	Ein 64-Bit Counter, der die Anzahl der vom Switch empfangenen Bytes enthält. Zur Berechnung des Wertes muss folgende Formel verwendet werden: Input-Bytes = (Acct-Input-Gigawords * 2³²) + Acct-Input-Octets

Acct-Output-Octets Acct-Output-Gigawords	Ein 64-Bit Counter, der die Anzahl der vom Switch gesendeten Bytes enthält. Zur Berechnung des Wertes muss folgende Formel verwendet werden: $\text{Output-Bytes} = (\text{Acct-Output-Gigawords} * 2^{32}) + \text{Acct-Output-Octets}$
Acct-Input-Packets	Ein 32-Bit Counter, der die Anzahl der vom Switch empfangenen Pakete enthält.
Acct-Output-Packets	Ein 32-Bit Counter, der die Anzahl der vom Switch gesendeten Pakete enthält.

HINWEIS:

Die Counter sind nicht im Start Paket enthalten, da beim Start alle Counter bei 0 beginnen.

10.61. TACACS+ Authentication

HW5-Switches unterstützen das TACACS+ Authentifizierungs-Protokoll gemäß Draft IETF-opsawg-tacacs-15.

Dieses Protokoll wird für folgende Authentifizierungsaufgaben im Switch verwendet:

- Telnet Authentifizierung von Name/Passwort
- SSHv2 Authentifizierung von Name/Passwort
- V.24 Authentifizierung von Name/Passwort
- SCP Authentifizierung von Name/Passwort

Die Funktionsweise der einzelnen Modi wird in den nachfolgenden Kapiteln detailliert beschrieben.

10.61.1. TACACS+ Authentication-Einstellungen

Die folgende Tabelle zeigt eine Übersicht der TACACS+ Authentication-Einstellungen:

Bez. im NEXMAN	Default Wert	Funktion
Server 1 Address		Es können vier TACACS+ Authentifizierungs-Server IP-Adressen angegeben, wobei die erste IP-Adresse immer den primären TACACS+ Server angibt. Abhängig vom eingestellten Algorithmus für Server-Anfragen sind die anderen IP-Adressen für die Backup TACACS+ Authentifizierungs-Server reserviert, oder sie werden abwechselnd oder parallel abgefragt (siehe Feld 'Server request algorithm' unten). Per NEXMAN (Reiter TACACS+State' und 'MAC+Security State') und per Console Kommando 'sh:ow t:acacs+' kann der Status der TACACS+ Authentifizierungs-Server kontrolliert werden.
Server 2 Address		
Server 3 Address		
Server 4 Address		
Authentication TCP Port	49	Die TCP Port-Nummer, auf der der TACACS+ Authentifizierungs-Servers Authentication Requests empfängt. Die offizielle Nummer ist 49.
Shared secret	<empty>	Das sogenannte 'Shared Secret' dient als Passwort gegenüber dem TACACS+ Authentifizierungs-Server. Dieses muss im Switch und im TACACS+ Authentifizierungs-Server identisch eingetragen werden.
Request timeout	5	Die maximale Zeit in Sekunden, die der Switch nach einem TACACS+ Authentication-Request auf die Antwort des TACACS+ Authentifizierungs-Servers wartet.
Server request algorithm	Strict-Priority	Hier kann konfiguriert werden, mit welchem Algorithmus die TACACS+ Authentifizierungs-Server abgefragt werden: Strict-Priority: Die TACACS+ Authentifizierungs-Server werden strikt in Reihenfolge unabhängig vom Status abgefragt. Es wird immer von dem als erstes eingetragenen TACACS+ Authentifizierungs-Server angefangen. Round-Robin: Im Gegensatz zur Strict-Priority wird beim Round-Robin die Reihenfolge der eingetragenen TACACS+ Authentifizierungs-Server fortgesetzt. Ist

		beispielsweise eine Authentifizierung bei Server 1 erfolgt, wird die nächste Anfrage bei Server 2 gestartet. Nach Abarbeiten des letzten Servers in der Liste beginnt die Anfrage erneut beim ersten. Durch diesen Algorithmus wird die Verbindung und Verwendung aller eingetragenen TACACS+ Authentifizierungs-Server gewährleistet. Parallel: Alle eingetragenen TACACS+ Authentifizierungs-Server werden bei einer Anfrage parallel abgefragt. Die erste Antwort, die vom Server zurückkommt, wird vom Switch akzeptiert.
--	--	--

10.62. TACACS+ Authorization

HW5-Switches unterstützen das TACACS+ Autorisierungs-Protokoll gemäß Draft IETF-opsawg-tacacs-15.

Dieses Protokoll wird für folgende Autorisierungsaufgaben im Switch verwendet:

- Telnet Autorisierung von Usern für allgemein Zugriffsrechte (read-write, read-only)
- Telnet Autorisierung von CLI-Befehlen
- SSHv2 Autorisierung von Usern für allgemein Zugriffsrechte (read-write, read-only)
- SSHv2 Autorisierung von CLI-Befehlen
- V.24 Autorisierung von Usern für allgemein Zugriffsrechte (read-write, read-only)
- V.24 Autorisierung von CLI-Befehlen
- SCP Autorisierung von Usern für allgemein Zugriffsrechte (read-write, read-only)

Die Funktionsweise der einzelnen Modi wird in den nachfolgenden Kapiteln detailliert beschrieben.

WICHTIG:

Für die TACACS+ Autorisierung (Telnet, SSHv2, V24, SCP) können separate Einstellungen konfiguriert werden. Wenn jedoch der 'TACACS+ Authorization Mode' auf 'Use Authentication Server Setup' gesetzt ist (factory default), werden die Authentifizierungs-Einstellungen für alle TACACS+ Autorisierungsanfragen verwendet.

Für die Autorisierung von Konsolen-Befehlen muss Option 'Command Authorization' aktiviert sein.

10.62.1. TACACS+ Authorization-Einstellungen

Die folgende Tabelle zeigt eine Übersicht der TACACS+ Authorization-Einstellungen:

Bez. im NEXMAN	Default Wert	Funktion
Authorization Mode	Use Authentication Server Setup	Gibt an, ob die globalen TACACS+ Authentifizierungs-Einstellungen oder der folgende separate Parametersatz für die Autorisierung von Usern und Konsolen-Befehlen (Telnet, SSHv2, V24, SCP) verwendet werden sollen.
Command Authorization	disabled	Gibt an, ob die Autorisierung von Konsolen-Befehlen aktiviert werden soll. Falls diese Option deaktiviert ist, werden die allgemeinen Zugriffsrechte, die bei der User-Authorisierung empfangen wurden, verwendet.
Server 1 Address		Es können vier TACACS+ Autorisierungs-Server IP-Adressen angegeben, wobei die erste IP-Adresse immer den primären TACACS+ Autorisierungs-Server angibt. Abhängig vom eingestellten Algorithmus für Server-Anfragen sind die anderen IP-Adressen für die Backup TACACS+ Autorisierungs-Server reserviert, oder sie werden abwechselnd oder parallel abgefragt (siehe Feld 'Server request algorithm' unten). Per NEXMAN (Reiter TACACS+State' und 'MAC+Security State') und per Console Kommando 'sh : ow t : acacs+' kann der Status der TACACS+ Autorisierungs-Server kontrolliert werden.
Server 2 Address		
Server 3 Address		
Server 4 Address		
Authorization TCP Port	49	Die TCP Port-Nummer, auf der der TACACS+ Autorisierungs-Server Authorization-Requests empfängt. Die offizielle Nummer ist 49.
Shared secret	<empty>	Das sogenannte 'Shared Secret' dient als Passwort gegenüber dem TACACS+ Autorisierungs-Server. Dieses muss im Switch und im TACACS+ Autorisierungs-Server identisch eingetragen werden.

Request timeout	5	Die maximale Zeit in Sekunden, die der Switch nach einem TACACS+ - Authorization-Request auf die Antwort des TACACS+ Authorisierungs-Servers wartet.
Server request algorithm	Strict-Priority	Hier kann konfiguriert werden, mit welchem Algorithmus die TACACS+ Authorisierungs-Server abgefragt werden: Strict-Priority: Die TACACS+ Authorisierungs-Server werden strikt in Reihenfolge unabhängig vom Status abgefragt. Es wird immer von dem als erstes eingetragenen TACACS+ Authorisierungs-Server angefangen. Round-Robin: Im Gegensatz zur Strict-Priority wird beim Round-Robin die Reihenfolge der eingetragenen TACACS+ Authorisierungs-Server fortgesetzt. Ist beispielsweise eine Authorisierung bei Server 1 erfolgt, wird die nächste Anfrage bei Server 2 gestartet. Nach abarbeiten des letzten Servers in der Liste beginnt die Anfrage erneut beim ersten. Durch diesen Algorithmus wird die Verbindung und Verwendung aller eingetragenen TACACS+ Authorisierungs-Server gewährleistet. Parallel: Alle eingetragenen TACACS+ Authorisierungs-Server werden bei einer Anfrage parallel abgefragt. Die erste Antwort, die vom Server zurückkommt, wird vom Switch akzeptiert.

10.63. TACACS+ Accounting

HW5-Switches unterstützen das TACACS+ Accounting-Protokoll gemäß Draft IETF-opsawg-tacacs-15.

Dieses Protokoll wird für folgende Accounting-Aufgaben im Switch verwendet:

- Aufzeichnung des exakten Zeitraums, in dem der TACACS+ User aktiv war
- Aufzeichnung der zugehörigen IP-Adressen
- Aufzeichnung der ausgeführten Konsolen-Befehle

Die Funktionsweise der einzelnen Modi wird in den nachfolgenden Kapiteln detailliert beschrieben.

WICHTIG:

Für das TACACS+ Accounting können separate Einstellungen konfiguriert werden. Wenn jedoch der 'TACACS+ Accounting Mode' auf 'Use Authentication Server Setup' gesetzt ist, werden die Authentifizierungs-Einstellungen für alle TACACS+ Accounting-Anfragen verwendet.

Für die Aufzeichnung von Konsolen-Befehlen muss Option 'Command Authorization' aktiviert sein.

10.63.1. TACACS+ Accounting-Einstellungen

Die folgende Tabelle zeigt eine Übersicht der TACACS+ Accounting-Einstellungen:

Bez. im NEXMAN	Default Wert	Funktion
Accounting Mode	disabled	Gibt an, ob die globalen TACACS+ Authentifizierungs-Einstellungen oder der folgende separate Parametersatz für die Aufzeichnung (Telnet, SSHv2, V24, SCP) verwendet werden sollen.
Server 1 Address		Es können vier TACACS+ Accounting-Server IP-Adressen angegeben, wobei die erste IP-Adresse immer den primären TACACS+ Accounting-Server angibt. Abhängig vom eingestellten Algorithmus für Server-Anfragen sind die anderen IP-Adressen für die Backup TACACS+ Accounting-Server reserviert, oder sie werden abwechselnd oder parallel abgefragt (siehe Feld 'Server request algorithm' unten). Per NEXMAN (Reiter TACACS+State' und 'MAC+Security State') und per Console Kommando 'sh : ow t : acacs+' kann der Status der TACACS+ Accounting Server kontrolliert werden.
Server 2 Address		
Server 3 Address		
Server 4 Address		
Accounting TCP Port	49	Die TCP Port-Nummer, auf der der TACACS+ Accounting-Servers Accounting-Requests empfängt. Die offizielle Nummer ist 49.

Shared secret	<empty>	Das sogenannte 'Shared Secret' dient als Passwort gegenüber dem TACACS+ Accounting-Server. Dieses muss im Switch und im TACACS+ Accounting-Server identisch eingetragen werden.
Request timeout	5	Die maximale Zeit in Sekunden, die der Switch nach einem TACACS+ Accounting-Request auf die Antwort des TACACS+ Accounting-Servers wartet.
Server request algorithm	Strict-Priority	Hier kann konfiguriert werden, mit welchem Algorithmus die TACACS+ Accounting-Server abgefragt werden: Strict-Priority: Die TACACS+ Accounting-Server werden strikt in Reihenfolge unabhängig vom Status abgefragt. Es wird immer von dem als erstes eingetragenen TACACS+ Accounting-Server angefangen. Round-Robin: Im Gegensatz zur Strict-Priority wird beim Round-Robin die Reihenfolge der eingetragenen TACACS+ Accounting-Server fortgesetzt. Ist beispielsweise eine Authentifizierung bei Server 1 erfolgt, wird die nächste Anfrage bei Server 2 gestartet. Nach abarbeiten des letzten Servers in der Liste beginnt die Anfrage erneut beim ersten. Durch diesen Algorithmus wird die Verbindung und Verwendung aller eingetragenen TACACS+ Accounting-Server gewährleistet. Parallel: Alle eingetragenen TACACS+ Accounting-Server werden bei einer Anfrage parallel abgefragt. Die erste Antwort, die vom Server zurückkommt, wird vom Switch akzeptiert.

10.64. TACACS+ Console Authentication Modes

Für die SSHv2-, Telnet- und V.24-Console können sechs verschiedene Authentifizierungs-Modi eingestellt werden:

- Local: Lokale Authentifizierung
- Disabled: Telnet Interface disabled
- Radius only: Authentifizierung ausschließlich durch den RADIUS Server
- Radius first, then local: Authentifizierung durch RADIUS, nur falls kein Server antwortet: lokale Authentifizierung
- TACACS+ only: Authentifizierung ausschließlich durch den TACACS+ Server
- TACACS+ first, then local: Authentifizierung durch TACACS+, nur falls kein Server antwortet: lokale Authentifizierung

Local (factory default):

Disabled:

Siehe Kapitel [10.14. V.24 Console Authentication Mode](#), [10.48 Telnet Console Authentication Mode](#) und [10.49. SSHv2 Console Authentication Mode](#).

Radius Only:

Radius first, then local:

Siehe Kapitel [10.56 RADIUS Console Authentication Modes](#)

TACACS+ only:

Statt die lokal gespeicherten Authentifizierungsdaten zu verwenden, wird die Authentifizierung durch einen zentralen TACACS+ Authentifizierungs-Server durchgeführt.

Zusätzlich wird der User durch einen TACACS+ Authorisierungs-Server für allgemeine Zugriffsrechte (read-write, read-only) autorisiert.

TACACS+ first, then local:

In diesem Modus wird zunächst eine Authentifizierung über TACACS+ Authentifizierungs-Server versucht. Nur wenn keiner der eingestellten TACACS+ Authentifizierungs-Server abhängig vom gesetzten Server-Anfragealgorithmus antwortet, wird der eingegebene Login-Name und das Passwort mit den lokal gespeicherten Daten verglichen.

Zusätzlich wird der User durch einen TACACS+ Authorisierungs-Server für allgemeine Zugriffsrechte (read-write, read-only) autorisiert. Nur wenn keiner der eingestellten TACACS+ Authorisierungs-Server abhängig vom gesetzten Server-Anfrage-Algorithmus antwortet, werden die lokale Zugriffsrechte verwendet.

Die TACACS+ Authentifizierung bzw. Authorisierung von Usern läuft wie folgt ab:

- Der User gibt beim Console Login seinen Namen und Passwort ein.
- Der Switch sendet den Namen per TACACS+ Authentication-Request an den TACACS+ Authentifizierungs-Server.
- Der TACACS+ Authentifizierungs-Server antwortet mit einem TACACS+ Authentication-Reply und Status "Send Password".
- Der Switch sendet das Passwort per TACACS+ Authentication-Request an den TACACS+ Authentifizierungs-Server.
- Der TACACS+ Authentifizierungs-Server überprüft Name und Passwort und antwortet mit einem TACACS+ Authentication-Reply, der den Status "Authentication Passed" oder "Authentication Failed" enthält.
- Wird ein Authentication-Reply mit Status "Authentication Failed" empfangen, so wird bei V.24- oder Telnet-Consolen die Fehlermeldung "Wrong Authentication" am Console-Prompt ausgegeben.
- Wird ein Authentication-Reply mit Status "Authentication Passed" empfangen, sendet der Switch einen TACACS+ Authorization-Request an den TACACS+ Authorisierungs-Server.
- Antwortet kein TACACS+ Authentifizierungs-Server abhängig vom gesetzten Anfrage-Algorithmus (Timeout), so wird bei V.24- oder Telnet-Consolen die Fehlermeldung "No Response From TACACS+ Authentication Server" am Console-Prompt ausgegeben. Außerdem wird ein Alarm in der Device List des Managers angezeigt.
- Der TACACS+ Authorisierungs-Server überprüft, ob der User autorisiert werden kann und welche allgemeinen Zugriffsrechte er hat, und antwortet mit einem TACACS+ Authorization-Reply, der den Status "PASS_ADD" oder "FAIL" enthält.
- Wird ein Authorization-Reply mit Status "FAIL" empfangen, so wird bei V.24- oder Telnet-Consolen die Fehlermeldung "Wrong Authorization" am Console-Prompt ausgegeben.
- Wird ein Authorization-Reply mit Status "PASS_ADD" empfangen, so werden die allgemeinen Zugriffsrechte gemäß dem enthaltenen Nexans-spezifischen Attribut 'nx-access' gewährt (NX-ACCESS-RW für Admin-Zugriffrechte (R/W) oder NX-ACCESS-RO for User-Zugriffrechte (R/O)). Wird ein Authorization-Reply ohne dieses Attribut oder mit einem unzulässigen 'nx-access'-Wert empfangen, so wird bei V.24- oder Telnet-Consolen die Fehlermeldung "Wrong Authorization" am Console-Prompt ausgegeben.
- Antwortet kein TACACS+ Authorisierungs-Server abhängig vom gesetzten Anfrage-Algorithmus (Timeout), so wird bei V.24- oder Telnet-Consolen die Fehlermeldung "No Response From TACACS+ Authorization Server" am Console-Prompt ausgegeben. Außerdem wird ein Alarm in der Device List des Managers angezeigt.
- Falls TACACS+ Accounting aktiviert ist, sendet der Switch den User-Namen per TACACS+ Accounting-Request an den TACACS+ Accounting-Server.
- Der TACACS+ Accounting-Server trägt den User-Login in einer Log-Datei ein und antwortet mit einem TACACS+ Accounting-Reply, der den Status "Success" oder "Error" enthält.

10.64.1. TACACS+ Attribute zur User-Authentifizierung

Folgende TACACS+ Attribute werden vom Switch an den TACACS+ Authentifizierungs-Server zur User-Authentifizierung gesendet:

Attribut	Attribut enthält ...
Action	Auszuführende Authentifizierungsaktion. Die einzige aktuell unterstützte Aktion ist: Inbound Login (1)
Privilege Level	Cisco Privilege Level 0...15 des angefragten Users (von Nexans Switchen nicht verwendet)
Authentication type	Zu verwendender Authentifizierungstyp. Der einzige aktuell unterstützte Typ ist: ASCII (1)
Service	Zu verwendendes Service-Protokoll. Das einzige aktuell unterstützte Protokoll ist: PPP (3)

User	User-Name oder Passwort
Data	Daten für Authentifizierung (nicht verwendet)

Folgende TACACS+ Attribute werden vom Switch zur User-Authentifizierung gelesen:

Attribut	Attribut enthält ...
Status	Der Status des Authentication-Requests: Send password (0x05) → Sende Passwort für User an TACACS+ Authentifizierungs-Server Authentication Passed (0x01) → User-Authentifizierung erfolgreich Authentication Failed (0x02) → User-Authentifizierung fehlgeschlagen
Flags	Status-Flags: Send password → 0x01 (NoEcho) Authentication Passed/Failed → 0x00
Server message	Anzuzeigende Nachricht vom TACACS+ Authentifizierungs-Server: Send password → Passwort-Prompt (default "Password:") Authentication Passed/Failed → -
Data	Daten für Authentifizierung (nicht verwendet)

10.64.2. TACACS+ Attribute zur User-Authorisierung

Folgende TACACS+ Attribute werden vom Switch an den TACACS+ Authorisierungs-Server zur User-Authorisierung gesendet:

Attribut	Attribut enthält ...
Auth Method	Anzuwendende Authorisierungsmethode: TACACSPLUS (0x06)
Privilege Level	Cisco Privilege Level 0...15 des angefragten Users (von Nexans Switchen nicht verwendet)
Authentication type	Zu verwendender Authentifizierungstyp. Der einzige aktuell unterstützte Typ ist: ASCII (1)
Service	Zu verwendendes Service-Protokoll. Das einzige aktuell unterstützte Protokoll ist: PPP (3)
User	User-Name
Port	Die TCP Port-Nummer, auf der der TACACS+ Authorisierungs-Server Authorization-Requests empfängt. Die offizielle Nummer ist 49.
Remote Address	Remote IP-Adresse des TACACS+ Authorisierungs-Servers
Arg[0...1] (AV-pairs):	service=shell → Shell-Authorisierung cmd= → Allgemeine Zugriffsrechte für Consolen-Befehle anfordern

Folgende TACACS+ Attribute werden vom Switch zur User-Authorisierung gelesen:

Attribut	Attribut enthält ...
Auth Status	Der Status des Authorization-Requests: PASS_ADD (0x01) → Authorisierung erfolgreich FAIL (0x02) → Authorisierung fehlgeschlagen
Data	Daten für Authorisierung (nicht verwendet)
Arg[0...1] (AV-pairs):	priv-lvl=0...15 → Cisco Privilege Level 0...15 des angefragten Users (von Nexans Switchen nicht verwendet)

	nx-access=<general access rights> → Der Authorization-Reply muss dieses <i>Nexans</i> -spezifische Attribut enthalten. Es gibt Auskunft darüber, ob der User als Admin-Account (R/W) oder User-Account (R/O) eingeloggt werden soll. Folgende Attribut-Werte sind zulässig: NX-ACCESS-RW → Admin access rights (R/W) NX-ACCESS-RO → User access rights (R/O)
--	--

10.64.3. TACACS+ Attribute zum User-Accounting

Falls TACACS+ Accounting aktiviert ist, werden folgende TACACS+ Attribute vom Switch an den TACACS+ Accounting-Server zum User-Accounting gesendet:

Attribut	Attribut enthält ...
Auth Method	Anzuwendende Accounting-Methode: TACACSPPLUS (0x06)
Privilege Level	Cisco Privilege Level 0...15 des angefragten Users (von <i>Nexans</i> Switchen nicht verwendet)
Authentication type	Zu verwendender Authentifizierungstyp. Der einzige aktuell unterstützte Typ ist: ASCII (1)
Service	Zu verwendendes Service-Protokoll. Das einzige aktuell unterstützte Protokoll ist: PPP (3)
User	User-Name
Port	Die TCP Port-Nummer, auf der der TACACS+ Accounting-Server Accounting-Requests empfängt. Die offizielle Nummer ist 49.
Remote Address	Remote IP-Adresse des TACACS+ Accounting-Servers
Arg[0...2] (AV-pairs):	task_id=<id> → Task ID zur Identifikation der AAA-Aktion timezone=UTC → Zeitzone für Accounting-Eintrag in der Log-Datei (UTC) service=shell → Shell-Accounting

Falls TACACS+ Accounting aktiviert ist, werden folgende TACACS+ Attribute vom Switch zum User-Accounting gelesen:

Attribut	Attribut enthält ...
Auth Status	Der Status des Accounting-Requests: Success (0x01) → Accounting erfolgreich Error (0x02) → Accounting fehlgeschlagen
Data	Daten für Accounting (nicht verwendet)

10.65. TACACS+ Console Command Authorization

Falls Console Command Authorization aktiviert ist, wird jeder Consolen-Befehl über einen TACACS+ Authorisierungs-Server autorisiert.

Die TACACS+ Authorisierung von Consolen-Befehlen für läuft wie folgt ab:

- Der User gibt den Consolen-Befehl ein.
- Der Switch sendet einen TACACS+ Authorization-Request mit dem Consolen-Befehl an den TACACS+ Authorisierungs-Server.
- Der TACACS+ Authorisierungs-Server überprüft, ob der User autorisiert ist den Befehl auszuführen, und antwortet mit einem TACACS+ Authorization-Reply, der den Status "PASS_ADD" oder "FAIL" enthält.
- Wird ein Authorization-Reply mit Status "FAIL" empfangen, so wird die Fehlermeldung "Command not allowed for user 'xyz'" am Console-Prompt ausgegeben.

- Wird ein Authorization-Reply mit Status "PASS_ADD" empfangen, so wird der Befehl ausgeführt.
- Antwortet kein TACACS+ Authorisierungs-Server abhängig vom gesetzten Anfrage-Algorithmus (Timeout), so hängt das Verhalten vom eingestellten TACACS+ Authentication Mode für die entsprechende Console ab:

TACACS+ only:

Die Ausführung des Consolen-Befehls wird abgelehnt.

TACACS+ first, then local:

Die allgemeinen Zugriffsrechte, die bei der User-Authorisierung empfangen wurden, werden für die Authorisierung des Consolen-Befehls verwendet.

- Falls TACACS+ Accounting aktiviert ist und der Befehl ausgeführt wurde, sendet der Switch den Consolen-Befehl per TACACS+ Accounting-Request an den TACACS+ Accounting-Server.
- Der TACACS+ Accounting-Server trägt den ausgeführten Befehl in einer Log-Datei ein und antwortet mit einem TACACS+ Accounting-Reply, der den Status "Success" oder "Error" enthält.

Falls Console Command Authorization deaktiviert ist, werden die allgemeinen Zugriffsrechte, die bei der User-Authorisierung empfangen wurden, zur Authorisierung von Consolen-Befehlen verwendet.

10.65.1. TACACS+ Attribute zur Consolen-Befehls-Authorisierung

Folgende TACACS+ Attribute werden vom Switch an den TACACS+ Authorisierungs-Server zur Consolen-Befehls-Authorisierung gesendet:

Attribut	Attribut enthält ...
Auth Method	Anzuwendende Authorisierungsmethode: TACACSPLUS (0x06)
Privilege Level	Cisco Privilege Level 0...15 des Users, für den der Consolen-Befehl autorisiert werden soll (von Nexans Switchen nicht verwendet)
Authentication type	Zu verwendender Authentifizierungstyp. Der einzige aktuell unterstützte Typ ist: ASCII (1)
Service	Zu verwendendes Service-Protokoll. Das einzige aktuell unterstützte Protokoll ist: PPP (3)
User	User-Name
Port	Die TCP Port-Nummer, auf der der TACACS+ Authorisierungs-Server Authorization-Requests empfängt. Die offizielle Nummer ist 49.
Remote Address	Remote IP-Adresse des TACACS+ Authorisierungs-Servers
Arg[0...n] (AV-pairs):	service=shell → Shell-Authorisierung cmd=<command> → Befehl (Argument 0) cmd-arg=<command argument i> → Befehls-Argument i, i = 1...(n-1) cmd-arg=<cr> → Befehls-Terminator ("carriage return") Beispiel: show config tacacs+ → cmd=show, cmd-arg=config, cmd-arg=tacacs+, cmd-arg=<cr>

Folgende TACACS+ Attribute werden vom Switch zur Consolen-Befehls-Authorisierung gelesen:

Attribut	Attribut enthält ...
Auth Status	Der Status des Authorization-Requests: PASS_ADD (0x01) → Authorisierung erfolgreich FAIL (0x02) → Authorisierung fehlgeschlagen
Data	Daten für Authorisierung (nicht verwendet)

10.65.2. TACACS+ Attributes zum Consolen-Befehls-Accounting

Falls TACACS+ Accounting aktiviert ist, werden folgende TACACS+ Attribute vom Switch an den TACACS+ Accounting-Server zum Consolen-Befehls-Accounting gesendet:

Attribut	Attribut enthält ...
Auth Method	Anzuwendende Accounting-Methode: TACACSPLUS (0x06)
Privilege Level	Cisco Privilege Level 0...15 des Users, für den der ausgeführte Consolen-Befehl aufgezeichnet werden soll (von Nexans Switchen nicht verwendet)
Authentication type	Zu verwendender Authentifizierungstyp. Der einzige aktuell unterstützte Typ ist: ASCII (1)
Service	Zu verwendendes Service-Protokoll. Das einzige aktuell unterstützte Protokoll ist: PPP (3)
User	User-Name
Port	Die TCP Port-Nummer, auf der der TACACS+ Accounting-Server Accounting-Requests empfängt. Die offizielle Nummer ist 49.
Remote Address	Remote IP-Adresse des TACACS+ Accounting-Servers
Arg[0...3] (AV-pairs):	task_id=<id> → Task ID zur Identifikation der AAA-Aktion timezone=UTC → Zeitzone für Accounting-Eintrag in der Log-Datei (UTC) service=shell → Shell-Accounting cmd=<complete command> <cr> → Vollständiger Consolen-Befehl + Befehls-Terminator ("carriage return") Beispiel: show config tacacs+ → cmd=show config tacacs+ <cr>

Falls TACACS+ Accounting aktiviert ist, werden folgende TACACS+ Attribute werden vom Switch zum Consolen-Befehls-Accounting gelesen:

Attribut	Attribut enthält ...
Auth Status	Der Status des Accounting-Requests: Success (0x01) → Accounting erfolgreich Error (0x02) → Accounting fehlgeschlagen
Data	Daten für Accounting (nicht verwendet)

10.66. TACACS+ SCP Authentication Modes

Für SCP können im Switch sieben verschiedene Authentifizierungs-Modi eingestellt werden:

- Local: Lokale Authentifizierung
- Radius only: Authentifizierung ausschließlich durch den RADIUS Server
- Radius first, then local: Authentifizierung durch RADIUS, nur falls kein Server antwortet: lokale Authentifizierung
- TACACS+ only: Authentifizierung ausschließlich durch den TACACS+ Server
- TACACS+ first, then local: Authentifizierung durch TACACS+, nur falls kein Server antwortet: lokale Authentifizierung
- Use SSHv2 mode: Es wird der SSHv2 authentication mode benutzt
- Disabled: SCP Interface deaktiviert

Use SSHv2 mode (Factory-Default):

Local:

Disabled:

Siehe Kapitel [10.50 SCP Authentication Mode](#)

Radius only:**Radius first, then local:**

Siehe Kapitel [10.58 RADIUS SCP Authentication Modes](#)

TACACS+ Only:**TACACS+ first, then local:**

Der Ablauf der Authentifizierung bzw. Authorisierung ist prinzipiell identisch zur Consolen-Authentifizierung per TACACS+ Server (siehe Kapitel [10.64 TACACS+ Console Authentication Modes](#)).

10.67. TACACS+ Server-Konfiguration

Grundsätzlich kann ein Satz von TACACS+ Servern für Authentifizierung, Authorisierung und Accounting verwendet werden. Jedoch ist es möglich separate Server-Sätze für jeden AAA-Service zu konfigurieren.

Ein TACACS+ Server ist ein dedizierter *Linux*- oder *Windows*-PC, auf dem ein TACACS+ Service oder Dämon läuft.

10.67.1. TACACS+ Server für *Linux*

Für *Linux*-Maschinen wird der TACACS+ Dämon `tac_plus` Version F4-0.04.27a oder höher empfohlen.

Um den `tac_plus` Dämon auf *Linux*-Maschinen mit *Debian* / *Genome* Betriebssystem zu betreiben, muss das Paket `tacacs+` installiert werden:

```
sudo apt-get install tacacs+
```

Zur Konfiguration von AAA auf dem TACACS+ Dämon muss die Konfigurationsdatei `tac_plus.conf` ediert werden. Standardmäßig ist die Konfigurationsdatei des TACACS+ Dämons zu finden unter

```
/etc/tacacs+/tac_plus.conf
```

Für Details wird auf die Man Pages des Pakets `tac_plus` und der Konfigurationsdatei `tac_plus.conf` verwiesen.

Allerdings müssen Sie zur Aktivierung der User-Authentifizierung dafür sorgen, dass zumindest die TACACS+ Authorisierungs-Server-Konfiguration das *Nexans*-spezifische Attribut 'nx-access' im Abschnitt `exec` des Users oder der User-Gruppe, zu der der User gehört, vorsieht:

```
service = exec {
    priv-lvl = 0...15
    nx-access = {NX-ACCESS-RW | NX-ACCESS-R0}
}
```

Beispiel:

```
# 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 für Windows

Für *Windows*-Maschinen wird der TACACS+ Server `tacacs.net` Version v1.1.2 oder höher empfohlen.

Um `tacacs.net` auf *Windows*-Maschinen zu betreiben, muss das Paket `tacacs.net` installiert werden:

Diese SW kann von der Homepage www.tacacs.net/download heruntergeladen werden.

Zur Konfiguration von AAA in `tacacs.net` müssen die folgenden XML-Konfigurationsdateien editiert werden, die standardmäßig unter `C:\ProgramData\TACACS.net\config` zu finden sind:

- `tacplus.xml`
- `clients.xml`
- `authentication.xml`
- `authorizatiom.xml`

Für Details wird auf die Online-Dokumentation unter www.tacacs.net/documentation verwiesen.

Allerdings müssen Sie zur Aktivierung der User-Authentifizierung dafür sorgen, dass zumindest die TACACS+ Autorisierungs-Server-Konfiguration das *Nexans*-spezifische Attribut 'nx-access' im Abschnitt `<AutoExec>` des Users oder der User-Gruppe, zu der der User gehört, vorsieht (Konfigurationsdatei `authorizatiom.xml`):

```

<AutoExec>
  <Set>priv-lvl=15</Set>
  <Set>nx-access={NX-ACCESS-RW | NX-ACCESS-RO}</Set>
</AutoExec>

```

Beispiel:**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-user</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>
```

authorization.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-R0</Set>
    </AutoExec>
    <Shell>
      <Permit>.*show.*</Permit> <!--This will allow all show commands -->
      <Permit>.*ping.*</Permit>
    </Shell>
  </Authorization>
</Authorizations>
```

```
<Deny>.*</Deny>          <!--This will deny all other commands -->
</Shell>
</Authorization>
</Authorizations>
```

10.68. Access Control Lists (ACLs)

Access Control Lists (ACLs) bestehen aus einer Reihe von Regeln zur Steuerung des Netzwerkverkehrs. Durch einfache Regeln kann der Switch so konfiguriert werden, dass IP-Adressen, Protokolle, MAC-Adressen in bestimmten VLANs und / oder pro Schnittstelle zugelassen oder abgelehnt werden. Die Regeln haben Prioritäten, mit denen definiert werden kann, welche Regeln zuerst abgeglichen werden.

Bei HW5-Switchen können ACLs als *statische Access Control Lists (statische ACLs, SACLs)* auf dem Switch konfiguriert oder von einem RADIUS-Server als *dynamische Access Control Lists (dynamische ACLs, DACLs)* gesendet werden.

Nexans-Switches unterstützen 200 Regeln, die in 64 ACLs zusammengefasst werden können.

Jede Schnittstelle unterstützt mehrere ACLs und jede Regel kann mehreren ACLs zugewiesen werden.

Wenn der Benutzer widersprüchliche oder überlappende Regeln definiert hat, hängt das Übereinstimmungsergebnis und die entsprechende Aktion von der Priorität der Regel ab.

10.68.1. ACL Allgemeine Konfigurationsschritte

Grundsätzlich müssen folgende Schritte ausgeführt werden, um eine ACL auf einen Port anzuwenden:

1. ACL für den Port erstellen
2. Regeln erstellen, die für die ACL gelten
3. Regeln zur ACL hinzufügen
4. ACL zum Port (Interface) hinzufügen

Zu diesem Zweck werden Konsolen-Befehle definiert, die in den folgenden Kapiteln näher beschrieben werden.

Der NEXMAN bietet auf der Registerkarte "Access Control List Commands" ein Bearbeitungsfeld "Access Control List", in dem Sie die entsprechenden Konsolen-Befehle in der richtigen Reihenfolge eingeben können.

10.68.2. ACL Globale Einstellungen

Um ACL für einen Port verwenden zu können, muss ACL global aktiviert sein. *Statische* und *dynamische ACLs* können unabhängig voneinander aktiviert oder deaktiviert werden:

```
acl {dynamic|static} {enable|disable}
```

Um alle statischen ACLs oder gespeicherten dynamischen ACLs vom RADIUS-Server zu löschen, muss der folgende Befehl eingegeben werden:

```
acl {dynamic|static} clear
```

HINWEIS:

Jeder Manipulations-Befehl für statische ACLs und dynamische ACLs muss mit dem Befehl `renew` bestätigt werden.

10.68.3. ACL Regel-Definition

Nexans-Switches unterstützen IPv4-, IPv6- und MAC-basierte Regeln. Die Regeln sind in einer bestimmten Reihenfolge sortiert. Die Reihenfolge wird durch die Priorität der Regel festgelegt. Wenn ein Paket mit einer Regel übereinstimmt, stoppt das Gerät den Übereinstimmungsprozess und führt die in der Regel definierte Ablehnungs- oder Zulassungsaktion aus.

Die Regeldefinitionen bestehen aus den folgenden Attributen, wobei jeder nicht verwendete Parameter außer 'Aktion' durch das Schlüsselwort `any` ersetzt werden kann:

Attribut	Standard-Wert	Funktion
priority number	any	Die Priorität der Regel. Je niedriger die Prioritätsnummer, desto höher ist die Priorität der Regel. Gültige Werte sind: any 1...200
VLAN	any	Das VLAN, für das die Regel gilt. Gültige Werte sind: any 1...4094
action	permit	Die von der Regel definierte Aktion: permit deny
IPv4 / IPv6 protocol	any	Für IPv4 / IPv6-Layer-3-Regeln: Das IPv4- oder IPv6-Protokoll, für das die Regel gilt. Gültige Werte sind: any TCP UDP 1...YYY, wobei YYY die von IANA in RFC 790 definierte Protokollnummer ist.
source IP address	any	Für IPv4-Layer-3-Regeln: Die Source-IPv4-Adresse, für die die Regel gilt.
source port number	any	Für IPv4-Layer-3-Regeln: Die Source-Portnummer, für die die Regel gilt.
destination IP address	any	Für IPv4 / IPv6-Layer-3-Regeln: Die Destination-IPv4- oder IPv6-Adresse, für die die Regel gilt.
destination port number	any	Für IPv4 / IPv6-Layer-3-Regeln: Die Destination-Portnummer, für die die Regel gilt.
MAC ethertype	any	Für MAC-Layer-2-Regeln: Der MAC EtherType, für den die Regel gilt. Gültige Werte sind: any 1...YYY, wobei YYY der von IANA in RFC 7042 definierte EtherType ist.
source MAC address	any	Für MAC-Layer-2-Regeln: Die Source-MAC-Adresse, für die die Regel gilt.
destination MAC address	any	Für MAC-Layer-2-Regeln: The Destination-MAC-Adresse, für die die Regel gilt.

10.68.3.1. IPv4 / IPv6-Layer-3-Regel erstellen

Basierend auf den Source- und / oder Destination-IP-Adressen und -Protokollen unterstützen *Nexans*-Switche das Filtern von Layer-3-Verkehr. Dazu muss eine der nachfolgend beschriebenen IPv4 / IPv6-Layer-3-Regeln erstellt werden.

IPv4-TCP/UDP-Layer-3-Regeln erstellen

Für TCP/UDP-IPv4-Layer-3-Verkehr müssen Source- und Destination-IPv4-Adressen sowie Source- und Destination-Portnummern von TCP/UDP-Protokollen definiert werden. Dazu muss folgender Befehl verwendet werden:

```
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)}
```

Andere IPv4-Layer 3-Regeln erstellen

Zum Filtern von Nicht-TCP/UDP-IPv4-Layer-3-Verkehr wird die von IANA definierte IP-Protokollnummer verwendet. Die Liste der IP-Protokollnummern finden Sie in RFC 790. Der zugehörige Befehl lautet:

```
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)]}
```

Um den vollständigen IPv4-Datenverkehr abzudecken, müssen Sie den folgenden Befehl verwenden:

```
rule create (1...200) vlan {(1...4095)|any} {permit|deny} ipv4 any
```

IPv6-TCP/UDP-Layer-3 Regeln erstellen

Für TCP/UDP-IPv6-Layer-3-Verkehr können die Destination-IPv6-Adresse und die Destination-Portnummer von TCP/UDP-Protokollen definiert werden. Dazu muss folgender Befehl verwendet werden:

```
rule create (1...200) vlan {(1...4095)|any} {permit|deny} ipv6 protocol {tcp |  
udp} destination {any | <ipv6-addr>[/ (1...128)]} port {any | (1...YYY)}
```

Andere IPv6-Layer-3-Regeln erstellen

Zum Filtern von Nicht-TCP/UDP-IPv6-Layer-3-Verkehr wird die von IANA definierte IP-Protokollnummer verwendet. Die Liste der IP-Protokollnummern finden Sie in RFC 790. Der zugehörige Befehl lautet:

```
rule create (1...200) vlan {(1...4095)|any} {permit|deny} ipv6 protocol {any |  
(1...YYY) } destination {any | <ipv6-addr>[/ (1...128)]}
```

Um den vollständigen IPv6-Datenverkehr abzudecken, müssen Sie den folgenden Befehl verwenden:

```
rule create (1...200) vlan {(1...4095)|any} {permit|deny} ipv6 any
```

10.68.3.2. MAC-Layer-2 Regel erstellen

Zum Filtern von MAC-Layer-2-Verkehr werden die Source- und Destination-MAC-Adressen sowie die von IANA definierte EtherType-Nummer verwendet. Die Liste der EtherType-Nummern finden Sie in RFC 7042. Der zugehörige Befehl lautet:

```
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)]}
```

Um den vollständigen MAC-Layer-2-Datenverkehr abzudecken, müssen Sie den folgenden Befehl verwenden:

```
rule create (1...200) vlan {(1...4095)|any} {permit|deny} mac any
```

10.68.3.3. Regel löschen

Jede Regel kann mit dem folgenden Befehl anhand ihrer Prioritätsnummer gelöscht werden:

```
rule delete (1...200)
```

10.68.3.4. Regel überschreiben

Beim Erstellen einer Regel wird die vorhandene Regel mit derselben Prioritätsnummer überschrieben und die Zuweisungen der Regel zu ACLs werden entfernt.

10.68.4. ACL-Definition

Eine ACL wird durch ihren eindeutigen Namen definiert. Die Konfiguration einer ACL besteht aus einer Folge von Regeln, die der ACL zugewiesen sind. ACLs können Ports zugewiesen oder von Ports entfernt werden.

10.68.4.1. ACL erstellen

Zum Erstellen einer ACL muss der folgende Befehl verwendet werden:

```
acl create [<string max. 64 chars>] (max. 64 ACLs allowed)
```

10.68.4.2. ACL löschen

Zum Löschen einer ACL muss der folgende Befehl verwendet werden:

```
acl delete [<string max. 64 chars>] (max. 64 ACLs allowed)
```

10.68.4.3. Regel zu ACL hinzufügen

Um einer ACL eine Regel hinzuzufügen, muss der folgende Befehl verwendet werden:

```
acl a:dd [<string max. 64 chars>] r:ule (1..200)
```

10.68.4.4. Regel von ACL entfernen

Um eine Regel aus einer ACL zu entfernen, muss der folgende Befehl verwendet werden:

```
acl remove [<string max. 64 chars>] rule (1..200)
```

10.68.5. ACL-Zuweisung zu Interfaces

ACLs können einer oder mehreren Interfaces zugewiesen werden. Zu diesem Zweck wird die ACL zu den entsprechenden Interfaces hinzugefügt, indem auf ihren eindeutigen Namen verwiesen wird.

10.68.5.1. ACL zu Interface hinzufügen

Um einem Interface eine ACL hinzuzufügen, muss der folgende Befehl verwendet werden:

```
interface {if-no range} acl add [<string max. 64 chars>]
```

10.68.5.2. ACL von Interface entfernen

Um eine ACL von einem Interface zu entfernen, muss der folgende Befehl verwendet werden:

```
interface {if-no range} acl remove [<string max. 64 chars>]
```

10.68.6. Statische ACLs

Statische ACLs werden statisch in der ACL-Konfiguration definiert und den Port zugewiesen.

Es gibt zwei Befehle, um die Static ACLs anzuzeigen:

```
show acl static
```

oder

```
show conf acl
```

10.68.7. Dynamische ACLs

Nexans-Switches unterstützen *dynamische* oder *Downloadable ACLs*. Der RADIUS-Server kann sie mit dem Attribut *Accept Command NAS-Filter-Rule* (RFC-4849) senden. Da der Port mit dem angeschlossenen Gerät dem RADIUS-Server nicht unbedingt bekannt ist, besteht die Möglichkeit, den angeschlossenen Port implizit ACLs zuzuweisen.

```
interface dacl [<ACL string max. 64 chars>]
```

Der Switch unterstützt gleichzeitig statische und dynamische ACLs. Um das Überlappen von Regeln zu vermeiden, die zu statischen und dynamischen ACLs gehören, entfernt der Switch die Zuweisung von Ports zu statischen ACLs an den Ports, an denen die erfolgreiche 802.1x- oder MAC-Authentifizierung mit dynamischen ACLs stattgefunden hat. Beim Entfernen des authentifizierten Geräts werden auch die für das Gerät gespeicherten dynamischen ACLs entfernt.

Um dynamische ACLs anzuzeigen, die vom RADIUS-Server empfangen wurden, muss der folgende Befehl verwendet werden:

```
show acl dynamic
```

Beispiel:

```
# 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. Aktive ACLs

Die *aktiven ACLs* sind die resultierenden statischen und dynamischen ACLs, wenn die dynamischen ACLs auf die jeweiligen Ports angewendet werden.

Nach dem Empfang Dynamischer ACLs vom RADIUS-Server führt der Switch die folgenden Schritte aus, um die aktiven ACLs abzurufen:

- Erstellen der statische ACL-Konfiguration.
- Entfernen der Ports aus der Konfiguration, an denen eine erfolgreiche 802.1x- oder MAC-Authentifizierung stattgefunden hat und der RADIUS-Server die NAS-Filterregeln mit dynamischer ACL gesendet hat.
- Verarbeiten der dynamischen ACLs und die Ergebnisse sind die aktiven ACLs.

Um die aktiven ACLs anzuzeigen, muss der folgende Befehl verwendet werden:

```
show acl active
```

10.68.9. ACL-Status

Um die Zuweisungen von ACLs zu Ports anzuzeigen, muss der folgende Befehl verwendet werden:

```
show acl status
```

Beispiel:

```
# 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-Strategien

Es gibt zwei allgemeine Strategien für die Filterung von Datenverkehr. Die erste Strategie besteht darin, den gesamten Datenverkehr zuzulassen und mit der ACL bestimmten Netzwerkverkehr zu verbieten. Standardmäßig lässt der Switch alle Pakete durch die Switch-Engine. Bei dieser Strategie muss der Administrator bestimmten Datenverkehr mit Verweigerungsregeln sperren. Um beispielsweise den TCP-IPv6-Verkehr zu sperren, müssen Sie die folgende ACL festlegen:

Beispiel:

Der gesamte Datenverkehr soll zugelassen und nur der TCP-IPv6-Datenverkehr auf Port 5 gesperrt werden:

```
#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
```

Die andere Strategie, die mehr Sicherheit bietet, besteht darin, bestimmten Datenverkehr zuzulassen und alle anderen Pakete zu verbieten. Auf Nexans-Switchen müssen Sie explizit IPv4-, IPv6- und Ethertype-

Datenverkehr sperren. Die entsprechenden Regeln müssen die niedrigste Priorität haben und die ACL-Tabelle vervollständigen.

Beispiel:

An den Ports 6, 7, 8 und 9 sollen nur IPv4-ICMP-Pakete zugelassen und anderer Datenverkehr gesperrt werden:

```
#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-Beispiele

10.68.11.1. SSH-Verkehr blockieren

Erstellen Sie eine statische ACL, um den SSH-Verkehr von der IP-Adresse 192.168.0.3 an Port 6 mit Priorität 5 zu blockieren:

```
#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. ICMP-Verkehr zulassen

Erstellen Sie eine statische ACL, um ICMP-Verkehr an Port 9 mit Priorität 6 zuzulassen (das ICMP-Protokoll hat 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. Dynamische ACL-Konfiguration auf RADIUS-Server (*Freeradius*)

Auf dem RADIUS-Server *Freeradius* für *Linux* wird die Benutzer-Konfiguration normalerweise in der Konfigurationsdatei `/etc/freeradius/users` gespeichert. Um den *Freeradius*-Server so zu konfigurieren, dass NAS-Filterregeln mit dynamischen ACLs von *Nexans* gesendet werden, können Sie den Befehl für die Zuweisung eines impliziten dynamischen ACL-Ports oder für die Zuweisung eines expliziten Ports verwenden:

```
#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)

Das Internet Group Management Protocol (IGMP) ist ein Netzwerkprotokoll der Internetprotokollfamilie und dient zur Organisation von Multicast-Gruppen. Es basiert auf dem Internet Protocol (IP) und ermöglicht IP-Multicasting (Gruppenkommunikation). IP-Multicasting ist die Verteilung von IP-Paketen unter einer IP-Adresse an mehrere Stationen gleichzeitig. IGMP bietet die Möglichkeit, dynamisch Gruppen zu verwalten. Die Verwaltung findet nicht in der Sende-Station statt, sondern in Routern oder Switches, an denen Empfänger einer Multicast-Gruppe direkt angeschlossen sind. IGMP bietet Funktionen, mit denen eine Station einem Router mitteilt, dass sie Multicast-IP-Pakete einer bestimmten Multicast-Gruppe empfangen will. Der Sender von Multicast-IP-Paketen weiß dabei nicht, welche und wie viele Stationen seine Pakete empfangen, denn er verschickt nur ein einziges Datenpaket für alle Empfänger an seinen übergeordneten Router. Der dupliziert das IP-Paket bei Bedarf, wenn er mehrere ausgehende Schnittstellen mit Empfängern hat.

Mittels IGMP Snooping kann verhindert werden, dass Multicast-Traffic an alle Switchports geflutet wird. So wird die Netzlast reduziert.

10.69.1. IGMP Snooping

Bei eingeschaltetem IGMP Snooping, belauscht der Switch (to snoop, schnüffeln) den IGMP-Traffic an seinen Ports. Nur Ports, die einer Multicast-Gruppe beigetreten sind (per Membership-Report bzw. Join-Group), werden in die Forwarding-Table für diese Multicast-Adresse eingetragen. Ports die die Gruppe verlassen (per Leave-Group), werden aus der Tabelle gelöscht. Ferner werden solche Gruppen gelöscht, für die über eine bestimmte Zeit kein Membership-Report empfangen wurde.

Weiterhin lauscht der Switch, am welchem Port der IGMP Querier angeschlossen ist.

Über den Button "Show IGMP State" im NEXMAN bzw. über das Konsole Kommando "show igmp status" kann der aktive Querier und die IGMP Forwarding Table angezeigt werden:

IGMP State					
Querier IP	Port	Type	Timer		
192.168.0.10	4	dynamic	00054		
Multicast IP	Multicast MAC	Joined Ports	Type	Timer	
239.255.255.250	01:00:5e:7f:ff:fa	2,3,4	dynamic	00056	
224.0.0.2	01:00:5e:00:00:02	3,4	dynamic	00056	
224.0.0.22	01:00:5e:00:00:16	3,4	dynamic	00054	

Die folgende Tabelle zeigt eine Übersicht aller IGMP Snooping Einstellungen:

Bez. im NEXMAN	Default Wert	Funktion
IGMP Snooping enable	disabled	Wenn ausgewählt, wird die IGMP Snooping Funktion aktiviert

Snoop Table Ageing Time (seconds)	60	Eine Gruppe wird gelöscht, wenn für die hier konfigurierte Zeit kein Membership-Report für diese Gruppe empfangen wurde.
Accept IGMP Version 1	disabled	Wenn ausgewählt, werden IGMP-V1 Pakete akzeptiert und ausgewertet. Falls deaktiviert, werden diese ignoriert.
Accept IGMP Version 2	enabled	Wenn ausgewählt, werden IGMP-V2 Pakete akzeptiert und ausgewertet. Falls deaktiviert, werden diese ignoriert.
Accept MLD Version 1	disabled	Wenn ausgewählt, werden MLD-V1 Pakete akzeptiert und ausgewertet. Falls deaktiviert, werden diese ignoriert.
Accept MLD Version 2	disabled	Wenn ausgewählt, werden MLD-V2 Pakete akzeptiert und ausgewertet. Falls deaktiviert, werden diese ignoriert.
IGMP Immediate Leave Mode	Accept vom User Ports only	Dieser Parameter bestimmt die Behandlung von "IGMP Immediate Leave Messages". Durch das Senden dieser IGMP Message kann ein angeschlossenes Endgerät das sofortige Verlassen einer Multicast-Gruppe anfordern. Unabhängig von der Möglichkeit des Immediate Leave, werden Ports automatisch nach Ablauf der obigen "Snoop Table Ageing Time" aus der Multicast-Gruppe gelöscht. Folgende Einstellungen sind möglich: • Accept Leave messages from User Ports only • Accept all Leave messages • Ignore all Leave messages Accept Leave messages from User Ports only: Dies ist die Werkseinstellung und akzeptiert ausschließlich Leave Messages, die von User Ports empfangen werden. Über die Einstellung 'Link type' kann definiert werden, welche Ports User Ports bzw. Uplink Ports sind. Falls Spanning Tree aktiviert ist, werden Leave Messages ausschließlich von Edge-Ports akzeptiert. Insbesondere bei einer Ring-Topologie, ist diese Einstellung für einen störungsfreien Betrieb zwingend erforderlich. Accept all Leave messages: Leave Messages werden grundsätzlich von jedem Port akzeptiert. Ignore all Leave messages: Leave Messages werden grundsätzlich ignoriert.

10.69.2. IGMP Querier

Bei eingeschaltetem IGMP Querier sendet der Switch IGMP-V1/V2 Query Pakete auf allen Ports. Daraufhin müssen alle angeschlossenen Endgeräte, die einer Gruppe beigetreten sind einen neuen Membership-Report senden. Anhand der Membership-Reports, kann dann die IGMP-Snooping Funktion ihre Forwarding Tabelle auffrischen.

In der entsprechenden RFC ist festgelegt, dass es pro Segment nur einen einzigen aktiven Querier geben darf. Sind im selben Segment mehrere Querier auf verschiedenen Switchen eingeschaltet, so darf nur derjenige mit der niedrigsten IP Adresse weitersenden. Alle anderen Querier müssen sich zurückziehen.

Sofern der aktuelle Nexans Switch gerade als aktiver Querier arbeitet, wird dies im IGMP Status durch den Typ 'local' angezeigt:

IGMP State					
Querier IP	Port	Type	Timer		
192.168.0.10	n/a	local	00020		
Multicast IP	Multicast MAC	Joined Ports	Type	Timer	
239.255.255.250	01:00:5e:7f:ff:fa	2,4,5	dynamic	00060	
224.0.0.2	01:00:5e:00:00:02	2,5	dynamic	00042	
224.0.0.22	01:00:5e:00:00:16	2,5	dynamic	00042	

HINWEIS:

Die Funktion des Queries wird in einem Netzwerk sinnvollerweise vom Core-Switch ausgeführt. Die Querier Funktion auf den Nexans Switches sollte nur dann aktiviert werden, wenn es sich um ein isoliertes Segment handelt (z.B. bei Maschinensteuerungen per Ethernet/IP Protokoll) und kein Core Switch vorhanden ist.

Die folgende Tabelle zeigt eine Übersicht aller IGMP Querier Einstellungen:

Bez. im NEXMAN	Default Wert	Funktion
IGMP Querier enable	disabled	Wenn ausgewählt, wird die IGMP Querier Funktion aktiviert
Query Interval (seconds)	20	Das Interval für das Versenden von IGMP Query Paketen

10.70. Link Layer Discovery Protocol (LLDP)

Das LLDP (Link Layer Discovery Protocol) ist ein herstellerunabhängiges Layer 2 Protokoll, das nach der IEEE-802.1AB-Norm definiert ist und die Möglichkeit bietet, Informationen zwischen Nachbargeräten auszutauschen.

Auf jedem Gerät, das LLDP unterstützt, arbeitet eine Softwarekomponente, der sogenannte LLDP-Agent, der in periodischen Abständen Informationen über sich selbst versendet und ständig Informationen von Nachbargeräten empfängt. Dies geschieht völlig unabhängig voneinander und deshalb wird das LLDP ein „Ein-Weg-Protokoll“ genannt, das keine Kommunikation zu anderen Geräten aufbaut.

Die folgende Tabelle zeigt eine Übersicht der LLDP Einstellungen:

Bez. im NEXMAN	Default Wert	Funktion
LLDP Mode	Disabled	Hier kann aus zwei verschiedenen Modi ausgewählt werden: • Disabled without LLDP filter Es werden keine LLDP Pakete gesendet, jedoch ist der Switch für LLDP Pakete transparent. Dies bedeutet, dass empfangene LLDP Pakete innerhalb des selben VLANs unverändert weitergeleitet werden. • Disabled with LLDP filter Es werden keine LLDP Pakete gesendet. Zusätzlich filtert der Switch empfangene LLDP Pakete, so dass keine LLDP Pakete auf andere Ports weitergeleitet werden. • Enabled Entsprechend den Parametern „TX Message Intervall „ und „TX Holdtime“ werden auf allen Ports LLDP Pakete gesendet. • Enabled with LLDP forwarding to Uplink Ergänzend zur Einstellung 'Enabled', werden hier LLDP Pakete von angeschlossenen Endgeräten (z.B. IP-Phones) zum Uplink weitergeleitet. Dies bedeutet, dass man am Coreswitch sowohl den Nexans Switch als auch alle daran angeschlossenen LLDP-fähigen Geräte in der Neighbor Table sieht. WICHTIG: Damit die Weiterleitung korrekt arbeitet, muss der

		'LinkTyp' für alle Ports entsprechend eingestellt werden. LLDP Pakete, die auf einem 'User-Port' empfangen werden, werden ausschließlich an 'Uplink/Downlink' Ports weitergeleitet.
TX Message Intervall (seconds)	30	Das Zeit-Intervall für das Versenden von LLDP Paketen
TX Holdtime Multiplier	4	Der 'TX Holdtime Multiplier' multipliziert mit dem obigen 'TX Message Intervall' ergibt die Lifetime des Paketes in der Empfangsstation.

Folgende LLDP Attribute werden vom Switch gesendet:

Attribut	Attribut enthält ...
Chassis ID TLV	MAC Adresse des Switches
Port ID TLV	Port Description (z.B. 'TP-1')
Time To Live TLV	TX Message Intervall * TX Holdtime Multiplier
Port Description TLV	Port Description (z.B. 'TP-1')
System Name TLV	Benutzerdefinierter Switch Name
System Description TLV	Device Description und Software Version
System Capabilities TLV	Bridge
Management Address TLV	IP Adresse
Port VLAN ID TLV	Default VLAN (Untagged)
Power Via MDI TLV	Power-over-Ethernet Leistungskennwerte, falls PoE für den betreffenden Port eingeschaltet ist.

10.71. LLDP for Media Endpoint Devices (LLDP-MED)

LLDP-MED ist eine Erweiterung des LLDP Standard gemäß ANSI Standard TIA-1057. Es wurde speziell dafür entwickelt um Informationen zwischen Endgeräten und Switches auszutauschen.

In Installationen bei denen LLDP-MED fähige IP-Phones zum Einsatz kommen, kann per LLDP-MED das Voice-VLAN, sowie die Layer 2 und Layer 3 priority values an das IP-Phone übermittelt werden. Hier wird die am jeweiligen Port des Nexans Switches konfigurierte Voice-VLAN-ID herangezogen. Die Layer 2 und Layer 3 Priority Values können für den Application Type Voice und Voice Signaling separat konfiguriert werden. Somit ist eine automatische Konfiguration des IP-Phones per LLDP-MED möglich.

Auch wenn LLDP per 'LLDP-Mode' aktiviert ist, werden die unten aufgeführten LLDP-MED TLVs nur dann in die gesendeten LLDP Pakete aufgenommen, wenn an dem betreffenden Port LLDP Pakete mit LLDP-MED TLVs vom Endgerät (z.B. IP-Phone) empfangen werden. Nach einem Link Down oder nach längerem Empfang keiner LLDP-MED TLVs, wird das Senden der LLDP-MED TLVs wieder deaktiviert.

Folgende LLDP-MED Attribute werden vom Switch gesendet:

TLV Typ	TLV enthält ...
LLDP-MED Capabilities TLV	Devicetyp und unterstützte TLV Typen
Network Policy TLV	Voice VLAN ID Layer 2 priority value Layer 3 DSCP value
Extended Power Via MDI TLV	PoE-Typ des Switches und PoE-Leistung in Watt, die der Switch dem angeschlossenen Endgerät zur Verfügung stellen kann.
Location Identification TLV	Einbauort des Switches

Folgende LLDP-MED Attribute werden vom Switch ausgewertet:

TLV Typ	TLV enthält ...
Network Policy TLV	Typ des angeforderten Netzwerk-Services, z.B. Voice.
Extended Power Via MDI TLV	PoE-Typ des angeschlossenen Endgerätes und angeforderte Leistung in Watt.
Inventory TLV	Die folgenden Inventory TLVs werden unterstützt: HW-Revision FW-Revision SW-Revision Serial-Number Manufacturer-Name Modell-Name

Die folgende Tabelle zeigt eine Übersicht der LLDP MED Einstellungen der Network Policy TLVs:

Bez. im NEXMAN	Default Wert	Funktion
Layer 2 priority value Voice	0	Layer 2 priority value der in der Network Policy Voice (TIA-1057) gesendet wird.
Layer 3 DSCP value Voice	0	Layer 3 DSCP value der in der Network Policy Voice (TIA-1057) gesendet wird.
Layer 2 priority value Voice Signaling	0	Layer 2 priority value der in der Network Policy Voice Signaling (TIA-1057) gesendet wird.
Layer 3 DSCP value Voice Signaling	0	Layer 3 DSCP value der in der Network Policy Voice Signaling (TIA-1057) gesendet wird.

Die folgende Tabelle zeigt eine Übersicht der LLDP MED Einstellungen der Location Identification TLVs:

Bez. im NEXMAN	Default Wert	Funktion
Building (25)	<leer>	Der Name eines einzelnen Gebäudes oder einer Struktur
Unit (26)	<leer>	Der Name oder die Nummer eines Teils eines Gebäudes oder einer Struktur
Place Type (29)	<leer>	Die Art des Ortes, z.B. Zuhause, Büro, Straße oder ein anderer öffentlicher Raum.

10.72. Cisco Discovery Protocol (CDP)

Das CDP (Cisco Discovery Protocol) ist ein Layer 2 Protokoll, das die Möglichkeit bietet, Informationen zwischen Nachbargeräten auszutauschen.

Jede Nachricht enthält Informationen wie zum Beispiel den Gerätenamen, die Betriebssystemversion, Schnittstellenbezeichner, Management-IP-Adressen und die Holdtime des Paketes. Bleibt eine periodische Aktualisierung der Geräteinformationen aus, wird die alte Information nach Ablauf der Holdtime verworfen.

In Installationen bei denen Cisco IP-Phones zum Einsatz kommen, kann per CDP das Voice-VLAN an das IP-Phone übermittelt werden. Hier wird die am jeweiligen Port des Nexans Switches konfigurierte Voice-VLAN-ID herangezogen. Somit ist eine automatische Konfiguration des Cisco IP-Phones per CDP möglich. Weitere Informationen zur Konfiguration von Nexans Switches in einer Cisco Umgebung, können auf Anfrage bei Nexans angefordert werden (Stichwort 'Cisco Evaluierung').

Bei Switches mit installierter Power-over-Ethernet (PoE) Option wird ggf. die zur Verfügung stehende Leistung per CDP an das Endgerät übermittelt. Diese Funktion ist insbesondere für Cisco Access Point mit höherer Leistungsaufnahme relevant, da diese ohne die entsprechenden CDP Informationen nicht korrekt hochfahren. Die vom Endgerät per CDP angeforderte Leistung kann über die Funktion "Show Neighbor Details" angezeigt werden.

Wichtiger HINWEIS: Da CDP ein CISCO proprietäres Protokoll ist, kann grundsätzlich nicht die entsprechende CISCO Private CDP-MIB unterstützen werden. Stattdessen können die per CDP gesammelten Discovery Informationen über die Standard LLDP-MIB nach IEEE 802.1AB ausgelesen werden. Voraussetzung ist allerdings, dass der CDP Mode auf „Enabled with entry in LLDP-MIB“ eingestellt ist.

Die folgende Tabelle zeigt eine Übersicht der CDP Einstellungen:

Bez. im NEXMAN	Default Wert	Funktion
CDP Mode	Disabled	Hier kann aus drei verschiedenen Modi ausgewählt werden: • Disabled without CDP filter Es werden keine CDP Pakete gesendet, jedoch ist der Switch für CDP Pakete transparent. Dies bedeutet, dass empfangene CDP Pakete innerhalb desselben VLANs unverändert weitergeleitet werden. • Disabled with CDP filter Es werden keine CDP Pakete gesendet. Zusätzlich filtert der Switch empfangene CDP Pakete, so dass keine CDP Pakete auf andere Ports weitergeleitet werden. • Enabled Entsprechend den Parametern „TX Message Intervall“ und „TX Holdtime“ werden CDP Pakete auf allen Ports gesendet. WICHTIG: Trotz der Einstellung 'Enabled', wird das Senden von Paketen durch den Nexans Switch nur dann aktiviert, wenn von einem Nachbargerät (z.B. Cisco-Coreswitch) CDP Pakete empfangen werden. Dies verhindert, dass in einer Nicht-Cisco-Umgebung CDP Pakete ins Netz gesendet werden. • Enabled with CDP forwarding to Uplink Ergänzend zur Einstellung 'Enabled' werden hier CDP Pakete von evtl. angeschlossenen Endgeräten (z.B. IP-Phones) zum Uplink weitergeleitet. Dies bedeutet, dass man am Coreswitch sowohl den Nexans Switch als auch alle daran angeschlossenen CDP fähigen Geräte in der Neighbor Table sieht. WICHTIG: Damit die Weiterleitung korrekt arbeitet, muss der 'LinkTyp' für alle Ports entsprechend eingestellt werden. Pakete, die auf einem 'User-Port' empfangen werden, werden ausschließlich an 'Uplink/Downlink' Ports weitergeleitet. • Enabled with entry in LLDP-MIB Ergänzend zur Einstellung 'Enabled', können hier alle CDP Neighbor Einträge per LLDP-MIB abgefragt werden. Ist zusätzlich LLDP eingeschaltet, so enthält die LLDP-MIB sowohl LLDP als auch CDP Einträge. Die einzelnen Einträge in der lldpRemTable werden dabei wie folgt mit den CDP TLVs besetzt: lldpRemChassisIdSubtype(4) = Fester Wert: local(7) lldpRemChassisId(5) = CDP TLV: Device-ID lldpRemPortIdSubtype(6) = Fester Wert: 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) = Fester Wert: Bridge lldpRemSysCapEnabled(12) = Fester Wert: Bridge
TX Message Intervall (seconds)	60	Das Zeit-Intervall für das Versenden von CDP Paketen
TX Holdtime (seconds)	180	Die 'TX Holdtime' bestimmt die Lifetime des Paketes in der Empfangsstation.

10.73. Rapid Spanning Tree Protocol (RSTP)

Das Rapid Spanning Tree Protocol (RSTP) ist ein Netzwerkprotokoll, um redundante Pfade in lokalen Netzwerken zu deaktivieren, bzw. im Bedarfsfall (Ausfall einer Verbindung) wieder zu aktivieren.

10.73.1. RSTP - Allgemeine Funktionsweise

Netzwerke sollten zu jedem möglichen Ziel immer nur einen Pfad haben, um zu vermeiden, dass Datenpakete (Frames) dupliziert werden und mehrfach am Ziel eintreffen, was zu Fehlfunktionen in darüber liegenden Netzwerkschichten führen könnte und die Leistung des Netzwerks vermindern kann. Andererseits möchte man mitunter redundante Netzwerkpfade als Backup für den Fehlerfall zur Verfügung haben. Der Spanning Tree Algorithmus wird beiden Bedürfnissen gerecht.

Zur Kommunikation zwischen den Switches wird das Bridge Protokoll genutzt. Die Pakete dieses Protokolls werden Bridge Protocol Data Unit (BPDU) genannt.

Zunächst wird unter den Spanning Tree fähigen Switches im Netzwerk eine sogenannte Root Bridge gewählt, die der Mittelpunkt (Root) des aufzuspannenden Baumes wird. Dies geschieht, indem alle Switches ihre Bridge-ID an eine bestimmte Multicast-Adresse senden. Die Bridge ID ist 8 Byte lang (2 Bytes Bridge Priority und 6 Bytes MAC Adresse). Der Switch mit der niedrigsten ID wird zur Root Bridge. Sollte die Bridge Priority identisch sein, wird als ergänzendes Kriterium die MAC Adresse des Switches benutzt (und zwar der Switch mit der niedrigeren MAC Adresse). Von der Root Bridge aus werden nun Pfade festgelegt, über die die anderen Switches im Netzwerk erreichbar sind. Sind redundante Pfade vorhanden, so müssen die dortigen Switches den entsprechenden Port auf 'Blocking' schalten. Die Pfade, über die kommuniziert werden darf, werden anhand von Pfadkosten bestimmt, die der dortige Switch übermittelt. Die Kosten sind abhängig vom Abstand zur Root Bridge und dem zur Verfügung stehenden Uplink zum Ziel. Ein 10 Mbit/s-Uplink hat beispielsweise höhere Pfadkosten als ein 100 Mbit/s-Uplink zum gleichen Ziel und würde dabei unter den Tisch fallen. Auf diese Weise ist jedes Teilnetz im geschalteten LAN nur noch über eine einzige, die Designated Bridge erreichbar. Wenn man es grafisch darstellt, ergibt sich ein Baum aus Netzwerkpfaden, der dem Algorithmus seinen Namen gab.

Alle Switches teilen den in der Hierarchie eine Stufe unterhalb liegenden Switchen im Abstand der Hello Time (typisch 2 Sekunden) mit, dass sie noch da ist. Wenn diese Hello-Pakete ausbleiben, hat sich folglich an der Topologie des Netzwerks etwas geändert, und das Netzwerk muss sich reorganisieren. Diese Neuberechnung des Baumes dauerte beim alten Spanning Tree Protocol im schlimmsten Fall bis zu 50 Sekunden. Während dieser Zeit durften die Spanning Tree fähigen Switches außer Spanning Tree Informationen keine Pakete im Netzwerk weiterleiten. Dies war einer der größten Kritikpunkte am Spanning Tree Algorithmus, da es möglich ist, mit gefälschten Spanning Tree Paketen eine Topologieänderung zu signalisieren und das gesamte Netzwerk für bis zu 30 Sekunden Lahmzulegen. Um diesen potenziellen Sicherheitsmangel zu beheben, aber auch, um bei echten Topologieänderungen das Netzwerk schnell wieder in einen benutzbaren Zustand zu bringen, wurde das Rapid Spanning Tree Protocol (RSTP) normiert. Die Idee hinter RSTP ist, dass bei signalisierten Topologieänderungen nicht sofort die Netzwerkstruktur gelöscht wird, sondern erst einmal wie gehabt weiter gearbeitet wird und Alternativpfade berechnet werden. Erst anschließend wird ein neuer Baum zusammengestellt. Die Ausfallzeit des Netzwerks lässt sich so von 30 Sekunden auf Werte im Millisekundenbereich drücken. In der 2004 verabschiedeten Revision des 1998 letztmalig überarbeiteten 802.1D-Standards ist das alte STP zugunsten von RSTP komplett entfallen.

Die RSTP Implementation im Nexans Switch beruht auf diesem aktuellen Standard IEEE802.1D-2004, der einige Verbesserungen gegenüber der ersten RSTP Revision IEEE802.1w aufweist.

10.73.2. RSTP - Globale Konfigurationsparameter

Bez. im NEXMAN	Default Wert	Funktion
RSTP global enable	disable	Nur wenn hier das Spanning Tree Protocol global eingeschaltet ist, werden alle Ports, bei denen ebenfalls Spanning Tree eingeschaltet ist, in die Berechnung der Topologie einbezogen. Ferner werden bei globaler Aktivierung von Spanning Tree alle BPDU Pakete geblockt und ausschließlich an die CPU des Switches weitergeleitet. WICHTIG: Ist Spanning Tree hier global ausgeschaltet, verhält sich der Switch für BPDU Pakete transparent und empfangene BPDU Pakete werden auf alle Ports weitergeleitet.
Protocol version	STP and RSTP	Hier sind zwei Einstellungen möglich: • STP and RSTP Hier wird vorzugsweise das RSTP Protocol auf allen aktivierten Ports verwendet. Nur wenn auf einem Port STP Pakete empfangen werden, wird automatisch für diesen Port das alte STP Protocol verwendet. Allerdings gehen dann die Vorteile des RSTP, wie schnelle Umschaltzeiten, verloren. • STP compatible Auf allen aktivierten Ports wird ausschließlich das alte STP Protocol verwendet. Die Vorteile des RSTP, wie schnelle Umschaltzeiten, gehen dabei verloren.
Bridge priority	32768	Hier kann die Priorität des Switches zwischen 0 und 61440 (in Schritten von 4096) eingestellt werden. Der Switch, welcher die kleinste Priorität besitzt wird zur Root Bridge. Besitzen zwei Switche die gleiche Priorität, so wird der Switch zur Root, welcher die kleinste MAC-Adresse besitzt.
Hello time (seconds) (1...10)	2	Diese Einstellung hat zwei Funktionen: a) Zeit-Intervall für das Versenden von BPDU Paketen: Gibt das Zeit-Intervall an, innerhalb dessen alle RSTP Switche regelmäßig BPDU Pakete auf allen Designated Ports senden. Bei Verwendung des alten STP Protocols sendet eine Nicht-Root-Bridge nur dann ein BPDU Paket, wenn sie an Ihrem Root-Port BPDU ein Paket empfangen hat. b) Timeout bei RSTP Bei RSTP timen die Port-Zustände nach 3 x Hello time aus (typisch 3 x 2 = 6 Sekunden). WICHTIG: Gemäß IEEE802.1D Standard muss der Wert für 'Hello time' kleiner oder gleich sein als: ('Max. age/hops' ÷ 2) - 1 Wird ein zu großer Wert für 'Hello time' konfiguriert, so wird diese automatisch auf ('Max. age/hops' ÷ 2) - 1 korrigiert. HINWEIS: Diese Einstellung wird von der Root Bridge an alle anderen Switche verteilt und wird deshalb bei allen Nicht-Root-Bridges ignoriert.

Max. age/hops (6...50) Bis einschließlich V3.61: (6...40)	20	Diese Einstellung hat zwei Funktionen: a) Max. Anzahl Switche bei RSTP und STP: Die Root-Bridge versendet BPDU Pakete mit einem age/hops Wert von '0' im Abstand der Hello-Time. Jeder folgende Switch erhöht den age/hops Wert der empfangenen BPDU um eins und sendet seinerseits dann BPDU's mit dem neuen (erhöhten) age/hops Wert. Empfängt ein Switch eine BPDU, bei der age/hops größer ist als 'Max. age/hops', so wird die BPDU verworfen. b) Timeout bei STP: Bei Verwendung des alten STP Protocols timen die Port Zustände nach Ablauf von 'Max. age/hops' aus. HINWEIS: Beim RSTP timen die Port-Zustände bereits nach 3 x Hello time aus WICHTIG: Gemäß IEEE802.1D Standard muss der Wert für 'Max. age/hops' kleiner oder gleich sein als: $2 \times (\text{'Forward delay'} - 1)$ Wird ein zu großer Wert für 'Max. age/hops' konfiguriert, so wird dieser automatisch auf $2 \times (\text{'Forward delay'} - 1)$ korrigiert. HINWEIS: Diese Einstellung wird von der Root Bridge an alle anderen Switche verteilt und wird deshalb bei allen Nicht-Root-Bridges ignoriert.
Forward delay (seconds) (4...30)	15	Der Forward delay Wert gibt an, wie lange die Switches warten sollen, um den Zustand eines Ports von Blocking zu Learning und von Learning nach Forwarding zu wechseln (2 x Forward Delay). Sofern der Switch unter 'Protocol version' für RSTP konfiguriert ist, und auf dem Port und ein entsprechender Switch mit RSTP Paketen antwortet, erfolgt der Wechsel von Blocking nach Forwarding durch das RSTP Protocol (ohne den Forward delay abzuwarten). Ist ein Port als Edge-Port konfiguriert (PortFast), so wird der Forward delay ebenfalls umgangen und der Port unmittelbar nach einem Link-Up auf Forwarding geschaltet. HINWEIS: Diese Einstellung wird von der Root Bridge an alle anderen Switches verteilt und wird deshalb bei allen Nicht-Root-Bridges ignoriert.
Transmit hold count (1...10)	6	Bestimmt die maximale Anzahl von BPDU Paketen die pro Sekunde und pro Port gesendet werden dürfen. Diese Funktion dient zum Schutz vor einer Überflutung des Netzes mit BPDU Paketen im Fehlerfall.
Re-enable time for BPDU-Disabled ports (seconds)	0	Ports, die aufgrund einer empfangenen BPDU abgeschaltet wurden, können optional nach 1 bis 60000 Sekunden automatisch wieder aktiviert werden. Ist die Zeit auf 0 konfiguriert, so muss der Port manuell reaktiviert werden.
Debugging mode	Disable	Wird der Debugging Mode eingeschaltet, so werden detaillierte Informationen zu Spanning Tree Zustandsänderungen in das lokale Logbuch geschrieben. WICHTIG: Diese Funktion sollte nur nach Rücksprache mit dem Herstellersupport aktiviert.

10.73.3. RSTP - Port Konfigurationsparameter

Bez. im NEXMAN	Default Wert	Funktion
Spanning Tree mode	Enabled	Nur wenn RSTP für den betreffenden Port aktiviert ist, wird dieser in die Berechnung der Topologie einbezogen. Ports, bei denen Spanning Tree disabled ist, senden grundsätzlich keine BPDU Pakete und empfangene BPDU Pakete werden ignoriert und nicht auf andere Ports weitergeleitet. Hinweis zu CISCO PVST+ Paketen: Ports, für die Spanning Tree disabled ist, blocken zusätzlich ausgehende PVST+ Pakete. Eingehende PVST+ Pakete werden dagegen nicht geblockt und an alle Ports im selben VLAN weitergeleitet, für die Spanning Tree enabled ist. Möchte man verhindern, dass PVST+ Pakete empfangen und weitergeleitet werden, so ist für den betreffenden Port der Spanning Tree Mode auf „Disabled (BPDU disables Port)“ einzustellen. In diesem Fall wird der Port abgeschaltet sobald eine Spanning Tree Paket empfangen wird. Hier kann aus drei verschiedenen Modi ausgewählt werden: • Enabled Der Port sendet und empfängt BPDU Pakete und wird in die Berechnung der Topologie einbezogen. • Enabled (Ring Loop Protection) Wie Mode „Enabled“, jedoch wird zusätzlich eine periodische Prüfung vorgenommen, ob eine Ring-Loop existiert. Diese Sicherheitsfunktion verhindert, dass Aufgrund eines Fehlers in der Berechnung der Spanning Tree Topology eine Loop im Ring geschaltet wird. WICHTIG: Diese Funktion sollte nur für Ring Topologien eingesetzt werden und darf nur auf einem einzigen Switch im Ring und einem Ring Port aktiviert werden. Wird eine Ring-Loop erkannt, so führt dies zu einer Abschaltung des Ports mit aktivierter „Ring Loop Protection“. Als Link Status des betreffenden Ports wird in diesem Fall "RING-LOOP-DISABLED" angezeigt und ein "Port Error Disable" Alarm versendet. Abgeschaltete Ports müssen manuell wieder aktiviert werden. • Disabled (BPDU filter) Der Port sendet keine BPDU Pakete und empfangene BPDU Pakete ignoriert. • Disabled (BPDU disables Port) Der Port sendet keine BPDU Pakete und empfangene BPDU Pakete führen zu einer Abschaltung des Ports. Als Link Status des betreffenden Ports wird in diesem Fall "BPDU-DISABLED" angezeigt und ein "Port Error Disable" Alarm versendet. Abgeschaltete Ports können optional nach einer einstellbaren "Re-Enable Time for BPDU-Disabled Ports" automatisch wieder aktiviert werden. Die Zeit ist dabei im Bereich von 1 bis 60000 Sekunden konfigurierbar. WICHTIG: Ist Spanning Tree global ausgeschaltet, verhält sich der Switch für BPDU Pakete transparent und empfangene BPDU Pakete werden auf alle Ports desselben VLANs weitergeleitet.

Priority	128	Hier kann die Priorität des Ports zwischen 0 und 240 (in Schritten von 16) eingestellt werden. Die Portpriorität (4 Bit) und die Portnummer (12 Bit) bilden zusammen die Port ID. Beim Vergleich zweier Port IDs ist diejenige die höhere 'bessere' Priorität, deren numerischer Wert niedriger ist. Die übliche Schreibweise für die Port ID lautet: Port-Priority / Port-Nummer
Path cost mode	Auto (RSTP)	Über diesen Parameter kann bestimmt werden, wie die Pfadkosten des Ports ermittelt werden. Hier kann aus drei verschiedenen Modi ausgewählt werden: • Auto (RSTP) Hier werden die Pfadkosten automatisch anhand der tatsächlichen Geschwindigkeit des Ports ermittelt. Dabei werden jeweils die in der Norm IEEE802.1D-2004 vorgeschlagenen Standardwerte eingesetzt: 10 Mbits/s = 2.000.000 100 Mbits/s = 200.000 1 Gbits/s = 20.000 10 Gbits/s = 2.000 • Auto (STP) Auch hier werden die Pfadkosten anhand der tatsächlichen Geschwindigkeit des Ports ermittelt, allerdings werden dabei die Standardwerte aus der alten STP Norm eingesetzt: 10 Mbits/s = 100 100 Mbits/s = 19 1 Gbits/s = 4 10 Gbits/s = 2 • Manual Bei Auswahl dieser Option können die gewünschten Pfadkosten manuell vorgegeben werden (siehe Parameter 'Manual path cost'). Die Geschwindigkeit des Ports ist in diesem Fall ohne Bedeutung.
Manual path cost	Abhängig vom maximaler Datenrate des Ports	Sofern der 'Path cost mode' auf 'Manual' eingestellt ist, kann hier ein beliebiger Wert im Bereich von 1 bis 200.000.000 für die Pfadkosten eingestellt werden.

Edge Port	No	Über diesen Parameter kann vorbestimmt werden, ob an dem Port kein weiterer Switch mit Spanning Tree Protocol erwartet wird (vermutlich ein Endgerät angeschlossen). Die hier eingestellte Vorgabe dient nur als Startwert unmittelbar nach einem Link-Up am betreffenden Port. Durch die standardmäßig eingeschaltete Auto-Edge Funktion, überprüft der Switch permanent, ob die Vorgabe mit der Wirklichkeit übereinstimmt und passt den tatsächlich verwendeten Edge Port Modus ggf. entsprechend an (siehe Statusparameter 'Edge Port' im Kapitel 10.73.5. RSTP - Port Statusparameter). Als Vorgabe kann aus zwei verschiedenen Modi ausgewählt werden: • No Nach einem Link-Up wird zunächst davon ausgegangen, dass an dem betreffenden Port ein Switch mit Spanning Tree Protocol angeschlossen ist. Insofern wird der Port zunächst auf Blocking geschaltet und geprüft, ob tatsächlich ein Switch mit BPDU Paketen antwortet. Antwortet innerhalb von 15 Sekunden kein Switch, so wird der aktuell verwendete Edge Port Modus automatisch auf 'Yes' umgestellt (siehe Statusparameter 'Edge Port' im Kapitel 10.73.5. RSTP - Port Statusparameter). • Yes (PortFast) Nach einem Link-Up wird zunächst davon ausgegangen, dass an dem betreffenden Port KEIN Switch mit Spanning Tree Protocol angeschlossen ist (typischerweise ein Endgerät). Deshalb wird der Port sofort auf Forwarding geschaltet, allerdings werden trotzdem BPDU Pakete versendet. Sollte dann ein Switch mit BPDU Paketen antworten, so wird der aktuell gültige Edge Port Modus automatisch auf 'No' umgestellt (siehe Statusparameter 'Edge Port' im Kapitel 10.73.5. RSTP - Port Statusparameter).
Point-to-Point link	Yes (forced)	Dieser Parameter gibt vor, ob der Port an einen geswitchten Port eines Nachbarswitches oder an einen Hub (Halb-Duplex) angeschlossen ist. Ports, die an einen Hub angeschlossen sind, und keine Edge Ports sind, verzögern die schnelle Rekonfiguration des Switches. In diesem Fall wird nämlich davon ausgegangen, dass am Hub mehrere Spanning Tree Bridges angeschlossen sind und eine schnelle Umschaltung nicht möglich ist. Als Vorgabe kann aus drei verschiedenen Modi ausgewählt werden: • Yes (forced) (Factory-Default) Unabhängig vom aktuellen Duplex Mode, wird fest vorgegeben, dass der Port an einen geswitchten Port eines Nachbarswitches angeschlossen ist. • No (forced) Unabhängig vom aktuellen Duplex Mode, wird fest vorgegeben, dass der Port an ein Hub Segment angeschlossen ist. • Auto Abhängig vom aktuellen Duplex Mode, wird der tatsächlich verwendete Point-to-Point Modus eingestellt. Bei einer Full-Duplex Verbindung, wird ein Point-to-Point Link angenommen und bei einer Halb-Duplex Verbindung, wird von einem angeschlossenen Hub Segment ausgegangen (siehe Statusparameter 'Point-to-Point link ' im Kapitel 10.73.5. RSTP - Port Statusparameter).

10.73.4. RSTP - Globale Statusparameter

Bezeichnung	Funktion
Root Bridge ID	Die Bridge ID der Root Bridge. Eine Bridge ID besteht aus acht Bytes als vorzeichenfreier Integer-Wert. Beim Vergleich zweier Bridge IDs ist diejenige die höhere 'bessere' Priorität, deren numerischer Wert niedriger ist. Die zwei ersten Bytes beinhalten die Bridge-Priority. Die letzten sechs Byte enthalten die MAC-Adresse und stellen damit die Eindeutigkeit der Bridge ID bei gleicher Priority sicher. Der Switch mit der niedrigsten numerischen Bridge ID wird die Root Bridge. Die übliche Schreibweise für eine Bridge ID lautet: Bridge-Priority / MAC-Adresse
Bridge Status	Zeigt an, ob dieser Switch die Funktion der Root Bridge oder einer Designated Bridge hat.
Root Port	Die Port-Nummer des Root Ports. Der Root Port ist der am nächsten zur Root-Bridge liegende Port. HINWEIS: Die Root Bridge ist der einzige Switch ohne Root-Port. In diesem Fall wird als Root Port der Wert 0 ausgegeben.
Root Cost	Die Pfadkosten vom Root Port bis zur Root Bridge. HINWEIS: Die Root Bridge ist der einzige Switch ohne Root-Port. In diesem Fall wird als Root Cost der Wert 0 ausgegeben.
Learned Max Age	Die von der Root Bridge übernommene Max Age.
Learned Hello Time	Die von der Root Bridge übernommene Hello Timet.
Learned Forward Delay	Der von der Root Bridge übernommene Forward Delay.
Topology Changes	Die Anzahl der Topologie Änderungen. Eine Topologie-Änderung kann ausgelöst werden durch: • Hinzukommen eines Datenpfades • Ausfallen eines Datenpfades • Hinzukommen eines Spanning Tree Switches oder • Ausfall eines Spanning Tree Switches Eine Topologie-Änderung wird automatisch erkannt und das Netz wird so rekonfiguriert, dass wieder ein Baum entsteht und alle Geräte in dem Baum erreichbar sind. Dabei treten auch vorübergehend keine Schleifen auf.
Time since last Topology Change	Die Zeit, die seit der letzten Topologie Änderung vergangen ist.

10.73.5. RSTP - Port Statusparameter

Bezeichnung	Funktion
State	Zeigt den aktuellen Spanning Tree Zustand des jeweiligen Ports an. Mögliche Zustände sind: • Forwarding Der Port ist in die aktive Topologie eingebunden und leitet Daten weiter. • Blocking Der Port nimmt nicht an der Datenübertragung der aktiven Topologie teil. Es werden ausschließlich BPDU Pakete gesendet und empfangen. • Learning Der Port nimmt nicht an der Datenübertragung der aktiven Topologie teil, aber MAC-Adressen werden gelernt. Es werden ausschließlich BPDU Pakete gesendet und empfangen. • no Link Der Port empfängt kein Link Signal und nimmt daher nicht an der Datenübertragung der aktiven Topologie teil.
Path Cost	Zeigt die für diesen Port verwendeten Pfadkosten an. Für weitere Informationen siehe Parameter 'Path cost mode' im Kapitel <u>10.73.3. RSTP - Port Konfigurationsparameter</u> .
Designated Root	Die Bridge ID der Root Bridge.
Designated Cost	Zeigt die Pfadkosten dieses Segments zur Root Bridge.
Designated Bridge	Die Bridge ID des Switch, von dem dieser Port die besten BPDUs erhält. Die übliche Schreibweise für eine Bridge ID lautet: 'Bridge-Priority / MAC-Adresse'.
Designated Port	Die Port ID des Ports, über den die BPDUs von der Designated Bridge gesendet werden. Die übliche Schreibweise für die Port ID lautet: 'Port-Priority / Port-Nummer'
Port Role	Zeigt die Rolle des Ports in der Spanning Tree Topologie an: • Root Port Der anhand der Pfadkosten am nächsten zur Root-Bridge liegende Port. Die Root-Bridge ist der einzige Switch ohne Root-Port. • Designated Port Ein Designated Port zeigt downstream, d.h. von der Root-Bridge weg und besitzt die günstigsten Pfadkosten in das Segment in welchem er sich befindet. • Alternate Port Ein Alternate Port stellt einen (alternativen) Weg zur Root dar und nimmt nicht an der aktiven Topologie teil. Falls der Root Port ausfällt, kann auf den Alternate Port schnell umgeschaltet werden. • Backup Port Ein Backup Port stellt einen Pfad in ein Segment dar, in das dieser Switch bereits einen Designated Port (mit besseren Pfadkosten) verbunden hat. D.h., dieser Port nimmt nicht an der aktiven Topologie teil. Falls der Designated Port ausfällt, kann auf den Backup Port schnell umgeschaltet werden.
Edge Port	Zeigt an, ob der Port als Edge Port arbeitet. Über den Konfiguration Parameter 'Edge Port' (siehe Kapitel <u>10.73.3. RSTP - Port Konfigurationsparameter</u>) kann der Startwert unmittelbar nach einem Link-Up vorbestimmt werden. Durch die standardmäßig eingeschaltete Auto-Edge Funktion, überprüft der Switch permanent, ob die konfigurierte Vorgabe mit der Wirklichkeit übereinstimmt und passt den tatsächlich verwendeten Edge Port Modus entsprechend an. Damit ein Port als Edge Port erkannt wird, dürfen an diesem Port alle möglichen Geräte wie z.B. Router, Server, PC usw. angeschlossen werden. Wichtig ist nur, dass diese Geräte keinerlei Spanning Tree Funktionalität besitzen und daher auch keine BPDU Pakete versenden.

Point-to-Point Link	Zeigt an, ob der Port als Point-to-Point Link arbeitet. Über den Konfiguration Parameter 'Point-to-Point link' (siehe Kapitel 10.73.3. RSTP - Port Konfigurationsparameter) kann der Modus fest vorgegeben werden oder, bei Auswahl der Option 'Auto', dynamisch zugewiesen werden. In Fall 'Auto', wird bei einer Full-Duplex Verbindung ein Point-to-Point Link angenommen und bei einer Halb-Duplex Verbindung, wird von einem angeschlossenen Hub Segment ausgegangen und als Point-to-Point Status 'No' angezeigt. In diesem Fall wird davon ausgegangen, dass am Hub mehrere Spanning Tree Switches angeschlossen sein können und eine schnelle Umschaltung im Fehlerfall nicht möglich ist.
Spanning Tree Protocol detected	Zeigt an, ob auf dem Port BPDU Pakete nach dem alten STP Standard gesendet und empfangen werden. Dies kann zwei Ursachen haben: a) Der Switch ist zwar unter 'Protocol version' für RSTP konfiguriert, aber am Port wurden BPDU Pakete nach dem alten STP Standard empfangen. In diesem Fall schaltet der Switch den betreffenden Port in den Kompatibilitätsmodus und sendet dann seinerseits ebenfalls STP Pakete. Die Vorteile des Rapid Spanning Tree gehen dann allerdings für den gesamten Switch verloren. b) Der Switch ist unter 'Protocol version' für 'STP only' konfiguriert und am betreffenden Port wurden ebenfalls BPDU Pakete nach dem alten STP Standard empfangen.

10.73.6. RSTP - Konfigurationshinweise

Folgende Regeln sind beim Aufbau eines Spanning Tree Netzes unbedingt zu beachten:

- Alle eingesetzten Infrastrukturkomponenten im Netzwerk, die Spanning Tree nicht aktiv unterstützen, müssen transparent für Spanning Tree Nachrichten (BPDUs) sein und alle BPDUs unverändert an alle Ports weiterleiten.
- Mediakonverter, die in den Spanning Tree Datenpfad eingeschleift werden, dürfen keine MAC-Adressen lernen. Vielfach sind solche Konverter simple Zweipor-Switches und haben entsprechende Adressentabellen. Dies kann im Fehlerfall dazu führen, dass die Rekonfiguration des Spanning Tree bis auf die Address-Ageing-Zeit des Mediakonverters verlängert wird (dies sind meist 5 Minuten).
- Ferner müssen Mediakonverter, die in den Spanning Tree Datenpfad eingeschleift werden, eine Link Verknüpfung zwischen Fiber und Twisted Pair Port aufweisen. Dies bedeutet, dass ein Linkausfall auf der Fiber Seite auf die Twisted Pair Seite durchgereicht werden muss und umgekehrt. Ansonsten kann ein Linkausfall nicht schnell genug erkannt werden und es laufen die normalen STP Timer ab.
- Die absolut maximale Anzahl von Switches, die in einen Ring geschaltet werden dürfen, ist 50 (dafür muss allerdings der RSTP Parameter 'Max. age/hops' von der Werkseinstellung 20 auf 50 erhöht werden). Erfahrungen haben aber gezeigt, dass nicht mehr als 30 Switches in einem einzelnen Ring verbunden werden sollten. Dies hat folgende Gründe:
 - Minimierung der Umschaltzeiten im Fehlerfall
 - Minimierung der Paketlaufzeiten (jeder Switch macht Store-and-Forward mit entsprechender Verzögerung)
 - Mehr Stabilität des Spanning Tree Protokolls gegenüber schlechten Fiber Strecken mit Paketverlusten

10.73.7. RSTP - Konfigurationshinweise in Verbindung mit Cisco PVST

Folgende Konfigurationshinweise sind zu beachten, falls ein Nexans Switch mit Rapid Spanning Tree (RSTP) nach IEEE802.1D an einen Cisco Switchport mit Per-VLAN Spanning Tree (PVST) angeschlossen wird:

- der Spanning Tree Mode des Cisco Switches muss auf Rapid-PVST+ eingestellt sein. Das Cisco CLI Kommando lautet: `spanning-tree mode rapid-pvst`.
- auf dem betreffenden Cisco Switchport muss das VLAN 1 aktiviert sein. Dabei es gleichgültig, ob dieses als Nativ-VLAN oder als getaggted VLAN konfiguriert ist.
- auf dem Nexans Port muss ebenfalls das VLAN 1 aktiviert sein. Dies kann entweder als Default-VLAN für den betreffenden Port konfiguriert werden, oder, falls der Trunking Mode des betreffenden Ports auf 802.1Q-Tagging konfiguriert ist, reicht es aus, wenn das VLAN 1 in der VLAN Table eingetragen ist.

Bei Beachtung der obigen Hinweise, ist sichergestellt, dass alle VLANs korrekt geblockt werden und keine Loop im Netz entstehen kann. Wenn bei Linkausfall ein Standby-Port von Blocking auf Forwarding geschaltet werden muss, so geschieht dies beim Nexans Switch zeitgleich für alle VLANs innerhalb weniger

Millisekunden. Auf der *Cisco* Seite kann jedoch nur das VLAN 1 entsprechend schnell durchgeschaltet werden. Bei allen anderen VLANs des betreffenden Trunk-Ports wird die Umschaltung von Blocking auf Forwarding über die PVST-Timer durchgeführt und dauert typischerweise ca. 15-30 Sekunden. Die Ursache dafür ist, dass auf dem Nexans Switch nur eine einzige Spanning Tree Instanz läuft und deshalb der *Cisco* Switch nur für diese eine Instanz eine schnelle Umschaltung durchführen kann.

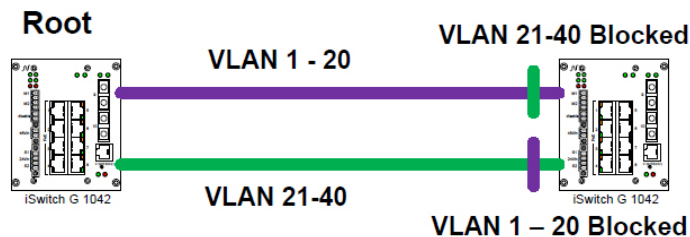
HINWEIS: Viele *Cisco* Switches unterstützen ebenfalls das Multiple Spanning Tree Protokoll nach IEEE802.1s bzw. IEEE802.1Q. Da dieses Protokoll ebenfalls von *Nexans* Switches unterstützt wird, kann hierüber eine einheitliche herstellerunabhängige Spanning Tree Topology aufgebaut werden.

10.74. Multiple Spanning Tree Protocol (MSTP)

10.74.1. MSTP - Allgemeine Funktionsweise

Das Multiple Spanning Tree Protokoll (MSTP) ermöglicht es, mehrere VLANs auf derselben Spanning Tree Instanz abzubilden. Im Vergleich zu Per-VLAN-Spanning Tree ermöglicht es so die Reduzierung der Spanning Tree Instanzen, die für eine hohe Anzahl von VLANs benötigt wird. MSTP erweitert den RSTP Standard. Mit dem Einsatz von MSTP kann Load-Balancing realisiert werden, da es möglich ist, verschiedenen VLANs unabhängig voneinander aufzuteilen.

Der große Vorteil des MSTP ist das Load-Balancing. Stellt man sich z.B. einen redundanten Link zwischen 2 Bridges vor, wurde bei Einsatz von RSTP/STP der komplette Datenverkehr über einen Link gesendet, da der redundante Pfad geblockt wurde. Verwendet man bei gleicher Topologie MSTP, so kann Load-Balancing realisiert werden



In diesem Beispiel gibt es VLAN 1-40. Um die Vorteile des MSTP nutzen zu können wurden zwei VLAN Instanzen erstellt. Die erste Instanz beinhaltet VLAN 1-20, die zweite VLAN 21-40. Durch gezielte Konfiguration werden die VLAN Instanzen an unterschiedlichen Stellen geblockt und somit der Datenverkehr über beide Verbindungen verteilt. Erst wenn ein Link ausfallen sollte, wird der Datenverkehr wieder über eine Verbindung realisiert.

In MSTP ist es vorgesehen MST Regionen zu definieren in denen sich Bridges miteinander verständigen und mehrere Spanning Tree Instanzen verwalten können. Eine Region umfasst eine Gruppe von Switchen, die denselben MST Configuration Name, dieselbe MST Configuration Revision Number und die gleiche Konfiguration von VLANs und Spanning Tree Instanzen haben. MSTP Instanzen haben keinen direkten Kontakt zur Außenwelt. An dieser Stelle würde man eine Inkompatibilität von MST mit STP und RSTP vermuten. Dies ist aber nicht der Fall und wird im folgenden noch erläutert. Auf jedem Switch der MST unterstützt, lassen sich folgende Attribute einstellen und somit verschiedene MST Instanzen erstellen:

Ein Konfigurationsname, der aus Zahlen und Buchstaben besteht (32 bytes).

Eine Konfiguration Revisionsnummer (2 bytes).

Eine 4096-Elemente Tabelle, die alle der potentiellen 4096 VLANs enthalten und den Zuordnungen zu den Instanzen enthält.

Um das VLAN-To-Instance Mapping zu ermöglichen, muss das Protokoll in der Lage sein die Regionsgrenzen zu ermitteln. Um dies zu ermöglichen, werden die Regionsinformationen innerhalb der BPDUs Frames versendet. Die BPDUs enthalten jedoch keine genauen Informationen über das VLAN-To-Instance Mapping, da die einzelnen Switche nur wissen müssen, ob sie sich in der gleichen Region wie ihre Nachbarn befinden.

Innerhalb des gesendeten BPDU befindet sich eine, durch eine mathematische Hash Funktion abgeleitete Zusammenfassung des VLAN-To-Instance Mapping, sowie der Konfigurationsnamen, und die Revisions Nummer. Wenn ein Switch einen solchen BPDU erhält, vergleicht er die VLAN Zusammenfassung, den Namen und die Revisionsnummer mit den eigenen Werten. Sollten einer dieser Werte nicht übereinstimmen, befindet sich der Port, über den die BPDU empfangen wurde, an einer Grenze zu einer anderen Region.

Eine MSTP Bridge muss in der Lage sein, mindestens zwei Instanzen verwalten zu können. Die sogenannte Internal Spanning Tree (IST) Instanz 0. Diese existiert immer auf allen Ports. Desweiteren muss mindestens eine Multiple Spanning Tree Instance (MSTI) verwaltet werden.

Um die Rolle von IST zu verstehen muss man sich klar machen, dass MSTP dem IEEE Standard angehört. Somit muss MSTP auch mit dem 802.1q Standard funktionieren. In diesem Standard gibt es aber nur eine

STP Instanz, die Common Spanning Tree (CST) genannt wird. Bei der IST Instanz handelt es sich um eine RSTP Instanz, die die Kommunikation zwischen CST und MSTP ermöglicht. Die IST Instanz repräsentiert die komplette MSTP Region als eine virtuelle Bridge. In Abbildung 10-1 IST Instance 1 sehen wir eine Topologie mit einer CST und einer IST Instanz. Schaut man sich die geblockten Verbindungen an, stellt man fest, dass bei Default Konfiguration von RSTP, der Link zwischen Switch A und Switch B geblockt sein sollte. Desweiteren erwartet man, dass der zweite Kreis irgendwo innerhalb der MST Region geblockt wird und nicht im Link zwischen Switch C und D.

Da die IST Instanz jedoch als eine virtuelle Bridge angesehen wird, die in einer einzigen Spanning Tree Instanz, der CST läuft, muss man sich die Topologie wie in Abbildung 10-2 IST Instance 2 vorstellen. Hier lässt sich gut erkennen, dass der Link zu Switch B als ein Alternate Port angesehen wird, und somit geblockt wird. Desweiteren lässt sich nun auch nachvollziehen, warum der Link zwischen C und D geblockt wird.

Die gesamte MSTP Region erscheint also nach außen als eine einzige virtuelle CST Bridge. In den BPDU Frames, die von Switch C gesendet werden, werden die Pfadkosten sowie die Message-Age so erhöht, als wäre nur ein einziger Switch passiert worden. Desweiteren fügt Switch C seine Bridge-ID in das Sender Bridge-ID Feld ein.

Abbildung 10-1 IST Instance 1

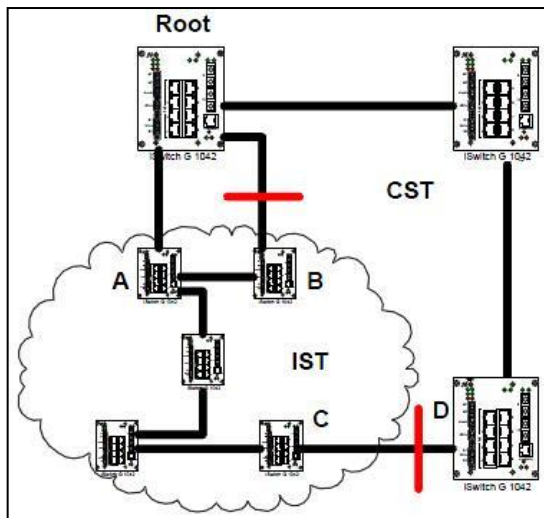
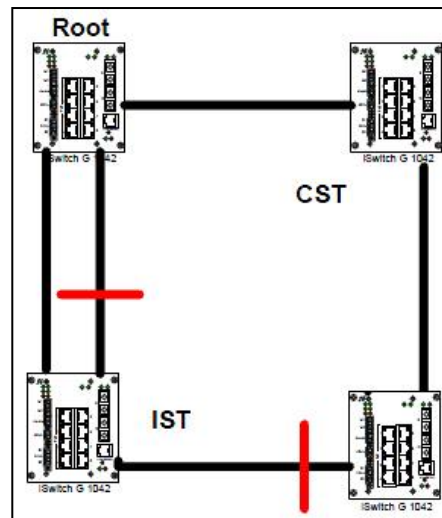


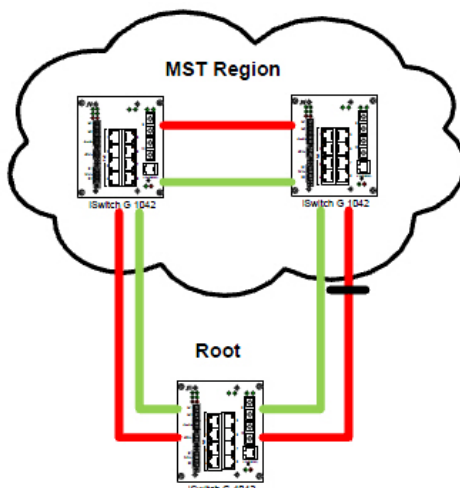
Abbildung 10-2 IST Instance 2



MSTIs sind RSTP Instanzen, die nur innerhalb einer MSTP Region existieren. Im Gegensatz zur IST Instanz haben MSTIs keinen Kontakt zu benachbarten Regionen oder zu STP/RSTP Instanzen. Sie versenden keine BPDU Pakete außerhalb der Region und werden somit auch nicht in RSTP Berechnungen außerhalb dieser Region mit einbezogen. Innerhalb der MSTP Region versenden die MSTIs BPDUs, die als normale RSTP BPDUs angesehen werden können. Jeder dieser BPDUs enthält zusätzlichen Informationen über alle MSTIs. Jeder Switch versendet nur einen BPDU. Es werden nicht, wie man vermuten könnte, für jede Instanz eigene BPDUs versendet. Das erste Informationsfeld dieser BPDUs enthält Informationen über die IST Instanz, gefolgt von den MSTI Informationen, dem sogenannten MRecord. Der MRecord enthält Informationen, um die RSTP Topologie der MSTIs zu berechnen

Der einzige Kontakt einer MSTP Region mit der Außenwelt ist die IST Instanz. In Abbildung 10-3 Interact with the Outside World ist folgendes Szenario gegeben: die rote Linie zeigt die IST Instanz. Da sie überall vorhanden ist, wird diese natürlich an einer Stelle geblockt. Nehmen wir an, innerhalb der MST Region wird VLAN 10 bis 50 gemapped und zusätzlich sind diese VLANs überall in der Netzwerktopologie z.B. durch Trunking erlaubt. Da keine BPDU Pakete von den beiden Switchen, die sich innerhalb der MSTP Region befinden, an die Root-Bridge gesendet werden, könnte man davon ausgehen, dass hier ein Loop entsteht, da es für diese VLANs keinen geblockten Pfad gibt. Um dies zu vermeiden, folgen die MSTIs der IST Instanz an Boundary-Ports. Somit wird hier nicht nur die IST Instanz, sondern ebenfalls die MST Instanz geblockt. Daraus resultiert, dass auch VLAN 10 bis 50 keinen Loop erzeugen.

Abbildung 10-3 Interact with the Outside World



Für detaillierte Hinweise zur Konfiguration der von MSTP setzten Sie sich bitte mit dem Nexans Support in Verbindung.

10.74.2. MSTP - Identifier Setup

Bez. im NEXMAN	Default Wert	Funktion
MSTP Name (1...32 chars)	NEXANS-<MAC-Adresse>	Der Name der MSTP Region. Per Factory-Default ist hier der Text "NEXANS-" mit angehängter MAC Adresse des Switches konfiguriert.
MSTP Revision (0...65535)	0	Die Revision der MSTP Region.

10.74.3. MSTP - Instance Setup

Bez. im NEXMAN	Default Wert	Funktion
Instance ID	-	Die ID der MSTP Instanz.
Bridge Priority	32768	Die Bridge Priority der MSTP Instanz.
Mapped VLANs	-	Die dieser MSTP Instanz zugeordneten VLANs.
Instance ID Offset	0	Dieser Wert bestimmt den zulässigen Bereich für die Instance IDs. Laut Norm dürfen die Instance IDs im Bereich 1-4094 liegen. Der Switch unterstützt daraus einen Teilbereich von 250 IDs. Wenn z.B. der Offset auf 1000 eingestellt ist, können IDs von 1000...1250 angelegt werden. Bei einem Offset von 0 (Default Wert), können IDs von 1...250 angelegt werden.

10.74.4. MSTP - Globale Statusparameter

Bezeichnung	Funktion
MSTP Digest	Damit zwei benachbarte Switch zur selben Region gehören, müssen beide Switches denselben MSTP Namen, dieselbe MSTP Revision und denselben MSTP Digest aufweisen. Aus der Konfiguration der einzelnen MSTP Instanzen wird der sogenannte MSTP Digest berechnet. Nur wenn auf beiden Switches alle MSTP Instanzen identisch konfiguriert sind, stimmen die beiden MSTP Digest Werte ebenfalls übereinstimmt.

10.74.5. MSTP - Instance Statusparameter

Bezeichnung	Funktion
State	Zeigt den aktuellen Spanning Tree Zustand des jeweiligen Ports an. Mögliche Zustände sind: • Forwarding Der Port ist in die aktive Topologie eingebunden und leitet Daten weiter. • Blocking Der Port nimmt nicht an der Datenübertragung der aktiven Topologie teil. Es werden ausschließlich BPDU Pakete gesendet und empfangen. • Learning Der Port nimmt nicht an der Datenübertragung der aktiven Topologie teil, aber MAC-Adressen werden gelernt. Es werden ausschließlich BPDU Pakete gesendet und empfangen. • no Link Der Port empfängt kein Link Signal und nimmt daher nicht an der Datenübertragung der aktiven Topologie teil.
Role	Zeigt die Rolle des Ports in der Spanning Tree Topologie an: • Root Der anhand der Pfadkosten am nächsten zur Root-Bridge liegende Port. Die Root-Bridge ist der einzige Switch ohne Root-Port. • Designated Ein Designated Port zeigt downstream, d.h. von der Root-Bridge weg und besitzt die günstigsten Pfadkosten in das Segment in welchem er sich befindet. • Alternate Ein Alternate Port stellt einen (alternativen) Weg zur Root dar und nimmt nicht an der aktiven Topologie teil. Falls der Root Port ausfällt, kann auf den Alternate Port schnell umgeschaltet werden. • Backup Ein Backup Port stellt einen Pfad in ein Segment dar, in das dieser Switch bereits einen Designated Port (mit besseren Pfadkosten) verbunden hat. D.h., dieser Port nimmt nicht an der aktiven Topologie teil. Falls der Designated Port ausfällt, kann auf den Backup Port schnell umgeschaltet werden. • Master Der Master Port kennzeichnet einen Port, der den Übergang von einer Region zu einer Andern darstellt.
Cost	Zeigt die für diesen Port verwendeten Pfadkosten an.
Prio.	Zeigt die für diesen Port verwendete Priorität an.
Designated Cost	Zeigt die Pfadkosten zur Root Bridge.
P2P	Zeigt an, ob der Port als Point-to-Point Link arbeitet.

Category	Zeigt die Kategorie der Verbindung an: • Edge Port arbeitet als Edge Port, d.h., es werden keine BPDU Pakete empfangen des angeschlossenen Gerätes empfangen. • Internal Das angeschlossenen Geräte unterstützt ebenfalls MSTP und gehört zu selben Region. Damit zwei benachbarte Switch zur selben Region gehören, müssen beide Switches denselben MSTP Namen, dieselbe MSTP Revision und denselben MSTP Digest aufweisen. • Boundary(RSTP) Das angeschlossenen Geräte unterstützt entweder ebenfalls MSTP aber gehört nicht zu selben Region, oder es unterstützt RSTP und gehört daher grundsätzlich nicht zu selben Region. • Boundary(STP) Das angeschlossenen Geräte unterstützt STP und gehört daher grundsätzlich NICHT zu selben Region.
-----------------	---

10.75. Link Aggregation

10.75.1. Link Aggregation - Allgemeine Funktionsweise

Link Aggregation (IEEE 802.1AX, ehemals IEEE 802.3ad) ist ein Netzwerkprotokoll um die verfügbare Bandbreite durch Bündelung mehrere physikalischer Schnittstellen zu einer logischen Einheit zu vergrößern. Gleichzeitig kann durch die Verwendung des Link Aggregation eine Redundanz aufgebaut werden.

Es steht sowohl das statische, als auch das dynamische Link Aggregation, auch LACP (Link Aggregation Control Protocol) genannt, zur Verfügung. Im Gegensatz zum statische Link Aggregation, werden beim dynamischen Link Aggregation sogenannte LACPDU (Link Aggregation Control Protocol Data Units) zwischen beiden Endpunkten gesendet. LACPDU dienen zur Konfigurationsbestätigung und zur Erkennung des Ausfalls eines physikalischen Links.

Um die korrekte Funktionsweise von Link Aggregation zu gewährleisten müssen folgende Voraussetzungen erfüllt sein:

- Alle Ports einer LAG müssen den Link State FDX haben
- Alle Ports einer LAG müssen dieselbe Datenrate aufweisen
- Es darf kein weiteres Redundanzprotokoll auf den zugehörigen Ports aktiviert sein
- Link Aggregation funktioniert nur zwischen zwei Endpunkten, es sei denn zwei unterschiedliche Endpunkte laufen als Virtuelle Einheit

10.75.2. Link Aggregation - Global Setup

Bez. im NEXMAN	Default Wert	Funktion
Link Aggregation global enable	Disable	Nur wenn hier Link Aggregation global eingeschaltet ist, werden die Konfigurierten LAGs aktiv.
Link Aggregation Protocol Timeout	Slow	Konfiguration des LACP Timeout für empfangene und des Zeitintervalls für gesendete LACP Pakete. Es können folgenden Timeout Modi konfiguriert werden: • Slow (Timeout 30 sec.) Dies ist die Standardeinstellung und kompatibel mit den meisten LACP Gegenstellen. Insbesondere bei Anbindung an einen Multi-Chassis Link Aggregation (MLAG) Verbund sollte diese Einstellung verwendet werden. • Fast (Timeout 1 sec.) Bestimmte Endgeräte, insbesondere Server, benötigen diese Einstellung.

10.75.3. Link Aggregation – Group Setup

Bez. im NEXMAN	Default Wert	Funktion
Mode	Deleted	Es können folgenden LAG Modi konfiguriert werden: • Deleted Die LAG existiert nicht. • Static Für diese LAG-ID ist das statische Link Aggregation aktiv. Sobald ein Port, der dieser LAG zugeordnet ist einen aktiven Link hat, wird er aktiv für das Link Aggregation genutzt. • LACP Im Gegensatz zum mode „Static“ wird bei der Verwendung von LACP eine Konfigurationsprüfung durchgeführt. Ein aktiver Link wird nur dann in einer LAG aktiv genutzt, wenn dieser von beiden Switchen bestätigt wurde. • Disabled Die Konfigurierte LAG ist deaktiviert.
Name (1...15 chars)	Empty	Der Name der LAG.
Edit Member Ports	-	Die dieser LAG-ID zugeordneten Ports.
Delete LAG	-	Löscht die LAG und deren Konfiguration.

10.76. Media Redundancy Protocol (MRP)

Das Medium Redundancy Protocol (MRP) ist ein deterministisches IEC 62439 Standard Protokoll für Ring-Topologie. MRP verwendet einen Redundanz Manager (RM), der den Ring überwacht und beim Ausfall eines Redundanz Clients den Ring schließt. Jeder Switch unterstützt bis zu fünf Ringe als Redundanz Manager und eine einzelne Instanz als Redundanz Client. Über Testpakete, die vom RM versendet werden, wird ermittelt, ob der Ring geschlossen ist. Sollten die gesendeten Testpakete ausbleiben, kann so festgestellt werden, dass der Ring unterbrochen ist.

In einem MRP Ring muss ein Redundanz Manager vom Anwender bestimmt werden. Einer seiner Ports befindet sich bei einer aktiven Ringtopologie im Blocking State. Ist ein Port des RM im Blocking State, sendet und empfängt er Testpakete sowie Link-Change (LC) Pakete, leitet jedoch keinen Data-Traffic weiter.

Die LC Pakete werden von Redundanz Clients (RC) versendet und werden später erläutert. Die beschriebenen Testpakete werden vom RM in beide Richtungen des Rings gesendet. Gehen drei dieser Pakete verloren, d.h. dass die gesendeten Pakete nicht vom RM empfangen werden, geht dieser davon aus, dass der Ring an einer Stelle unterbrochen ist.

Sollte festgestellt werden, dass der Ring unterbrochen ist, so werden von dem RM Topologie Change (TC) Pakete an die Redundanz Clients versendet.

Empfängt ein RC ein Topologie Change Paket, dass vom RM gesendet wurde, so löscht er nach dem Ablauf des im Paket enthaltenen Intervalls seine Forwarding-Database.

Die Redundanz Clients werden ebenfalls vom User konfiguriert. Auch sie spielen eine wichtige Rolle in der Netzwerktopologie. Sollte ein RC feststellen, dass einer seiner Ports, der sich in der Ringtopologie befindet, den Status wechselt, also von Link-Up nach Link-Down oder umgekehrt, so sendet er LC Pakete. Empfängt der RM ein solches LC Paket sendet er seine TC Pakete um das Löschen der Forwarding-Database zu initialisieren.

Sollte es beim MRP zu einer Unterbrechung des Ringes kommen, so wird zwischen drei verschiedenen Fällen unterschieden.

Die Unterbrechung des Rings befindet sich zwischen dem Forwarding-Port des Masters und dem ersten Client. Nun wird der geblockte Port des Masters auf Forwarding gestellt. Wird nun die Unterbrechung aufgehoben und somit der Ring wiederhergestellt, bleibt dieser Port im Forwarding State. Der sogenannte „neue“ Port geht in den Blocking State. Anders als zur Ausgangssituation sind nun Blocking und Forwarding-Ports vertauscht. Der Vorteil hierfür ist, dass es anders als z.B. beim RSTP keine Rekonfigurationszeit gibt. Somit wird ein erneuter Paketverlust vermieden.

Die Unterbrechung des Rings findet nicht unmittelbar an den beiden Ringports des Masters statt. Damit nun der komplette Ring erreichbar ist, geht der bis jetzt geblockte Port in den Forwarding State. Sollte der Ring wieder geschlossen werden, so geht dieser Port in den Blocking State.

Die Unterbrechung ist am Blocking-Port. In diesem Fall wird nichts an den Port Zuständen geändert. Durch das unterschiedliche Verhalten bei der Rekonfiguration wird in zwei Fällen ein erneuter Paketverlust vermieden.

HINWEIS:

Bis einschließlich Firmware Version V5.03go, muss eine Memory Karte mit einer MRP Lizenz im Switch vorhanden sein. Ab Firmware Version V5.03gp kann MRP auch ohne entsprechende Memory Karte aktiviert werden da das MRP Patent im Mai 2019 ausgelaufen ist.

10.76.1. MRP – Global Setup

Bez. im NEXMAN	Default Wert	Funktion
MRP global enable	Disabled	Nur wenn hier das Media Redundancy Protocol global eingeschaltet ist, werden alle Ports, bei denen ebenfalls Media Redundancy Protocol eingeschaltet ist, in die Überwachung der Ring Topologie einbezogen. WICHTIG: Ist das Media Redundancy Protocol hier global ausgeschaltet, verhält sich der Switch für MRP-BPDU Pakete transparent und empfangene MRP-BPDU Pakete werden auf alle Ports weitergeleitet.

Max. recovery time	500ms	Hier sind zwei Einstellungen möglich, 200ms oder 500ms. Das sind die garantierten Erholungszeiten des Media Redundancy Protocols.
---------------------------	-------	---

10.76.2. MRP – Instance Setup

Bez. im NEXMAN	Default Wert	Funktion
Instance ID	-	Die ID der MRP Instanz.
Admin Role	Disabled	Hier sind drei Einstellungen möglich: • Disabled Die MRP Instanz ist disabled • Manager Die MRP Instanz ist ein Redundanz Manager. • Manager (with Ring Port 1 Priority) Die MRP Instanz ist ein Manager (with Ring Port 1 Priority). Der Unterschied zum Standard Manager Mode ist, dass bei einer geschlossenen Ringtopologie grundsätzlich der Ring Port 1 auf forwarding und der Ring Port 2 auf blocking geschaltet wird. • Client Die MRP Instanz ist ein Redundanz Client. HINWEIS: Auf dem Switch ist nur eine Client Instanz zulässig.
Domain-ID	FF - FB	Domain-ID ist ein Universally Unique Identifier (UUID), der eindeutig ein MRP Ring im Netz identifiziert. Jede Instanz muss mit dem eindeutigen Identifier konfiguriert werden. Der Identifier wird automatisch generiert mit dem ersten einstellbaren Byte. Beispiel: Domain-ID 55 entspricht der UUID 55FFFFFF-FFFF-FFFF-FFFF- FFFFFFFF
VLAN-ID	0	Die der MRP Instanz zugeordnete VLAN-ID. Bei VLAN-ID 0 wird kein VLAN zugeordnet und die MRP Pakete werden ohne VLAN-Tag versendet. WICHTIG: Bei der konfigurierten VLAN-ID, darf dieses VLAN nicht dem Default-VLAN der benutzten Ports entsprechen.
Ring-Port 1 Ring-Port 2	0	Die der MRP Instanz zugeordneten Ports. Wenn der Ring-Port auf 0 gesetzt ist, wird kein Port der Instanz zugeordnet. Jeder Port darf nur auf einer Instanz konfiguriert werden. WICHTIG: Beide Ports der Instanz müssen mit derselben Default VLAN-ID und eingeschalteten Trunking 802.1q konfiguriert werden.

10.76.3. MRP – Statusparameter

Bezeichnung	Funktion
ID0-ID4	Zeigt an, ob die Instanz konfiguriert ist und ob der Ring offen oder geschlossen ist. Wenn <Ring Open> angezeigt wird, ist ein Switch oder eine Leitung im Ring ausgefallen.
UUID	Der Universally Unique Identifier.
Transitions/Last change	Zeigt an, wie lange die Ring-Topologie unveränderbar geblieben ist.
Remote Manager	Nur bei Redundanz Client Instanzen zeigt dies die MAC Adresse vom Redundanz Manager an
Link/Admin State	Link Status des MRP Ports.

Role	Die Port Role zeigt an, ob der Port vom MRP Protokoll als Primary oder Secondary eingestellt wurde.
VLAN	Konfigurierte VLAN-ID für MRP Protokoll.
Default-VLAN	Default VLAN-ID von dem Port.
Egress VLAN	Die VLAN-ID mit der MRP Pakete versendet werden.

Für detaillierte Hinweise zur Konfiguration des Media Redundancy Protokolls setzen Sie sich bitte mit dem Nexans Support in Verbindung.

10.76.4. MRP – MRP to Spanning Tree network coupling

Um einen MRP Ring redundant an eine Spanning Tree Topologie anzubinden, wird durch die Verwendung des „MRP to Spanning Tree network coupling“ sichergestellt, dass es unter keinen Umständen zu einem Switching-Loop im Netzwerk kommen kann.

Nachfolgenden Erläuterungen beziehen sich auf die Topologie „Variante A“, bzw. „Variante B“:

Sind beide Ringe (Spanning Tree / MRP) geschlossen, so ist der Link des MRP Rings zwischen den Switchen „C“ und „D“ auf Blocking geschaltet. Das Spanning Tree ist so konfiguriert, dass der Link Zwischen Switch „A“ und „C“ auf Blocking steht.

Fällt nun ein Link im MRP Ring aus, z.B. zwischen Switch „F“ und „G“, so wird der Link zwischen Switch „C“ und „D“ auf Forwarding geschaltet. Zu diesem Zeitpunkt gibt es keine Veränderung der Spanning Tree Topologie. Wird der MRP Ring wieder geschlossen, so geht der auf Forwarding gewechselte Link zurück in den Blocking State und die Topologie ist wieder in der Ausgangslage.

Wenn zusätzlich zu dem Link zwischen Switch „F“ und „G“ der Link zwischen „C“ und „D“ ausfällt, so gibt es eine Veränderung der Spanning Tree Topologie. In diesen Fall geht der Link zwischen Switch „A“ und „C“ nach Verlust von drei „Hello“ Paketen in den Forwarding State.

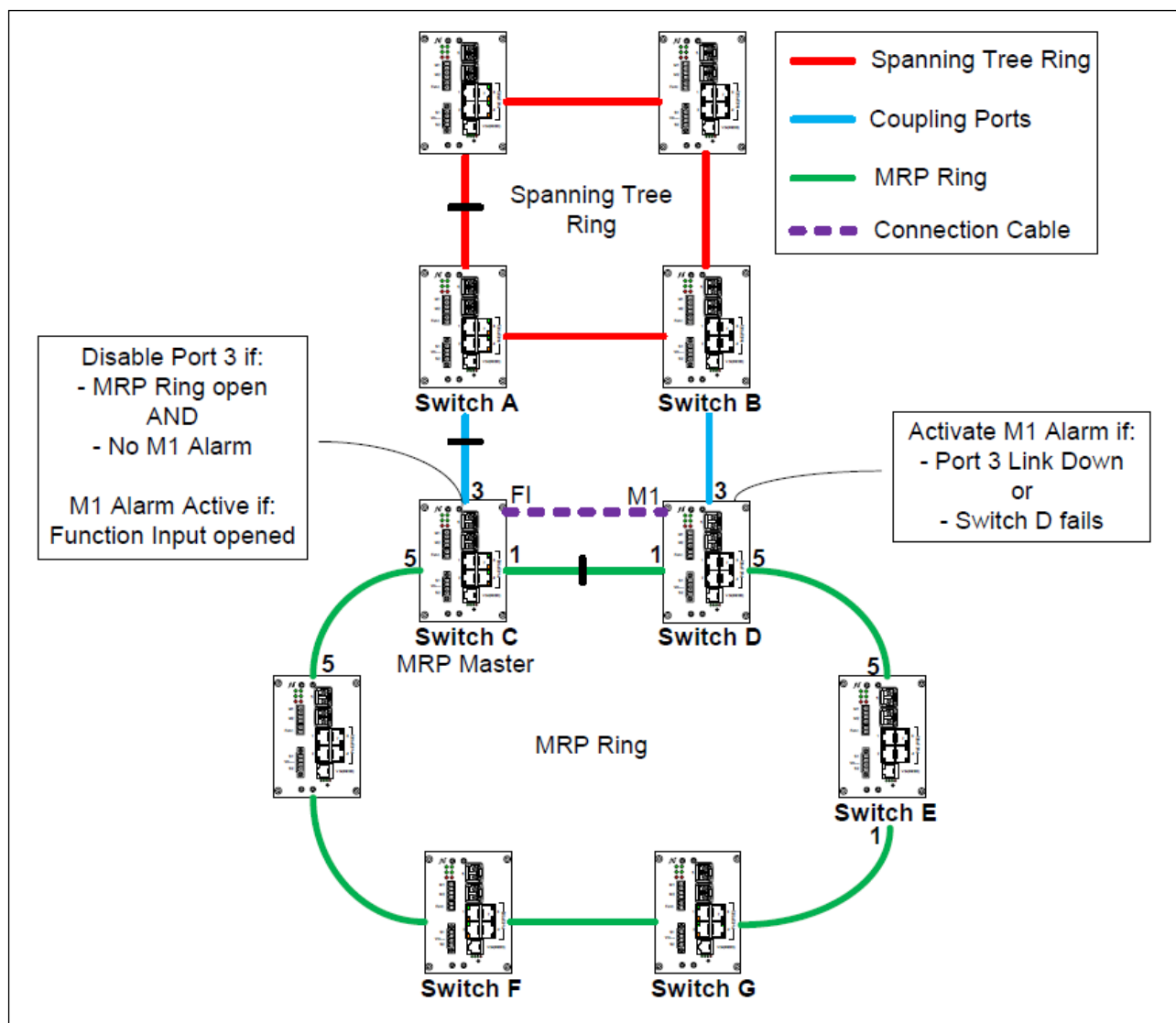
Wird nun der Link zwischen Switch „C“ und „D“, oder „F“ und „G“ wiederhergestellt, so kann das Spanning Tree dies nur durch den Empfang eines „Hello time“ BPDU erkennen. Je nach Spanning Tree Konfiguration kann dies mehrere Sekunden dauern und dazu führen, dass ein Switching-Loop entsteht.

Um diesem Verhalten entgegenzuwirken wird der Port „3“ des Switches „C“ auf „Admin Disabled“ geschaltet, sobald der MRP Ring geöffnet ist. Dieser Port wird nur dann wieder aktiv wenn M1 einen aktiven Alarm hat, oder der MRP Ring geschlossen wird.

Es gibt zwei Szenarien um den M1 Alarm auszulösen:

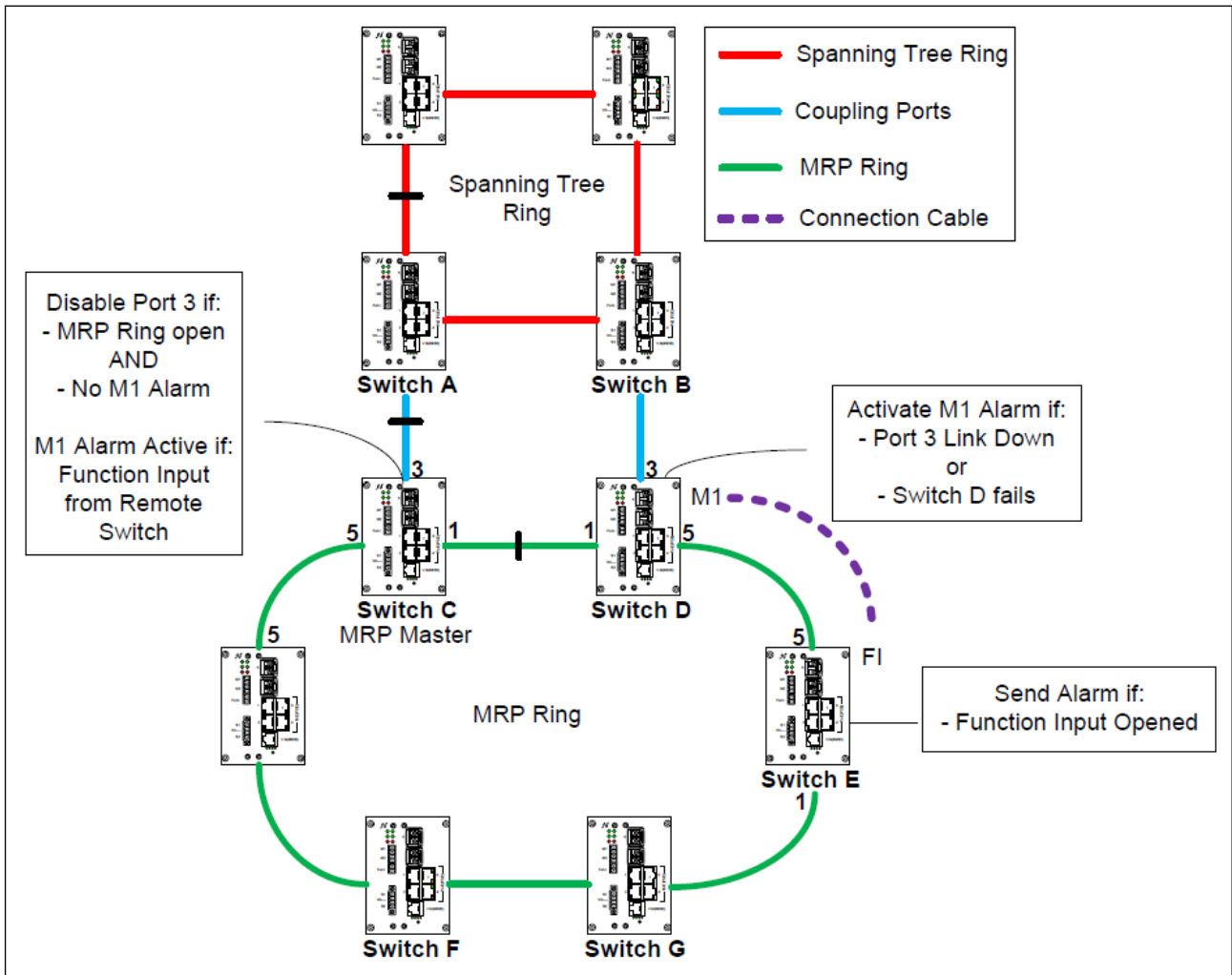
Variante A)

Der Funktionseingang des Switches „C“ ist mit dem M1 Alarm Ausgang des Switches „D“ verbunden. M1 des Switches „D“ wird ausgelöst, wenn der Port „3“ einen Link Down hat, und somit die Spanning Tree Topologie bei geöffnetem Ring abgeschottet wäre, oder wenn der Switch „D“ inaktiv ist. Switch „C“ ist so konfiguriert, dass der M1 Alarm aktiv ist, sobald der Funktionseingang geöffnet ist.



Variante B)

Der M1 Alarm des Switches „D“ ist mit dem Funktionseingang des Switches „E“ verbunden. M1 des Switches „D“ wird ausgelöst, wenn der Port „3“ einen Link Down hat, und somit die Spanning Tree Topologie bei geöffnetem Ring abgeschottet wäre, oder wenn der Switch „D“ inaktiv ist. Switch „E“ sendet einen Alarm in eine Konfigurierte „Alarm Group“ wenn der Funktionseingang geöffnet ist. Switch „C“ ist so konfiguriert, dass der M1 Alarm aktiv ist, wenn in der Konfigurierten „Alarm Group“ ein aktiver Alarm vorhanden ist.



Variante „A“ ist die bevorzugte Variante, jedoch kann es z.B. aufgrund der Örtlichkeit nicht möglich sein den Funktionseingang des Switches „C“ mit dem M1 Alarm Ausgang des Switches „D“ zu verbinden. Das Problem kann ebenfalls bei der Variante „B“ auftreten, jedoch kann dem durch die Hinzunahme eines Switches der nur für die Übertragung des Alarms verwendet wird, entgegengewirkt werden.

10.77. Zeroloss Redundancy

Durch das Nexans Zeroloss Redundancy Protokoll wird sichergestellt, dass in Ringtopologien für einen festgelegten Ethertype kein Paketverlust auftreten kann. Normalerweise gehen durch eine Unterbrechung und die darauffolgende Rekonfiguration der Topologie Pakete verloren. Zeroloss garantiert, dass für den eingestellten Ethertype mindestens 1000 Pakete pro Sekunde verlustfrei übertragen werden. Ein Anwendungsbeispiel ist die Übertragung von GOOSE Paketen mit dem Ethertype 88B8 in IEC 61850 Netzwerken.

10.77.1. Zeroloss – Global Setup

Bezeichnung	Default Wert	Funktion
Zeroloss global enable	Disabled	Nur wenn hier Zeroloss eingeschaltet ist, nimmt der Switch am Zeroloss verfahren teil. WICHTIG: Ist hier Zeroloss ausgeschaltet nimmt der Switch nicht am Zeroloss verfahren teil, und es kann bei einer Unterbrechung des Rings zu einem Paketverlust kommen

10.77.2. Zeroloss – Port Setup

Bezeichnung	Default Wert	Funktion
Zeroloss Role	Disabled	Hier sind drei Einstellungen möglich: • Disabled Zeroloss ist auf diesem Port disabled • Ringport Die Ringports bilden der Zeroloss Ring. • User Port Über diesen Port werden Daten in den Zeroloss Ring gesendet
Ethertype (8800...FFFF)	88B8	Hier wird der Ethertyp bestimmt, der über den User Port in den Zeroloss Ring gesendet werden sollen.

10.78. DHCP Relay / Snooping

10.78.1. DHCP Snooping

Wird DHCP Snooping auf enable gesetzt, so wird dies auf allen Ports, deren Link Type auf „Userport“ bzw. „Userport with active Loop protection“ steht, aktiviert. Sobald an diesen Ports ein Paket empfangen wird, dass von einem DHCP Server stammt, schaltet der Switch den Admin State des entsprechenden Ports auf „Disabled by DHCP Snooping“. Es kann somit unterbunden werden, dass ein DHCP Server an die Userports des Switches angeschlossen wird.

Abgeschaltete Ports können optional nach einer einstellbaren "Re-enable time for DHCP Snooping Disabled ports" automatisch wieder aktiviert werden. Die Zeit ist dabei im Bereich von 1 bis 60000 Sekunden konfigurierbar. kann ein

10.78.2. DHCP Snooping – Global Setup

Bez. im NEXMAN	Default Wert	Funktion
DHCP Snooping enable	Disabled	Hier wird das DHCP Snooping global eingeschaltet. Wenn die Option auf Disable steht, sind beliebige DHCP Pakete auf den Userports erlaubt.
Re-enable time for DHCP Snooping Disabled ports	0	Ports, die Aufgrund von DHCP Snooping abgeschaltet wurden, können optional nach 1 bis 60000 Sekunden automatisch wieder aktiviert werden. Ist die Zeit auf 0 konfiguriert, so muss der Port manuell reaktiviert werden.

10.78.3. DHCP Relay Agent

Der DHCP Relay Agent (Option 82) erlaubt es, die DHCP Anfragen von den angeschlossenen Endgeräten zu verschiedenen DHCP Servers zu verteilen. Das wird erreicht, indem der Switch eine DHCP Option,

bestehende aus dem Remote-ID und dem Circuit-ID, in die DHCP Anfragen von Endgeräten eingefügt. Der DHCP Relay Agent wird pro Port konfiguriert und lässt bis zu drei DHCP Servers pro Port zu.

10.78.4. DHCP Relay Agent – Global Setup

Bez. im NEXMAN	Default Wert	Funktion
DHCP Relay Agent global enable	Disabled	Hier wird der DHCP Relay Agent global eingeschaltet. Wenn die Option auf Disable steht, werden die DHCP Anfragen von den Endgeräten ohne Änderungen weitergeleitet.
Filter original Client DHCP requests	Disabled	Die Original DHCP Anfragen von den Endgeräten werden durch einschalten dieser Option aus dem Netz gefiltert. Wenn diese Option ausgeschaltet ist, wird der Switch zusätzlich zu der originalen Anfrage von dem Endgerät eine DHCP Anfrage mit der Option 82 generieren. Dies geschieht jedoch nur für DHCP anfragen die sich im Management VLAN des Switches befinden.
Remote ID	Port No	Die Remote ID ist ein Teil von der Option 82, und identifiziert das Endgerät. Bei der Einstellung der Remote ID ist es möglich, folgende Parameter als Teil der Remote ID zu generieren: • Port No Die Nummer des Ports • Port MAC Die MAC Adresse des Ports • VLAN-ID Wenn Trunking auf dem Port ausgeschaltet ist, wird die Default VLAN ID des Ports als Teil der Remote ID eingefügt. Wenn Trunking auf dem Port eingeschaltet ist, wird die VLAN-ID von der empfangenen DHCP Anfrage als Teil von Remote ID eingefügt. • User defined Ein vom Benutzer festgelegter Text. WICHTIG: Den Wert der Remote ID kann man aus dem DHCP Relay Agent Status entnommen werden. Dafür ist das erste Byte der Remote ID reserviert und wird von dem Switch als Format Byte benutzt
Circuit ID	Port No	Die Circuit ID ist der zweite Teil der Option 82 und identifiziert ein Netz. Hier können die selben Parameter wie bei der Remote ID konfiguriert werden.

10.78.5. DHCP Relay Agent – Port Setup

Bez. im NEXMAN	Default Wert	Funktion
Role	DHCP Transparent	Hier sind drei Einstellungen möglich: • DHCP Transparent Alle DHCP Anfragen werden von dem Switch unverändert weitergeleitet • DHCP Option 82 Client Die Anfragen von den Endgeräten über diesen Port werden von Switch bearbeitet und mit der Option 82 weitergeleitet • DHCP Server An diesem Port ist ein DHCP Server angeschlossen
Server IP 1 Server IP 2 Server IP 3	0.0.0.0	Es können bis zu drei DHCP Server konfiguriert werden. WICHTIG: Die Server müssen über das Management VLAN erreichbar sein.

10.78.6. DHCP Relay Agent – GlobalStatus

Zeigt den aktuellen DHCP Relay Agent Status. Bei richtig eingestellten Parametern muss der Status auf "running" stehen. Zusätzlich wird angezeigt, ob die originalen DHCP Anfragen von Endgeräten gefiltert werden.

10.78.7. DHCP Relay Agent – Port Status

Bezeichnung	Funktion
Role	Zeigt die eingestellte Role an
Remote ID	Hier wird die Remote ID angezeigt, die vom Switch bei DHCP Anfragen eingefügt wird. Die Flags zeigen dabei lediglich an, aus welchen Teilen die Remote ID besteht und sind kein Teil Bestandteil der Remote ID. Die angezeigten Flags sind: 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	Hier wird die Circuit ID angezeigt, die vom Switch bei DHCP Anfragen eingefügt wird.

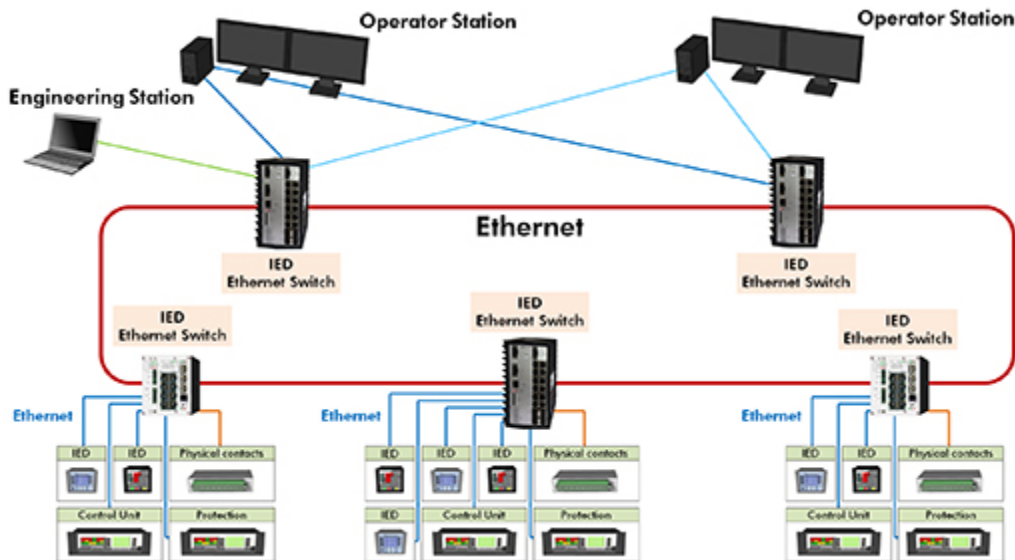
Für detaillierte Hinweise zur Konfiguration des DHCP Relay Agent setzen Sie sich bitte mit dem Nexans Support in Verbindung.

10.79. IEC61850 Protokoll Unterstützung

10.79.1. IEC61850 Übersicht

Die Implementierung des IEC 61850 Protokolls bietet die Möglichkeit, dass Geräte in Umspannstationen (mit Überwachungs-, Steuerungs-, Mess- und Überwachungseinheiten usw.) miteinander kommunizieren und

spezielle Informationen ohne zusätzliche Konverter oder spezielle Teilnetze übertragen können. Nexans IEC 61850 Ethernet-Switches werden Teil eines universellen standardisierten Netzwerks für den Austausch von EID-Daten, -Dienstern und -Netzwerkinformationen gemäß IEC 61850-8-1 / -9-1 / 9-2. Der Nexans IEC61850 Protokollstack hat alle KEMA-Zertifizierungstests bestanden, die auf IEC 61850 basieren und die Interoperabilität und Kompatibilität mit Netzwerkgeräten und Kraftwerkskomponenten verschiedener Hersteller bestätigen.



10.79.2. IEC61850 Access Mode

Über den IEC61850-Access Mode kann der IEC61850-Protokollstack aktiviert werden. Die folgenden Einstellungen sind verfügbar:

- IEC61850 disabled
- Read/Write
- Read/Only

Disabled:

Dies ist die Standardeinstellung. In diesem Modus ist der IEC 61850-Protokollstack deaktiviert.

Read/Write:

In diesem Modus ist der Zugriff auf den IEC61850 Protokollstack mit Read/Write Zugriffsrechten aktiviert.

Read/Only:

In diesem Modus ist der Zugriff auf den IEC61850 Protokollstack mit Read/Only Zugriffsrechten aktiviert.

10.79.3. IEC61850 Objects

Der IEC 61850 Protokollstack unterstützt die folgenden Objekte:

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.lLim	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.LocChsldTyp.stVal	MMS_INTEGER	Type of local chassis identifier 'LocChsld' according to IEEE 802.1AB	R
LPHD1.LocChsld.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 set 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.InNs	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.InNs	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.InNs	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. Funktionsbeschreibung PoE (Power-over-Ethernet)

11.1. Funktionsbeschreibung PoE Allgemein

11.1.1. PoE-Messwerte

Die folgenden PoE-Messwerte werden auf dem PoE-Adapter kontinuierlich ermittelt und können bei Bedarf angezeigt werden:

Pro Port:

- Ausgangsspannung (in V)
- Ausgangsstrom (in mA)
- Ausgangsleistung (in W)
- Powerclass / max. Power (W) (wird nicht von allen PoE-Adaptoren unterstützt)

Für das PoE Powersupply:

- Eingangsspannung (in V)
- Eingangsstrom (in mA)
- Eingangsleistung (in W)

HINWEIS:

Die einzelnen Port-Ausgangsströme werden über Messwiderstände im negativen Zweig der PoE-Ausgangssignale gemessen. Daher darf für eine korrekte Anzeige der Ströme das angeschlossene PoE-Endgerät keinen Kurzschluss zwischen negativer PoE-Spannung und Masse aufweisen. Dies ist üblicherweise nie der Fall, da PoE-Geräte in der Regel Stand-Alone arbeiten. Nur in Sonderfällen, wenn z.B. an einen Accesspoint temporär ein seriell Kabel zwecks Konfiguration angeschlossen wird, kann ein Massekurzschluß entstehen. Ein solcher Kurzschluss führt NICHT zur Zerstörung des Nexans PoE-Adapters, allerdings werden die Ströme und Leistungen dann mit 0 angezeigt.

11.1.2. PoE Power Setup

Hier stehen fünf mögliche Einstellungen zur Verfügung:

- Off
- On (Forced)
- Auto 802.3af
- Auto 802.3af High-Power (Ignores Power Class)
- Auto 802.3at High-Power

Off:

Bei dieser Einstellung ist die POE Spannung permanent **abgeschaltet**.

Overload-Off:

Bei dieser Einstellung hat der Switch eine Überschreitung des eingestellten Powerlimits detektiert und daraufhin die PoE-Spannung automatisch abgeschaltet.

On (Forced):

Hier ist die PoE-Spannung permanent **eingeschaltet**.

Diese Einstellung wird z.B. benötigt, um Endgeräte mit Spannung zu versorgen, die nicht dem IEEE802.3af Standard entsprechen.

VORSICHT:

Wird an einen Port mit permanent eingeschalteter PoE-Spannung ein Nicht-PoE-Endgerät angeschlossen, so kann dies zur Zerstörung der Ethernet-Schnittstelle des betreffenden Endgerätes führen.

Auto 802.3af:

Diese Einstellung wird ausschließlich von PoE-Adaptoren vom **Typ AF** unterstützt.

Bei dieser Einstellung wird die PoE-Spannung entsprechend dem Standard **IEEE802.3af** aufgeschaltet. D.h., nur wenn ein standardkonformes Endgerät auf den betreffenden Port aufgesteckt wird, schaltet der TP-Aufsatz die 48 Volt Spannung durch. Wird das Endgerät wieder abgezogen, so wird durch die integrierte Zero-Current-Detection die Spannung des Ports wieder abgeschaltet.

WICHTIGER HINWEIS:

Es genügt nicht, dass das Endgerät die Pin-Belegung nach IEEE802.3af aufweist, sondern es muss ebenfalls die im Standard definierte Discovery Funktion unterstützen. Einige am Markt erhältliche Endgeräte werben zwar mit Inline Power nach IEEE802.3af, unterstützen aber lediglich die Pin-Belegung des Standards. Möchten Sie trotzdem ein derartiges Endgerät anschließen, so muss die Einstellung {On} gewählt werden.

Auto 802.3af High-Power (Ignores Power Class):

Dieser Mode ist speziell für solche Endgeräte vorgesehen, die zwar nach dem alten Standard IEEE802.3af arbeiten, aber dennoch eine höhere Leistung als 15,4W benötigen. In diesem Fall wird die vom Endgerät übermittelte Powerclass ignoriert und grundsätzlich bis zu 30W zur Verfügung gestellt.

Diese Einstellung benötigen z.B. bestimmte Access Points von Cisco, die die benötigte Leistung nicht über den neuen Standard IEEE802.3at, sondern über das Cisco "Intelligent Power Management" per CDP aushandeln. Möchte man einen solchen Access Point an einem Nexans PSE+ Port betreiben, so muss zusätzlich CDP im Nexans Switch aktiviert sein. Dieser teilt dann dem Access Point die benötigten Informationen per CDP mit.

Auto 802.3at High-Power:

Hierbei können dem angeschlossenen Endgerät bis zu 30W Leistung zur Verfügung gestellt werden. Damit das Endgerät die volle Leistung ziehen darf, muss dieses ebenfalls IEEE802.3at unterstützen und zusätzlich die Powerclass 4 an den Switch melden. Meldet das Endgerät dagegen eine kleinere Powerclass, so werden maximal 15,4W bereitgestellt und ggf. bei Überschreitung der Leistung die Spannung abgeschaltet.

11.1.3. PoE Powerlimit pro Port

Hier kann pro Port eingestellt werden, welche maximale Leistung ein angeschlossenes Endgerät verbrauchen darf. Bei Überschreiten des eingestellten Powerlimits wird für den betreffenden Port die PoE-Ausgangsspannung abgeschaltet und, bei Firmware-Versionen mit SNMP, ein 'Port PoE Overload Event' gesendet. Durch ein spezielles Messverfahren wird verhindert, dass der Port bereits bei einzelnen Leistungsspitzen abgeschaltet wird.

11.1.4. PoE Input Power Limit

Hier wird eingestellt, welche maximale Gesamtleistung aus dem PoE Powersupply entnommen werden darf. Bei Überschreiten des eingestellten Powerlimits wird, beginnend mit der höchsten Port-Nummer, ein Port nach dem anderen abgeschaltet bis die Leistungsaufnahme wieder innerhalb des Limits liegt. D.h. Port TP-1 hat die höchste Priorität und wird immer als letztes abgeschaltet. Dabei werden aber nur Ports abgeschaltet, die tatsächlich einen PoE Verbraucher angeschlossen haben.

Ferner wird in Falle einer Überlast, bei Firmware-Versionen mit SNMP, ein 'Switch PoE Overload Event' gesendet.

11.1.5. PoE Input Voltage Alarm Limits

Sollte die Spannung des PoE Powersupply unter dem konfigurierten Low Limit absinken bzw. über das konfigurierte Upper Limit ansteigen, so werden alle PoE-Ausgangsspannungen temporär abgeschaltet. Die Einstellung der Ports bleibt dabei unverändert, d.h., dass nachdem die korrekte Spannung wieder anliegt auch die Ports automatisch wieder eingeschaltet werden.

11.1.6. PoE Power Source

Diese Einstellung ist nur für Office Switches verfügbar, die über den TP Uplink Port via PoE gespeist werden können und zusätzlich in der Lage sind einen Teil der Leistung an die angeschlossenen Endgeräte weiterzuleiten. Die betreffenden Switches sind in der Artikelbezeichnung mit dem Zusatz "PD-F" (IEEE802.3af, max. 12,95 Watt) und "PD-F+" (IEEE802.3at, max. 25,5 Watt) gekennzeichnet und können wahlweise über den TP Uplink oder mit einem externen Netzteil gespeist werden. Eine gleichzeitige Speisung über den TP Uplink und einem externen Netzteil ist unzulässig und kann zur Beschädigung des Switches führen.

Folgende Modi stehen hier zur Verfügung:

- 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:

Der Switch wird über den TP Uplink Port mit PoE-Spannung gemäß IEEE802.3af versorgt (max. 12,95 Watt).

Hier wird die maximal zulässige PoE-Leistungsabgabe aller PoE-Ports auf 8 Watt limitiert. Ferner erfolgt vor dem Zuschalten der PoE-Spannung auf den einzelnen Ports eine Überprüfung der Power-Klassen der angeschlossenen PoE-Endgeräte. Vom Switch werden dabei max. zwei Class-1 Endgeräte (2x 3,84 Watt) oder ein einzelnes Class-2 Endgerät (1x 6,49 Watt) zugelassen. Werden mehr Endgeräte mit Class-1 bzw. Class-2 angeschlossen als zulässig, so wird an den betreffenden Ports keine PoE-Spannung aufgeschaltet und die PoE Anzeige-LED leuchtet rot.

AF Power from TP uplink, Max. 2x Class-1 or 2x Class-1 devices allowed:

Dieser Mode ist analog zum vorherigen Mode, jedoch werden bis zu zwei Class-2 Geräte unterstützt. Falls tatsächlich zwei Class-2 Endgeräte angeschlossen werden, muss der Anwender sicherstellen, dass beide Geräte zusammen maximal 8 Watt Leistung aufnehmen. Wird die Leistungsaufnahme überschritten, so kann es evtl. zu einem Hardware-Reboot des Switches kommen, da der speisende Core-Switch die Spannungsversorgung des TP Uplink Ports u.U. wegen Überlast abschaltet.

Als Schutzmaßnahme wird die einstellbare Leistungsgrenze pro Port auf maximal 4 Watt begrenzt. D.h., dass der Switch die Spannung unverzüglich abschaltet, falls die Leistungsaufnahme des Endgerätes 4 Watt überschreitet. Zusätzlich geht der Port in den Fehlerzustand „PoE Overload Failure“ und muss manuell wieder zugeschaltet werden. Je nach Sensibilität des Core-Switches bezüglich kurzzeitiger Überschreitung der maximalen Leistungsabgabe greift u.U. die Schutzschaltung im Core-Switch bevor der Nexans Switch die PoE-Spannung abschalten konnte. Das tatsächliche Zusammenspiel zwischen Core-Switch, Nexans Switch und den angeschlossenen Endgeräten ist im Einzelfall durch Tests vor Ort zu überprüfen.

AT Power from TP uplink, max. 20 W allowed (Port power limits not forced):

Dieser Mode ist nur für Office Switches mit „PD-F+“ PoE+-Adapter verfügbar.

Der Switch wird über den TP Uplink Port mit PoE-Spannung gemäß IEEE802.3at versorgt (max. 25,5 Watt). Hier wird die maximal zulässige PoE-Leistungsabgabe aller PoE-Ports auf 20 Watt limitiert. Ferner erfolgt vor dem Zuschalten der PoE-Spannung auf den einzelnen Ports eine Überprüfung der Power-Klassen der angeschlossenen PoE-Endgeräte. Vom Switch werden dabei Class-1, Class-2 und Class-3 Endgeräte zugelassen. Die Anzahl der akzeptierten Endgeräte ist allein von der resultierenden Gesamtleistungsabgabe abhängig. Wird die PoE-Leistungsabgabe aller PoE-Ports von 20 Watt überschritten, so wird an den betreffenden Ports keine PoE-Spannung aufgeschaltet und die PoE Anzeige-LED leuchtet rot.

AT Power from TP uplink, max. 20 W or 1x Class-4 allowed (Port power limits not forced):

Dieser Mode ist nur für Office Switches mit „PD-F+“ PoE+-Adapter verfügbar.

Dieser Mode ist analog zum vorherigen Mode, jedoch kann alternativ ein Class-4 Gerät angeschlossen werden. Falls tatsächlich ein Class-4 Endgerät angeschlossen wird, muss der Anwender sicherstellen, dass das Gerät maximal 20 Watt Leistung aufnimmt. Wird die Leistungsaufnahme überschritten, so kann es evtl. zu einem Hardware-Reboot des Switches kommen, da der speisende Core-Switch die Spannungsversorgung des TP Uplink Ports u.U. wegen Überlast abschaltet.

Als Schutzmaßnahme schaltet der Switch die Spannung unverzüglich ab, falls die Leistungsaufnahme des Class-4 Geräts 20 Watt überschreitet. Zusätzlich geht der Port in den Fehlerzustand „PoE Overload Failure“ und muss manuell wieder zugeschaltet werden. Je nach Sensibilität des Core-Switches bezüglich kurzzeitiger Überschreitung der maximalen Leistungsabgabe greift jedoch u.U. die Schutzschaltung im Core-Switch bevor der Nexans Switch die PoE-Spannung abschalten konnte. Das tatsächliche Zusammenspiel zwischen Core-Switch, Nexans Switch und den angeschlossenen Endgeräten ist im Einzelfall durch Tests vor Ort zu überprüfen.

External power supply:

Der Switch ist an ein externes Netzteil angeschlossen. Eine Überprüfung der Power-Klassen findet hier nicht statt und die Leistungsbegrenzung erfolgt ausschließlich gemäß der pro Port und Switch eingestellten maximal zulässigen Leistungsaufnahmen.

11.1.7. PoE Reset-Befehl

Durch den PoE Reset-Befehl wird die PoE-Ausgangsspannung für den betreffenden Port für ca. sechs Sekunden abgeschaltet und anschließend automatisch wieder aufgeschaltet.

Diese Funktion ist sehr hilfreich um z.B. einen angeschlossenen Accesspoint neu zu booten.

11.1.8. Programmierung der gelben Port-LEDs beim Desk Switch

Die gelbe Port-LED bei den Desk Switchen kann so programmiert werden, dass diese leuchtet, wenn die PoE-Funktion für den betreffenden Port eingeschaltet ist. Die Einstellung der LEDs hat dabei keinerlei Einfluss auf die Funktion des Ports.

Für die gelbe Status-LED können folgende Einstellungen vorgenommen werden:

- 1) Show Duplex - die LED leuchtet, wenn der Port im Voll-Duplex Betriebszustand ist
- 2) Off - die LED ist dauerhaft aus
- 3) On - die LED ist dauerhaft an
- 4) Show POE - **die LED leuchtet, wenn PoE für den betreffenden Port eingeschaltet ist.**

HINWEIS:

Die Einstellung 4) ist die Factory-Default Einstellung falls ein PoE-Adapter installiert ist.

12. Release Notes

Die Release Notes für den Manager, den Basic Configurator und die Firmware befinden sich ab Release V3.64 in einem separaten Dokument mit der Bezeichnung "**Nexans Switch Management - Release Notes**".

Technische Änderungen vorbehalten



Nexans Netzwerklösungen befinden sich weltweit im Einsatz und haben Ihre Zuverlässigkeit vielfältig bewiesen. Unsere Referenzen schließen führende Firmen der Welt, Energieversorger, Bahngesellschaften, Flughäfen, industrielle Liegenschaften, Häfen und Wasserstraßen ein. Ein LAN System, das mit den Bedürfnissen seiner Benutzer wachsen kann, muss von Beginn an so flexibel konzipiert sein, dass insbesondere häufige Umzüge, Upgrades und Neugestaltungen unterstützt werden.

**Mit der Erfahrung von mehr als 25 Jahren in der
Entwicklung und Produktion von optischen Lösungen
bieten die Systeme von Nexans die Zuverlässigkeit
und die Sicherheit, die Sie von
Ihrem Netzwerk erwarten.**



Nexans Deutschland GmbH • Advanced Networking Solutions

Bonnenbroicher Str. 2-14 • 41238 Mönchengladbach • Tel (0) 2166 27-2985 • Fax (0) 2166 27-2499

E-Mail: sales.ans@nexans.com • www.nexans.de/ans