Reference Manual

Command Line Interface (CLI)
HiSecOS (Global Overview)
The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2020 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at the Hirschmann product site (www.hirschmann.com).

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany
Contents

Safety instructions 20

First login (Password change) 21

About this Manual 22

1 Access Control List (ACL) 23

1.1 mac 23
   1.1.1 mac acl add 23
   1.1.2 mac acl delete 23
   1.1.3 mac acl assign 23
   1.1.4 mac acl deassign 23
   1.1.5 mac acl counter reset 23
   1.1.6 mac acl trapflag 24
   1.1.7 mac acl rule add 24
   1.1.8 mac acl rule delete 24

1.2 ip 25
   1.2.1 ip acl add 25
   1.2.2 ip acl delete 25
   1.2.3 ip acl assign 26
   1.2.4 ip acl deassign 26
   1.2.5 ip acl counter reset 26
   1.2.6 ip acl trapflag 26
   1.2.7 ip acl rule add 26
   1.2.8 ip acl rule delete 26

1.3 show 29
   1.3.1 show access-list trapflag 29
   1.3.2 show access-list mac rules 29
   1.3.3 show access-list mac lists 29
   1.3.4 show access-list mac counters 30
   1.3.5 show access-list mac assignment 30
   1.3.6 show access-list ip rules 30
   1.3.7 show access-list ip lists 30
   1.3.8 show access-list ip counters 30
   1.3.9 show access-list ip assignment 30

2 Application Lists 31

2.1 applists 31
   2.1.1 applists set-authlist 31
   2.1.2 applists enable 31
   2.1.3 applists disable 31

2.2 show 31
   2.2.1 show applists 31

3 Authentication Lists 32

3.1 authlists 32
   3.1.1 authlists add 32
   3.1.2 authlists delete 32
   3.1.3 authlists set-policy 32
   3.1.4 authlists enable 32
   3.1.5 authlists disable 33

3.2 show 33
   3.2.1 show authlists 33

4 Class Of Service 34

4.1 classofservice 34
   4.1.1 classofservice dot1p-mapping 34

4.2 show 34
5 Command Line Interface (CLI)

5.1 cli
   5.1.1 cli serial-timeout
   5.1.2 cli prompt
   5.1.3 cli numlines
   5.1.4 cli banner operation
   5.1.5 cli banner text

5.2 show
   5.2.1 show cli global
   5.2.2 show cli command-tree

5.3 logging
   5.3.1 logging cli-command

5.4 show
   5.4.1 show logging cli-command

6 Clock

6.1 clock
   6.1.1 clock set
   6.1.2 clock timezone offset
   6.1.3 clock timezone zone

6.2 show
   6.2.1 show clock

7 Configuration

7.1 save
   7.1.1 save profile

7.2 config
   7.2.1 config watchdog admin-state
   7.2.2 config watchdog timeout
   7.2.3 config encryption password set
   7.2.4 config encryption password clear
   7.2.5 config envm choose-active
   7.2.6 config envm log-device
   7.2.7 config envm auto-update
   7.2.8 config envm config-save
   7.2.9 config envm load-priority
   7.2.10 config profile select
   7.2.11 config profile delete
   7.2.12 config fingerprint verify nvm profile
   7.2.13 config fingerprint verify nvm num
   7.2.14 config fingerprint verify envm profile
   7.2.15 config fingerprint verify envm num

7.3 copy
   7.3.1 copy sysinfo system envm
   7.3.2 copy sysinfoall system envm
   7.3.3 copy firmware envm
   7.3.4 copy firmware remote
   7.3.5 copy config running-config nvm
   7.3.6 copy config running-config remote
   7.3.7 copy config nvm
   7.3.8 copy config envm
   7.3.9 copy config remote

7.4 clear
   7.4.1 clear config
   7.4.2 clear factory
   7.4.3 clear sfp-white-list

7.5 show
   7.5.1 show running-config
   7.5.2 show running-config xml

7.6 show
7.6.1 show config envm settings
7.6.2 show config envm properties
7.6.3 show config envm active
7.6.4 show config watchdog
7.6.5 show config encryption
7.6.6 show config profiles
7.6.7 show config status
7.7 swap
  7.7.1 swap firmware system backup

8 Device Monitoring

8.1 device-status
  8.1.1 device-status monitor link-failure
  8.1.2 device-status monitor temperature
  8.1.3 device-status monitor envm-removal
  8.1.4 device-status monitor envm-not-in-sync
  8.1.5 device-status monitor power-supply
  8.1.6 device-status trap
8.2 device-status
  8.2.1 device-status link-alarm
8.3 show
  8.3.1 show device-status monitor
  8.3.2 show device-status state
  8.3.3 show device-status trap
  8.3.4 show device-status events
  8.3.5 show device-status link-alarm
  8.3.6 show device-status all

9 Device Security

9.1 security-status
  9.1.1 security-status monitor pwd-change
  9.1.2 security-status monitor pwd-min-length
  9.1.3 security-status monitor pwd-policy-config
  9.1.4 security-status monitor pwd-policy-inactive
  9.1.5 security-status monitor http-enabled
  9.1.6 security-status monitor snmp-unsecure
  9.1.7 security-status monitor sysmon-enabled
  9.1.8 security-status monitor extnvm-upd-enabled
  9.1.9 security-status monitor no-link-enabled
  9.1.10 security-status monitor hidisc-enabled
  9.1.11 security-status monitor extnvm-load-unsecure
  9.1.12 security-status monitor https-certificate
  9.1.13 security-status trap
9.2 security-status
  9.2.1 security-status no-link
9.3 show
  9.3.1 show security-status monitor
  9.3.2 show security-status state
  9.3.3 show security-status no-link
  9.3.4 show security-status trap
  9.3.5 show security-status events
  9.3.6 show security-status all

10 Domain Name System (DNS)

10.1 dns
  10.1.1 dns caching-server adminstate
  10.1.2 dns caching-server flush
  10.1.3 dns client adminstate
  10.1.4 dns client cache adminstate
  10.1.5 dns client servers add
  10.1.6 dns client servers delete
  10.1.7 dns client servers modify
  10.1.8 dns client servers enable
  10.1.9 dns client servers disable
## 12.1.41dpi amp protect-mode

| 12.1.42dpi amp digital-input | 76 |

## 12.2 show

| 12.2.1 show dpi modbus profiletable | 76 |
| 12.2.2 show dpi modbus pending | 77 |
| 12.2.3 show dpi opc profiletable | 77 |
| 12.2.4 show dpi opc pending | 77 |
| 12.2.5 show dpi iec104 profiletable | 77 |
| 12.2.6 show dpi iec104 pending | 77 |
| 12.2.7 show dpi dnp3 profiletable | 77 |
| 12.2.8 show dpi dnp3 pending | 77 |
| 12.2.9 show dpi dnp3 objectlist | 77 |
| 12.2.10 show dpi amp global | 77 |
| 12.2.11 show dpi amp profiletable | 78 |
| 12.2.12 show dpi amp taskcodetable | 78 |

## 13 Filtering Database (FDB)

| 13.1 mac-filter | 79 |
| 13.1.1 mac-filter | 79 |
| 13.2 bridge | 79 |
| 13.2.1 bridge aging-time | 79 |
| 13.3 show | 79 |
| 13.3.1 show mac-filter-table static | 79 |
| 13.4 show | 79 |
| 13.4.1 show bridge aging-time | 79 |
| 13.5 show | 80 |
| 13.5.1 show mac-addr-table | 80 |
| 13.6 clear | 80 |
| 13.6.1 clear mac-addr-table | 80 |

## 14 Firewall Learning Mode (FLM)

| 14.1 flm | 81 |
| 14.1.1 flm operation | 81 |
| 14.1.2 flm action | 81 |
| 14.1.3 flm interface add | 81 |
| 14.1.4 flm interface delete | 81 |
| 14.2 show | 81 |
| 14.2.1 show flm global | 82 |
| 14.2.2 show flm interface | 82 |

## 15 HiDiscovery

| 15.1 network | 83 |
| 15.1.1 network hidiscovery operation | 83 |
| 15.1.2 network hidiscovery mode | 83 |
| 15.1.3 network hidiscovery blinking | 83 |
| 15.2 show | 83 |
| 15.2.1 show network hidiscovery | 83 |

## 16 Hypertext Transfer Protocol (HTTP)

| 16.1 http | 84 |
| 16.1.1 http port | 84 |
| 16.1.2 http server | 84 |
| 16.2 show | 84 |
| 16.2.1 show http | 84 |

## 17 HTTP Secure (HTTPS)

| 17.1 https | 85 |
| 17.1.1 https server | 85 |
| 17.1.2 https port | 85 |
| 17.1.3 https fingerprint-type | 85 |
17.1.4 https certificate 85
17.2 copy 85
  17.2.1 copy https cert remote 85
  17.2.2 copy https cert envm 86
17.3 show 86
  17.3.1 show https 86

18 Interface 87
  18.1 shutdown 87
    18.1.1 shutdown 87
  18.2 auto-negotiate 87
    18.2.1 auto-negotiate 87
  18.3 auto-power-down 87
    18.3.1 auto-power-down 87
  18.4 cable-crossing 88
    18.4.1 cable-crossing 88
  18.5 linktraps 88
    18.5.1 linktraps 88
  18.6 speed 88
    18.6.1 speed 88
  18.7 name 88
    18.7.1 name 88
  18.8 power-state 89
    18.8.1 power-state 89
  18.9 mac-filter 89
    18.9.1 mac-filter 89
  18.10 show 89
    18.10.1 show port 89
  18.11 show 89
  18.12 show 90

19 Interface Statistics 91
  19.1 utilization 91
    19.1.1 utilization control-interval 91
    19.1.2 utilization alarm-threshold lower 91
    19.1.3 utilization alarm-threshold upper 91
  19.2 clear 91
    19.2.1 clear port-statistics 91
  19.3 show 91
    19.3.1 show interface counters 91
    19.3.2 show interface statistics 92
    19.3.3 show interface ether-stats 92

20 Intern 93
  20.1 help 93
  20.2 logout 93
  20.3 history 93
  20.4 vlan 93
    20.4.1 vlan database 93
  20.5 vlan-mode 93
    20.5.1 vlan-mode 93
  20.6 exit 94
  20.7 end 94
  20.8 serviceshell 94
    20.8.1 serviceshell start 94
20.8.2 serviceshell deactivate 94
20.9 traceroute 94
20.10 traceroute
  20.10.1 traceroute source 94
20.11 reboot 95
20.12 ping
  20.12.1 ping count 95
20.13 ping
  20.13.1 ping source 95
20.14 show
  20.14.1 show serviceshell 95

21 Intrusion Detection System (IDS) 96
21.1 ids
  21.1.1 ids operation 96
  21.1.2 ids user 96
21.2 show
  21.2.1 show ids global 96

22 Open Shortest Path First (OSPF) 97
22.1 ip
  22.1.1 ip ospf area 97
  22.1.2 ip ospf trapflags all 99
  22.1.3 ip ospf operation 99
  22.1.4 ip ospf 1583 compatibility 99
  22.1.5 ip ospf default-metric 99
  22.1.6 ip ospf router-id 100
  22.1.7 ip ospf external-lsdb-limit 100
  22.1.8 ip ospf exit-overflow 100
  22.1.9 ip ospf maximum-path 100
  22.1.10 ip ospf spf-delay 100
  22.1.11 ip ospf spf-holdtime 100
  22.1.12 ip ospf auto-cost 101
  22.1.13 ip ospf distance intra 101
  22.1.14 ip ospf distance inter 101
  22.1.15 ip ospf distance external 101
  22.1.16 ip ospf re-distribute 101
  22.1.17 ip ospf distribute-list 102
  22.1.18 ip ospf default-info originate 102
22.2 ip
  22.2.1 ip ospf operation 102
  22.2.2 ip ospf area-id 103
  22.2.3 ip ospf link-type 103
  22.2.4 ip ospf priority 103
  22.2.5 ip ospf transmit-delay 103
  22.2.6 ip ospf retransmit-interval 103
  22.2.7 ip ospf hello-interval 103
  22.2.8 ip ospf dead-interval 104
  22.2.9 ip ospf cost 104
  22.2.10 ip ospf mtu-ignore 104
  22.2.11 ip ospf authentication type 104
  22.2.12 ip ospf authentication key 104
  22.2.13 ip ospf authentication key-id 104
22.3 show
  22.3.1 show ip ospf global 105
  22.3.2 show ip ospf area 105
  22.3.3 show ip ospf stub 105
  22.3.4 show ip ospf database internal 105
  22.3.5 show ip ospf database external 105
  22.3.6 show ip ospf range 105
  22.3.7 show ip ospf interface 105
  22.3.8 show ip ospf virtual-link 105
  22.3.9 show ip ospf virtual-neighbor 106
22.3.10 show ip ospf neighbor
22.3.11 show ip ospf statistics
22.3.12 show ip ospf re-distribute
22.3.13 show ip ospf nssa
22.3.14 show ip ospf route

23 Virtual Router Redundancy Protocol (VRRP) 107

23.1 ip
23.1.1 ip vrrp operation
23.1.2 ip vrrp trap auth-failure
23.1.3 ip vrrp trap new-master

23.2 ip
23.2.1 ip vrrp add
23.2.2 ip vrrp modify
23.2.3 ip vrrp delete
23.2.4 ip vrrp enable
23.2.5 ip vrrp disable
23.2.6 ip vrrp virtual-address add
23.2.7 ip vrrp virtual-address delete
23.2.8 ip vrrp track add
23.2.9 ip vrrp track modify
23.2.10 ip vrrp track delete

23.3 show
23.3.1 show ip vrrp interface
23.3.2 show ip vrrp global

24 Address Resolution Protocol (IP ARP) 110

24.1 ip
24.1.1 ip arp add
24.1.2 ip arp delete
24.1.3 ip arp enable
24.1.4 ip arp disable
24.1.5 ip arp timeout
24.1.6 ip arp response-time
24.1.7 ip arp retries

24.2 show
24.2.1 show ip arp info
24.2.2 show ip arp table
24.2.3 show ip arp static
24.2.4 show ip arp entry

24.3 clear
24.3.1 clear ip arp-cache

25 Internet Protocol Version 4 (IPv4) 112

25.1 network
25.1.1 network parms

25.2 clear
25.2.1 clear arp-table-switch

25.3 show
25.3.1 show network parms

25.4 show
25.4.1 show arp

26 Link Layer Discovery Protocol (LLDP) 113

26.1 lldp
26.1.1 lldp operation
26.1.2 lldp config chassis admin-state
26.1.3 lldp config chassis notification-interval
26.1.4 lldp config chassis re-init-delay
26.1.5 lldp config chassis tx-delay
26.1.6 lldp config chassis tx-hold-multiplier
26.1.7 lldp config chassis tx-interval
26.2 show
26.2.1 show lldp global
26.2.2 show lldp port
26.2.3 show lldp remote-data

26.3 lldp
26.3.1 lldp admin-state
26.3.2 lldp fdb-mode
26.3.3 lldp max-neighbors
26.3.4 lldp notification
26.3.5 lldp tlv mac-phy-config-state
26.3.6 lldp tlv max-frame-size
26.3.7 lldp tlv mgmt-addr
26.3.8 lldp tlv port-desc
26.3.9 lldp tlv port-vlan
26.3.10 lldp tlv protocol
26.3.11 lldp tlv sys-cap
26.3.12 lldp tlv sys-desc
26.3.13 lldp tlv sys-name
26.3.14 lldp tlv vlan-name
26.3.15 lldp tlv protocol-based-vlan

27 Logging

27.1 logging
27.1.1 logging audit-trail
27.1.2 logging buffered severity
27.1.3 logging host add
27.1.4 logging host delete
27.1.5 logging host enable
27.1.6 logging host disable
27.1.7 logging host modify
27.1.8 logging syslog operation
27.1.9 logging current-console operation
27.1.10 logging current-console severity
27.1.11 logging console operation
27.1.12 logging console severity
27.1.13 logging persistent operation
27.1.14 logging persistent numfiles
27.1.15 logging persistent filesize
27.1.16 logging persistent severity-level

27.2 show
27.2.1 show logging buffered
27.2.2 show logging traplogs
27.2.3 show logging console
27.2.4 show logging persistent
27.2.5 show logging syslog
27.2.6 show logging host

27.3 copy
27.3.1 copy eventlog buffered envm
27.3.2 copy eventlog buffered remote
27.3.3 copy eventlog persistent
27.3.4 copy traplog system envm
27.3.5 copy traplog system remote
27.3.6 copy audittrail system envm
27.3.7 copy audittrail system remote

27.4 clear
27.4.1 clear logging buffered
27.4.2 clear logging persistent
27.4.3 clear eventlog

28 Management Access

28.1 network
28.1.1 network management access web timeout
28.1.2 network management access add
28.1.3 network management access delete
28.1.4 network management access modify
Contents

28.1.5 network management access operation 128
28.1.6 network management access status 128

28.2 show 128
28.2.1 show network management access global 128
28.2.2 show network management access rules 128

29 Network Address Translation (NAT) 129

29.1 nat 129
29.1.1 nat dnat commit 129
29.1.2 nat dnat add 129
29.1.3 nat dnat modify 129
29.1.4 nat dnat delete 130
29.1.5 nat dnat logtrap 130
29.1.6 nat dnat state 130
29.1.7 nat dnat if add 131
29.1.8 nat dnat if delete 131
29.1.9 nat 1to1nat commit 131
29.1.10nat 1to1nat add 131
29.1.11nat 1to1nat modify 131
29.1.12nat 1to1nat delete 132
29.1.13nat 1to1nat logtrap 132
29.1.14nat 1to1nat state 132
29.1.15nat masq commit 132
29.1.16nat masq add 132
29.1.17nat masq modify 133
29.1.18nat masq delete 133
29.1.19nat masq logtrap 133
29.1.20nat masq ipsec-exempt 133
29.1.21nat masq state 133
29.1.22nat masq if add 134
29.1.23nat masq if delete 134
29.1.24nat doublenat commit 134
29.1.25nat doublenat add 134
29.1.26nat doublenat modify 134
29.1.27nat doublenat delete 134
29.1.28nat doublenat logtrap 135
29.1.29nat doublenat state 135
29.1.30nat doublenat if add 135
29.1.31nat doublenat if delete 135

29.2 show 135
29.2.1 show nat dnat global 135
29.2.2 show nat dnat rules 136
29.2.3 show nat dnat if 136
29.2.4 show nat dnat logtrap 136
29.2.5 show nat masq global 136
29.2.6 show nat masq rules 136
29.2.7 show nat masq logtrap 136
29.2.8 show nat masq if 136
29.2.9 show nat 1to1nat global 136
29.2.10show nat 1to1nat rules 137
29.2.11show nat 1to1nat logtrap 137
29.2.12show nat doublenat global 137
29.2.13show nat doublenat rules 137
29.2.14show nat doublenat logtrap 137
29.2.15show nat doublenat if 137

30 Network Time Protocol (NTP) 138

30.1 ntp 138
30.1.1 ntp client operation 138
30.1.2 ntp client operating-mode 138
30.1.3 ntp server operation 138
30.1.4 ntp server operating-mode 138
30.1.5 ntp server localclock-stratum 138
30.1.6 ntp peers add 138
30.1.7 ntp peers delete 139

30.2 show 139
30.2.1 show ntp client-status 139
30.2.2 show ntp server-status 139

31 Packet Filter 140

31.1 packet-filter 140
  31.1.1 packet-filter l3 commit 140
  31.1.2 packet-filter l3 defaultpolicy 140
  31.1.3 packet-filter l3 checksum-validation 140
  31.1.4 packet-filter l3 addrule 140
  31.1.5 packet-filter l3 modifyrule 141
  31.1.6 packet-filter l3 delrule 141
  31.1.7 packet-filter l3 enablerule 141
  31.1.8 packet-filter l3 disablerule 142
  31.1.9 packet-filter l3 logmode 142
  31.1.10 packet-filter l3 addif 142
  31.1.11 packet-filter l3 delif 142
  31.1.12 packet-filter l3 enableif 142
  31.1.13 packet-filter l3 disableif 143
  31.1.14 packet-filter l2 commit 143
  31.1.15 packet-filter l2 defaultpolicy 143
  31.1.16 packet-filter l2 fcs-validation 143
  31.1.17 packet-filter l2 rule add 143
  31.1.18 packet-filter l2 rule modify 145
  31.1.19 packet-filter l2 rule delete 146
  31.1.20 packet-filter l2 rule enable 146
  31.1.21 packet-filter l2 rule disable 146
  31.1.22 packet-filter l2 if add 146
  31.1.23 packet-filter l2 if delete 147
  31.1.24 packet-filter l2 if enable 147
  31.1.25 packet-filter l2 if disable 147

31.2 clear 147
  31.2.1 clear fw-state-table 147

31.3 show 148
  31.3.1 show packet-filter l3 global 148
  31.3.2 show packet-filter l3 maxrules 148
  31.3.3 show packet-filter l3 defaultpolicy 148
  31.3.4 show packet-filter l3 ruletable 148
  31.3.5 show packet-filter l3 iftable 148
  31.3.6 show packet-filter l3 pending 148
  31.3.7 show packet-filter l2 global 148
  31.3.8 show packet-filter l2 rule 148
  31.3.9 show packet-filter l2 if 148

32 Password Management 149

32.1 passwords 149
  32.1.1 passwords min-length 149
  32.1.2 passwords max-login-attempts 149
  32.1.3 passwords min-uppercase-chars 149
  32.1.4 passwords min-lowercase-chars 149
  32.1.5 passwords min-numeric-chars 149
  32.1.6 passwords min-special-chars 149
  32.1.7 passwords login-attempt-period 150

32.2 show 150
  32.2.1 show passwords 150

33 Radius 151

33.1 radius 151
  33.1.1 radius server attribute 4 151
  33.1.2 radius server auth add 151
  33.1.3 radius server auth delete 151
  33.1.4 radius server auth modify 151
  33.1.5 radius server retransmit 152
  33.1.6 radius server timeout 152

33.2 show 152
  33.2.1 show radius global 152
  33.2.2 show radius auth servers 152
34 Remote Authentication 154

34.1 ldap 154
34.1.1 ldap operation 154
34.1.2 ldap cache-timeout 154
34.1.3 ldap flush-user-cache 154
34.1.4 ldap role-policy 154
34.1.5 ldap basedn 154
34.1.6 ldap search-attr 154
34.1.7 ldap bind-user 155
34.1.8 ldap bind-passwd 155
34.1.9 ldap default-domain 155
34.1.10 ldap client server add 155
34.1.11 ldap client server delete 155
34.1.12 ldap client server enable 155
34.1.13 ldap client server disable 156
34.1.14 ldap client server modify 156
34.1.15 ldap mapping add 156
34.1.16 ldap mapping delete 156
34.1.17 ldap mapping enable 156
34.1.18 ldap mapping disable 157

34.2 show 157
34.2.1 show ldap global 157
34.2.2 show ldap client server 157
34.2.3 show ldap mapping 157

34.3 copy 157
34.3.1 copy ldapcacert remote 157
34.3.2 copy ldapcacert envm 157

35 Remote Monitoring (RMON) 159

35.1 show 159
35.1.1 show rmon statistics 159

36 Script File 160

36.1 script 160
36.1.1 script apply 160
36.1.2 script validate 160
36.1.3 script list system 160
36.1.4 script list envm 160
36.1.5 script delete 160

36.2 copy 160
36.2.1 copy script envm 160
36.2.2 copy script remote 161
36.2.3 copy script nvm 161

36.3 show 161
36.3.1 show script envm 161
36.3.2 show script system 161

37 Selftest 162

37.1 selftest 162
37.1.1 selftest action 162
37.1.2 selftest ramtest 162
37.1.3 selftest system-monitor 162
37.1.4 selftest boot-default-on-error 162

37.2 show 163
37.2.1 show selftest action 163
37.2.2 show selftest settings 163

38 Small Form-factor Pluggable (SFP) 164
38.1 show
   38.1.1 show sfp 164

39 Signal Contact 165
39.1 signal-contact
   39.1.1 signal-contact mode 165
   39.1.2 signal-contact monitor link-failure 165
   39.1.3 signal-contact monitor envm-not-in-sync 165
   39.1.4 signal-contact monitor envm-removal 165
   39.1.5 signal-contact monitor temperature 166
   39.1.6 signal-contact monitor power-supply 166
   39.1.7 signal-contact state 166
   39.1.8 signal-contact trap 166
39.2 signal-contact
   39.2.1 signal-contact link-alarm 167
39.3 show
   39.3.1 show signal-contact 167

40 Simple Network Management Protocol (SNMP) 168
40.1 snmp
   40.1.1 snmp access version v1 168
   40.1.2 snmp access version v2 168
   40.1.3 snmp access version v3 168
   40.1.4 snmp access port 168
40.2 show
   40.2.1 show snmp access 169

41 SNMP Community 170
41.1 snmp
   41.1.1 snmp community ro 170
   41.1.2 snmp community rw 170
41.2 show
   41.2.1 show snmp community 170

42 SNMP Logging 171
42.1 logging
   42.1.1 logging snmp-request get operation 171
   42.1.2 logging snmp-request get severity 171
   42.1.3 logging snmp-request set operation 171
   42.1.4 logging snmp-request set severity 172
42.2 show
   42.2.1 show logging snmp 172

43 Secure Shell (SSH) 173
43.1 ssh
   43.1.1 ssh server 173
   43.1.2 ssh timeout 173
   43.1.3 ssh port 173
   43.1.4 ssh max-sessions 173
   43.1.5 ssh key rsa 173
   43.1.6 ssh key fingerprint-type 173
43.2 copy
   43.2.1 copy sshkey remote 174
   43.2.2 copy sshkey envm 174
43.3 show
   43.3.1 show ssh 174

44 Storm Control 175
44.1 storm-control 175
44.1.1 storm-control flow-control 175

44.2 storm-control 175
  44.2.1 storm-control flow-control 175
  44.2.2 storm-control ingress unit 175
  44.2.3 storm-control ingress unicast operation 175
  44.2.4 storm-control ingress unicast threshold 176
  44.2.5 storm-control ingress multicast operation 176
  44.2.6 storm-control ingress multicast threshold 176
  44.2.7 storm-control ingress broadcast operation 176
  44.2.8 storm-control ingress broadcast threshold 176

44.3 show 176
  44.3.1 show storm-control flow-control 177
  44.3.2 show storm-control ingress 177

45 System 178
  45.1 system 178
    45.1.1 system name 178
    45.1.2 system location 178
    45.1.3 system contact 178
    45.1.4 system pre-login-banner operation 178
    45.1.5 system pre-login-banner text 178
    45.1.6 system resources operation 179
  45.2 temperature 179
    45.2.1 temperature upper-limit 179
    45.2.2 temperature lower-limit 179
  45.3 show 179
    45.3.1 show eventlog 179
    45.3.2 show system info 179
    45.3.3 show system pre-login-banner 179
    45.3.4 show system flash-status 180
    45.3.5 show system temperature limits 180
    45.3.6 show system temperature extremes 180
    45.3.7 show system temperature histogram 180
    45.3.8 show system temperature counters 180
    45.3.9 show system resources 180
    45.3.10 show hardware by-pass 180

46 Tracking 181
  46.1 track 181
    46.1.1 track add 181
    46.1.2 track delete 181
    46.1.3 track enable 181
    46.1.4 track disable 181
    46.1.5 track trap 181
    46.1.6 track description 182
    46.1.7 track modify interface 182
    46.1.8 track modify ping 182
    46.1.9 track modify logical 183
  46.2 show 183
    46.2.1 show track overview 183
    46.2.2 show track interface 183
    46.2.3 show track ping 183
    46.2.4 show track logical 183
    46.2.5 show track application 183

47 L3 Relay 184
  47.1 ip 184
    47.1.1 ip udp-helper operation 184
    47.1.2 ip udp-helper server add 184
    47.1.3 ip udp-helper server delete 184
    47.1.4 ip udp-helper server enable 184
    47.1.5 ip udp-helper server disable 184
    47.1.6 ip udp-helper maxhopcount 185
    47.1.7 ip udp-helper minwaittime 185
47.1.8 ip udp-helper cidoptmode 185
47.2 ip 185
  47.2.1 ip udp-helper server add 185
  47.2.2 ip udp-helper server delete 185
  47.2.3 ip udp-helper server enable 186
  47.2.4 ip udp-helper server disable 186
47.3 show 186
  47.3.1 show ip udp-helper status 186
  47.3.2 show ip udp-helper global 186
  47.3.3 show ip udp-helper interface 186
  47.3.4 show ip udp-helper statistics 186
47.4 clear 186
  47.4.1 clear ip udp-helper 187
48 Traps 188
  48.1 snmp 188
    48.1.1 snmp trap operation 188
    48.1.2 snmp trap mode 188
    48.1.3 snmp trap delete 188
    48.1.4 snmp trap add 188
  48.2 show 188
    48.2.1 show snmp traps 189
49 Unicast Routing 190
  49.1 routing 190
    49.1.1 routing add 190
    49.1.2 routing delete 190
  49.2 ip 190
    49.2.1 ip routing 190
    49.2.2 ip proxy-arp max-delay 190
  49.3 show 190
    49.3.1 show ip global 191
  49.4 show 191
    49.4.1 show ip interface 191
    49.4.2 show ip statistics 191
  49.5 ip 191
    49.5.1 ip routing 191
    49.5.2 ip proxy-arp operation 191
    49.5.3 ip address secondary 192
    49.5.4 ip address primary 192
    49.5.5 ip mtu 192
    49.5.6 ip icmp redirects 192
  49.6 ip 192
    49.6.1 ip route add 193
    49.6.2 ip route modify 193
    49.6.3 ip route delete 193
    49.6.4 ip route distance 193
    49.6.5 ip route track add 193
    49.6.6 ip route track delete 193
    49.6.7 ip default-route add 194
    49.6.8 ip default-route modify 194
    49.6.9 ip default-route delete 194
    49.6.10 ip default-route track add 194
    49.6.11 ip default-route track delete 194
    49.6.12 ip loopback add 194
    49.6.13 ip loopback delete 195
    49.6.14 ip icmp redirects 195
    49.6.15 ip icmp echo-reply 195
    49.6.16 ip icmp rate-limit interval 195
    49.6.17 ip icmp rate-limit burst-size 195
  49.7 show 195
    49.7.1 show ip route all 195
    49.7.2 show ip route local 196
50 Users 197
50.1 users 197
50.1.1 users add 197
50.1.2 users delete 197
50.1.3 users enable 197
50.1.4 users disable 197
50.1.5 users password 197
50.1.6 users snmpv3 authentication 197
50.1.7 users snmpv3 encryption 198
50.1.8 users access-role 198
50.1.9 users lock-status 198
50.1.10 users password-policy-check 198
50.2 show users 198
50.2.1 show users 198

51 Virtual LAN (VLAN) 199
51.1 name 199
51.1.1 name 199
51.2 vlan 199
51.2.1 vlan add 199
51.2.2 vlan delete 199
51.3 vlan 199
51.3.1 vlan acceptframe 199
51.3.2 vlan ingressfilter 199
51.3.3 vlan priority 200
51.3.4 vlan pvid 200
51.3.5 vlan tagging 200
51.3.6 vlan participation include 200
51.3.7 vlan participation exclude 200
51.3.8 vlan participation auto 200
51.4 show vlan 201
51.4.1 show vlan id 201
51.4.2 show vlan brief 201
51.4.3 show vlan port 201
51.4.4 show vlan member current 201
51.4.5 show vlan member static 201
51.5 network 201
51.5.1 network management vlan 201
51.5.2 network management priority dot1p 201
51.5.3 network management priority ip-dscp 202

52 Virtual Private Network (VPN) 203
52.1 ipsec 203
52.1.1 ipsec certificate delete 203
52.1.2 ipsec certificate upload passphrase 203
52.1.3 ipsec connection add 203
52.1.4 ipsec connection modify 203
52.1.5 ipsec connection status 206
52.1.6 ipsec connection delete 206
52.1.7 ipsec traffic-selector 206
52.2 show ipsec 207
52.2.1 show ipsec general 207
52.2.2 show ipsec connections summary 207
52.2.3 show ipsec connections access 207
52.2.4 show ipsec connections certificates 208
52.2.5 show ipsec connections key-exchange 208
52.2.6 show ipsec connections data-exchange 208
52.2.7 show ipsec connections status 208
52.2.8 show ipsec connections tunnels 208
# Safety instructions

<table>
<thead>
<tr>
<th>WARNING</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UNCONTROLLED MACHINE ACTIONS</strong></td>
</tr>
<tr>
<td>To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually. Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all data transmission devices.</td>
</tr>
<tr>
<td>Failure to follow these instructions can result in death, serious injury, or equipment damage.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WARNING</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UNWANTED APPLICATION BEHAVIOR</strong></td>
</tr>
<tr>
<td>Configuration of the Ethernet devices shall be done by an Ethernet expert. Before you start any application based on an AFS and/or AFF network, be sure to complete the configuration of all Ethernet devices correctly.</td>
</tr>
<tr>
<td>Failure to follow these instructions can result in equipment damage, serious injury or even death.</td>
</tr>
</tbody>
</table>
First login (Password change)

To help prevent undesired access to the device, it is imperative that you change the default password during initial setup.

Perform the following steps:
- Open the Graphical User Interface, the Command Line Interface, or HiView the first time you log on to the device.
- Log on to the device with the default password.
  - The device prompts you to type in a new password.
- Type in your new password.
  - To help increase security, choose a password that contains at least 8 characters which includes upper-case characters, lower-case characters, numerical digits, and special characters.
- The device prompts you to confirm your new password.
- Log on to the device again with your new password.

Note: If you lost your password, then use the System Monitor to reset the password.

For further information see: hirschmann-support.belden.com.
About this Manual

The “Installation” user manual contains a device description, safety instructions, a description of the display, and the other information that you need to install the device.

The “Configuration” user manual contains the information you need to start operating the device. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.

The “Graphical User Interface” reference manual contains detailed information on using the graphical user interface to operate the individual functions of the device.

The “Command Line Interface” reference manual contains detailed information on using the Command Line Interface to operate the individual functions of the device.

The Industrial HiVision Network Management software provides you with additional options for smooth configuration and monitoring:
- Auto-topology discovery
- Browser interface
- Client/server structure
- Event handling
- Event log
- Simultaneous configuration of multiple devices
- Graphical user interface with network layout
- SNMP/OPC gateway
1 Access Control List (ACL)

1.1 mac

Set MAC parameters.

1.1.1 mac acl add

Create a new MAC ACL

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `mac acl add <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..10100</td>
<td>MAC ACL ID</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter an ACL name, alphanumeric ASCII character string with 1 to 32 characters.</td>
</tr>
</tbody>
</table>

1.1.2 mac acl delete

Delete an existing MAC ACL.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `mac acl delete <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..10100</td>
<td>MAC ACL ID</td>
</tr>
</tbody>
</table>

1.1.3 mac acl assign

Assign a MAC ACL to a VLAN.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `mac acl assign <P-1> vlan <P-2> <P-3> <P-4>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..10100</td>
<td>MAC ACL ID</td>
</tr>
<tr>
<td>P-2</td>
<td>0..4095</td>
<td>Enter a VLAN ID in the given range.</td>
</tr>
<tr>
<td>P-3</td>
<td>in</td>
<td>Incoming traffic</td>
</tr>
<tr>
<td>P-4</td>
<td>1..4294967295</td>
<td>Sequence</td>
</tr>
</tbody>
</table>

1.1.4 mac acl deassign

Deassign a MAC ACL from a VLAN.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `mac acl deassign <P-1> vlan <P-2> <P-3> <P-4>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..10100</td>
<td>MAC ACL ID</td>
</tr>
<tr>
<td>P-2</td>
<td>0..4095</td>
<td>Enter a VLAN ID in the given range.</td>
</tr>
<tr>
<td>P-3</td>
<td>in</td>
<td>Incoming traffic</td>
</tr>
<tr>
<td>P-4</td>
<td>1..4294967295</td>
<td>Sequence</td>
</tr>
</tbody>
</table>

1.1.5 mac acl counter reset

Reset the counter for one or all MAC ACL rules.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `mac acl counter reset [<P-1>] [<P-2>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..10100</td>
<td>MAC ACL ID</td>
</tr>
<tr>
<td>P-2</td>
<td>1..239</td>
<td>MAC ACL Rule ID</td>
</tr>
</tbody>
</table>
1.1.6 mac acl trapflag
Change the trap flag.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** mac acl trapflag <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

1.1.7 mac acl rule add
Add a rule to an existing MAC ACL.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** mac acl rule add <P-1> <P-2> permit src <P-3> <P-4> dst <P-5> <P-6> [etype <P-7>] [vlan <P-8>] [cos <P-9>] [log] deny src <P-10> <P-11> dst <P-12> <P-13> [etype <P-14>] [vlan <P-15>] [cos <P-16>] [log]

**permit:** Add a permit rule.
src: Specify the src MAC address/mask.
dst: Specify the dst MAC address/mask.
[etype]: Ethertype
[vlan]: Specify a VLAN to match.
[cos]: Specify a COS to match.
[log]: Enable Logging

deny: Add a deny rule.
src: Specify the src MAC address/mask.
dst: Specify the dst MAC address/mask.
[etype]: Ethertype
[vlan]: Specify a VLAN to match.
[cos]: Specify a COS to match.
[log]: Enable Logging

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..10100</td>
<td>MAC ACL ID</td>
</tr>
<tr>
<td>P-2</td>
<td>1..239</td>
<td>MAC ACL Rule ID</td>
</tr>
<tr>
<td>P-3</td>
<td>any</td>
<td>Enter any as a shortcut for the MAC address 00:00:00:00:00:00.</td>
</tr>
<tr>
<td></td>
<td>aa:bb:cc:dd:ee:ff</td>
<td>Enter the MAC address in hexadecimal format.</td>
</tr>
<tr>
<td>P-4</td>
<td>any</td>
<td>Enter any as a shortcut for the MAC address 00:00:00:00:00:00.</td>
</tr>
<tr>
<td></td>
<td>aa:bb:cc:dd:ee:ff</td>
<td>Enter the MAC mask in hexadecimal format. The 'Don't care bits' are represented by binary 0's and 'Do care bits' are represented by binary 1's.</td>
</tr>
<tr>
<td>P-5</td>
<td>any</td>
<td>Enter any as a shortcut for the MAC address 00:00:00:00:00:00.</td>
</tr>
<tr>
<td></td>
<td>aa:bb:cc:dd:ee:ff</td>
<td>Enter the MAC address in hexadecimal format.</td>
</tr>
<tr>
<td>P-6</td>
<td>any</td>
<td>Enter any as a shortcut for the MAC address 00:00:00:00:00:00.</td>
</tr>
<tr>
<td></td>
<td>aa:bb:cc:dd:ee:ff</td>
<td>Enter the MAC mask in hexadecimal format. The 'Don't care bits' are represented by binary 0's and 'Do care bits' are represented by binary 1's.</td>
</tr>
<tr>
<td>P-7</td>
<td>0x0600-0xffff</td>
<td>Ethertype value</td>
</tr>
<tr>
<td></td>
<td>appletalk</td>
<td>Appletalk</td>
</tr>
<tr>
<td></td>
<td>arp</td>
<td>ARP</td>
</tr>
<tr>
<td></td>
<td>ibmsna</td>
<td>IBM SNA</td>
</tr>
<tr>
<td></td>
<td>ipv4</td>
<td>IPv4</td>
</tr>
<tr>
<td></td>
<td>ipv6</td>
<td>IPv6</td>
</tr>
<tr>
<td></td>
<td>ipx-old</td>
<td>IPX (old)</td>
</tr>
<tr>
<td></td>
<td>mpls-mcast</td>
<td>MPLS Multicast</td>
</tr>
<tr>
<td></td>
<td>mpls-ucast</td>
<td>MPLS Unicast</td>
</tr>
<tr>
<td></td>
<td>netbios</td>
<td>NetBIOS</td>
</tr>
<tr>
<td></td>
<td>novell</td>
<td>Novell</td>
</tr>
<tr>
<td></td>
<td>pppoe-disc</td>
<td>PPPoE Discovery Stage</td>
</tr>
<tr>
<td></td>
<td>rarp</td>
<td>RARP</td>
</tr>
<tr>
<td></td>
<td>pppoe-sess</td>
<td>PPPoE Session Stage</td>
</tr>
<tr>
<td></td>
<td>ipx-new</td>
<td>IPX (new)</td>
</tr>
<tr>
<td></td>
<td>powerlink</td>
<td>POWERLINK</td>
</tr>
<tr>
<td></td>
<td>profinet</td>
<td>PROFINET</td>
</tr>
<tr>
<td></td>
<td>ethercat</td>
<td>EtherCAT</td>
</tr>
<tr>
<td>P-8</td>
<td>0..4095</td>
<td>Enter a VLAN ID in the given range.</td>
</tr>
<tr>
<td>P-9</td>
<td>1..7</td>
<td>Enter a COS in the given range.</td>
</tr>
</tbody>
</table>
### 1.2 ip

Set IP parameters.

#### 1.2.1 ip acl add

Create a new IP ACL.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip acl add \(<P-1>\) \(<P-2>\)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..10100</td>
<td>IP ACL ID</td>
</tr>
<tr>
<td>P-2</td>
<td>1..239</td>
<td>MAC ACL Rule ID</td>
</tr>
</tbody>
</table>

#### 1.2.2 ip acl delete

Delete an existing IP ACL.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip acl delete \(<P-1>\)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..10100</td>
<td>IP ACL ID</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter an ACL name, alphanumeric ASCII character string with 1 to 32 characters.</td>
</tr>
</tbody>
</table>
1.2.3  ip acl assign
Assign an IP ACL to a VLAN.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip acl assign <P-1> vlan <P-2> <P-3> <P-4>

vlan: Specify a VLAN.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..10100</td>
<td>IP ACL ID</td>
</tr>
<tr>
<td>P-2</td>
<td>vlan</td>
<td>Specify VLAN</td>
</tr>
<tr>
<td>P-3</td>
<td>0..4095</td>
<td>Enter a VLAN ID in the given range.</td>
</tr>
<tr>
<td>P-4</td>
<td>in</td>
<td>Incoming traffic</td>
</tr>
<tr>
<td>P-5</td>
<td>1..4294967295</td>
<td>Sequence</td>
</tr>
</tbody>
</table>

1.2.4  ip acl deassign
Remove an IP ACL from a VLAN.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip acl deassign <P-1> vlan <P-2> <P-3> <P-4>

vlan: Specify a VLAN.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..10100</td>
<td>IP ACL ID</td>
</tr>
<tr>
<td>P-2</td>
<td>vlan</td>
<td>Specify VLAN</td>
</tr>
<tr>
<td>P-3</td>
<td>0..4095</td>
<td>Enter a VLAN ID in the given range.</td>
</tr>
<tr>
<td>P-4</td>
<td>in</td>
<td>Incoming traffic</td>
</tr>
<tr>
<td>P-5</td>
<td>1..4294967295</td>
<td>Sequence</td>
</tr>
</tbody>
</table>

1.2.5  ip acl counter reset
Reset the counter for one or all IP ACL rules.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip acl counter reset [P-1] [P-2]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..10100</td>
<td>IP ACL ID</td>
</tr>
<tr>
<td>P-2</td>
<td>1..239</td>
<td>IP ACL Rule ID</td>
</tr>
</tbody>
</table>

1.2.6  ip acl trapflag
Change a trap flag.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip acl trapflag <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

1.2.7  ip acl rule add
Add a rule to an existing IP ACL.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip acl rule add <P-1> <P-2> permit src <P-3> <P-4> [sport <P-5>] dst <P-6> [<P-7>] [dport <P-8>] [proto <P-9>] [fragments] [log] [dscp <P-10>] [mirror <P-11>] [redirect <P-12>] [rate-limit <P-13> <P-14> <P-15> [tos <P-16> <P-17> [mirror <P-18> [redirect <P-19> [rate-limit <P-20> <P-21> <P-22> [precedence <P-23> [mirror <P-24> [redirect <P-25> [rate-limit <P-26> <P-27> <P-28> deny src <P-29> <P-30> [sport <P-31>] dst <P-32> <P-33> [dport <P-34> [proto <P-35> [fragments] [log] [dscp <P-36>] [tos <P-37> <P-38> [precedence <P-39>]]]

permit: Add a permit rule to an existing IP ACL.
src: Specify the source IP/mask.
sport: Specify the source L4 port.
**Access Control List (ACL)**

1.2 ip

**HiSecOS**

**Release 04.2.01 12/2021**

dst: Specify the destination IP/mask.

[dport]: Specify the destination L4 port.

[proto]: Specify the protocol.

[fragments]: Match non-initial fragments

[log]: Enable Logging

[dscp]: Specify the DSCP.

[mirror]: Specify the mirror port.

[redirect]: Specify the redirect port.

[rate-limit]: Specify the rate limit and burst size.

[tos]: Specify the TOS.

[mirror]: Specify a mirror port.

[redirect]: Specify the redirect port.

[rate-limit]: Specify the rate limit and burst size.

[precedence]: Specify the IP precedence.

[mirror]: Specify the mirror port.

[redirect]: Specify the redirect port.

[rate-limit]: Specify the rate limit and burst size.

deny: Add a deny rule to an existing IP ACL.

src: Specify the source IP/mask.

[sport]: Specify the source L4 port.

dst: Specify the destination IP/mask.

[dport]: Specify the destination L4 port.

[proto]: Specify a protocol.

[fragments]: Match non-initial fragments

[log]: Enable Logging

[dscp]: Specify the DSCP.

[tos]: Specify the TOS.

[precedence]: Specify the IP precedence.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1-10100</td>
<td>IP ACL ID</td>
</tr>
<tr>
<td>P-2</td>
<td>1-255</td>
<td>IP ACL Rule ID</td>
</tr>
<tr>
<td>P-3</td>
<td>any</td>
<td>Enter 'any' to match any ip address.</td>
</tr>
<tr>
<td></td>
<td>a.b.c.d</td>
<td>Enter the IP address to match.</td>
</tr>
<tr>
<td>P-4</td>
<td>any</td>
<td>Enter 'any' to match any ip mask.</td>
</tr>
<tr>
<td></td>
<td>a.b.c.d</td>
<td>Enter an IP mask to match. The 'Don’t care bits' are represented by binary 1's and 'Do care bits' are represented by binary 0's.</td>
</tr>
<tr>
<td>P-5</td>
<td>domain</td>
<td>Domain</td>
</tr>
<tr>
<td></td>
<td>echo</td>
<td>Echo</td>
</tr>
<tr>
<td></td>
<td>ftp</td>
<td>FTP</td>
</tr>
<tr>
<td></td>
<td>ftpdata</td>
<td>FTP Data</td>
</tr>
<tr>
<td></td>
<td>http</td>
<td>HTTP</td>
</tr>
<tr>
<td></td>
<td>https</td>
<td>HTTPS</td>
</tr>
<tr>
<td></td>
<td>smtp</td>
<td>SMTP</td>
</tr>
<tr>
<td></td>
<td>snmp</td>
<td>SNMP</td>
</tr>
<tr>
<td></td>
<td>telnet</td>
<td>Telnet</td>
</tr>
<tr>
<td></td>
<td>ssh</td>
<td>SSH</td>
</tr>
<tr>
<td></td>
<td>tftp</td>
<td>TFTP</td>
</tr>
<tr>
<td></td>
<td>www</td>
<td>WWW</td>
</tr>
<tr>
<td></td>
<td>1-65535</td>
<td>Port number</td>
</tr>
<tr>
<td>P-6</td>
<td>any</td>
<td>Enter 'any' to match any ip address.</td>
</tr>
<tr>
<td></td>
<td>a.b.c.d</td>
<td>Enter the IP address to match.</td>
</tr>
<tr>
<td>P-7</td>
<td>any</td>
<td>Enter 'any' to match any ip mask.</td>
</tr>
<tr>
<td></td>
<td>a.b.c.d</td>
<td>Enter an IP mask to match. The 'Don’t care bits' are represented by binary 1's and 'Do care bits' are represented by binary 0's.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Meaning</td>
</tr>
<tr>
<td>-----------</td>
<td>-------</td>
<td>---------</td>
</tr>
<tr>
<td>domain</td>
<td>Domain</td>
<td></td>
</tr>
<tr>
<td>echo</td>
<td>Echo</td>
<td></td>
</tr>
<tr>
<td>ftp</td>
<td>FTP</td>
<td></td>
</tr>
<tr>
<td>ftpdata</td>
<td>FTP Data</td>
<td></td>
</tr>
<tr>
<td>http</td>
<td>HTTP</td>
<td></td>
</tr>
<tr>
<td>https</td>
<td>HTTPS</td>
<td></td>
</tr>
<tr>
<td>smtp</td>
<td>SMTP</td>
<td></td>
</tr>
<tr>
<td>snmp</td>
<td>SNMP</td>
<td></td>
</tr>
<tr>
<td>telnet</td>
<td>Telnet</td>
<td></td>
</tr>
<tr>
<td>ssh</td>
<td>SSH</td>
<td></td>
</tr>
<tr>
<td>tfp</td>
<td>TFTP</td>
<td></td>
</tr>
<tr>
<td>www</td>
<td>WWW</td>
<td></td>
</tr>
<tr>
<td>1-65535</td>
<td>Port number</td>
<td></td>
</tr>
<tr>
<td>1-255</td>
<td>Enter a protocol number.</td>
<td></td>
</tr>
<tr>
<td>icmp</td>
<td>Match the ICMP protocol.</td>
<td></td>
</tr>
<tr>
<td>igmp</td>
<td>Match the IGMP protocol.</td>
<td></td>
</tr>
<tr>
<td>ip</td>
<td>Match the IPinIP tunnel.</td>
<td></td>
</tr>
<tr>
<td>tcp</td>
<td>Match the TCP protocol.</td>
<td></td>
</tr>
<tr>
<td>udp</td>
<td>Match the UDP protocol.</td>
<td></td>
</tr>
<tr>
<td>1.64</td>
<td>DSCP</td>
<td></td>
</tr>
<tr>
<td>slot/port</td>
<td>Enter a single interface in slot/port format.</td>
<td></td>
</tr>
<tr>
<td>0..10000000</td>
<td>Committed rate value, specified in kbps or pps</td>
<td></td>
</tr>
<tr>
<td>0..128</td>
<td>Committed burst size value, specified in kbytes or pps</td>
<td></td>
</tr>
<tr>
<td>pps</td>
<td>Packets per second.</td>
<td></td>
</tr>
<tr>
<td>kbps</td>
<td>kbytes per second.</td>
<td></td>
</tr>
<tr>
<td>1..31</td>
<td>Specify the IP TOS bits to match.</td>
<td></td>
</tr>
<tr>
<td>1..31</td>
<td>Specify the IP TOS bits that are of interest.</td>
<td></td>
</tr>
<tr>
<td>slot/port</td>
<td>Enter a single interface in slot/port format.</td>
<td></td>
</tr>
<tr>
<td>slot/port</td>
<td>Enter a single interface in slot/port format.</td>
<td></td>
</tr>
<tr>
<td>0..10000000</td>
<td>Committed rate value, specified in kbps or pps</td>
<td></td>
</tr>
<tr>
<td>0..128</td>
<td>Committed burst size value, specified in kbytes or pps</td>
<td></td>
</tr>
<tr>
<td>pps</td>
<td>Packets per second.</td>
<td></td>
</tr>
<tr>
<td>kbps</td>
<td>kbytes per second.</td>
<td></td>
</tr>
<tr>
<td>1..7</td>
<td>IP Precedence</td>
<td></td>
</tr>
<tr>
<td>slot/port</td>
<td>Enter a single interface in slot/port format.</td>
<td></td>
</tr>
<tr>
<td>slot/port</td>
<td>Enter a single interface in slot/port format.</td>
<td></td>
</tr>
<tr>
<td>0..10000000</td>
<td>Committed rate value, specified in kbps or pps</td>
<td></td>
</tr>
<tr>
<td>0..128</td>
<td>Committed burst size value, specified in kbytes or pps</td>
<td></td>
</tr>
<tr>
<td>pps</td>
<td>Packets per second.</td>
<td></td>
</tr>
<tr>
<td>kbps</td>
<td>kbytes per second.</td>
<td></td>
</tr>
<tr>
<td>any</td>
<td>Enter 'any' to match any ip address.</td>
<td></td>
</tr>
<tr>
<td>a.b.c.d</td>
<td>Enter the IP address to match.</td>
<td></td>
</tr>
<tr>
<td>any</td>
<td>Enter 'any' to match any ip mask.</td>
<td></td>
</tr>
<tr>
<td>a.b.c.d</td>
<td>Enter an IP mask to match. The 'Don't care bits' are represented by binary 1's and 'Do care bits' are represented by binary 0's..</td>
<td></td>
</tr>
<tr>
<td>domain</td>
<td>Domain</td>
<td></td>
</tr>
<tr>
<td>echo</td>
<td>Echo</td>
<td></td>
</tr>
<tr>
<td>ftp</td>
<td>FTP</td>
<td></td>
</tr>
<tr>
<td>ftpdata</td>
<td>FTP Data</td>
<td></td>
</tr>
<tr>
<td>http</td>
<td>HTTP</td>
<td></td>
</tr>
<tr>
<td>https</td>
<td>HTTPS</td>
<td></td>
</tr>
<tr>
<td>smtp</td>
<td>SMTP</td>
<td></td>
</tr>
<tr>
<td>snmp</td>
<td>SNMP</td>
<td></td>
</tr>
<tr>
<td>telnet</td>
<td>Telnet</td>
<td></td>
</tr>
<tr>
<td>ssh</td>
<td>SSH</td>
<td></td>
</tr>
<tr>
<td>tfp</td>
<td>TFTP</td>
<td></td>
</tr>
<tr>
<td>www</td>
<td>WWW</td>
<td></td>
</tr>
<tr>
<td>1-65535</td>
<td>Port number</td>
<td></td>
</tr>
<tr>
<td>any</td>
<td>Enter 'any' to match any ip address.</td>
<td></td>
</tr>
<tr>
<td>a.b.c.d</td>
<td>Enter the IP address to match.</td>
<td></td>
</tr>
<tr>
<td>any</td>
<td>Enter 'any' to match any ip mask.</td>
<td></td>
</tr>
<tr>
<td>a.b.c.d</td>
<td>Enter an IP mask to match. The 'Don't care bits' are represented by binary 1's and 'Do care bits' are represented by binary 0's..</td>
<td></td>
</tr>
</tbody>
</table>
### 1.3 show

Display device options and settings.

#### 1.3.1 show access-list trapflag

Display the trap flag status.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show access-list trapflag`

#### 1.3.2 show access-list mac rules

Display the rules of a specific MAC ACL.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show access-list mac rules [P-1] [P-2]`

#### 1.3.3 show access-list mac lists

Display an overview of the existing MAC ACLs.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show access-list mac lists [P-1]`
### 1.3 show

**1.3.4 show access-list mac counters**

Display the counters of a specific MAC ACL.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show access-list mac counters [P-1] [P-2]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..10100</td>
<td>MAC ACL ID</td>
</tr>
<tr>
<td>P-2</td>
<td>1..239</td>
<td>MAC ACL Rule ID</td>
</tr>
</tbody>
</table>

**Parameter Value Meaning**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..10100</td>
<td>MAC ACL ID</td>
</tr>
<tr>
<td>P-2</td>
<td>1..239</td>
<td>MAC ACL Rule ID</td>
</tr>
</tbody>
</table>

**1.3.5 show access-list mac assignment**

Display the assignments of the existing MAC ACLs.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show access-list mac assignment <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..10100</td>
<td>MAC ACL ID</td>
</tr>
</tbody>
</table>

**1.3.6 show access-list ip rules**

Display the rules of a specific IP ACL.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show access-list ip rules [P-1] [P-2]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..10100</td>
<td>IP ACL ID</td>
</tr>
<tr>
<td>P-2</td>
<td>1..239</td>
<td>IP ACL Rule ID</td>
</tr>
</tbody>
</table>

**1.3.7 show access-list ip lists**

Display an overview of the existing IP ACLs.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show access-list ip lists [P-1]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..10100</td>
<td>IP ACL ID</td>
</tr>
</tbody>
</table>

**1.3.8 show access-list ip counters**

Display the counters of a specific IP ACL.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show access-list ip counters [P-1] [P-2]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..10100</td>
<td>IP ACL ID</td>
</tr>
<tr>
<td>P-2</td>
<td>1..239</td>
<td>IP ACL Rule ID</td>
</tr>
</tbody>
</table>

**1.3.9 show access-list ip assignment**

Display the assignments of the existing IP ACLs.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show access-list ip assignment <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..10100</td>
<td>IP ACL ID</td>
</tr>
</tbody>
</table>
2 Application Lists

2.1 appllists
Configure an application list.

2.1.1 appllists set-authlist
Set an authentication list reference that shall be used by given application.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: appllists set-authlist <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;application&gt; Name of an application list.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>&lt;authlist name&gt; Name of referenced authentication list.</td>
</tr>
</tbody>
</table>

2.1.2 appllists enable
Activate a login application list.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: appllists enable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;application&gt; Name of an application list.</td>
</tr>
</tbody>
</table>

2.1.3 appllists disable
Deactivate a login application list.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: appllists disable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;application&gt; Name of an application list.</td>
</tr>
</tbody>
</table>

2.2 show
Display device options and settings.

2.2.1 show appllists
Display the ordered methods for application lists.
- Mode: Command is in all modes available.
- Privilege Level: Administrator
- Format: show appllists
3 Authentication Lists

3.1 authlists

Configure an authentication list.

3.1.1 authlists add

Create a new login authentication list.

Mode: Global Config Mode
Privilege Level: Administrator
Format: authlists add <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;authlist_name&gt; Name of an authentication list.</td>
</tr>
</tbody>
</table>

3.1.2 authlists delete

Delete an existing login authentication list.

Mode: Global Config Mode
Privilege Level: Administrator
Format: authlists delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;authlist_name&gt; Name of an authentication list.</td>
</tr>
</tbody>
</table>

3.1.3 authlists set-policy

Set the policies of a login authentication list.

Mode: Global Config Mode
Privilege Level: Administrator
Format: authlists set-policy <P-1> <P-2> [P-3] [P-4] [P-5] [P-6]]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;authlist_name&gt; Name of an authentication list.</td>
</tr>
<tr>
<td>P-2</td>
<td>reject</td>
<td>Authentication is rejected / not allowed</td>
</tr>
<tr>
<td>local</td>
<td></td>
<td>Authentication by local user DB</td>
</tr>
<tr>
<td>radius</td>
<td></td>
<td>Authentication by RADIUS server</td>
</tr>
<tr>
<td>ldap</td>
<td></td>
<td>Authentication by remote server</td>
</tr>
<tr>
<td>P-3</td>
<td>reject</td>
<td>Authentication is rejected / not allowed</td>
</tr>
<tr>
<td>local</td>
<td></td>
<td>Authentication by local user DB</td>
</tr>
<tr>
<td>radius</td>
<td></td>
<td>Authentication by RADIUS server</td>
</tr>
<tr>
<td>ldap</td>
<td></td>
<td>Authentication by remote server</td>
</tr>
<tr>
<td>P-4</td>
<td>reject</td>
<td>Authentication is rejected / not allowed</td>
</tr>
<tr>
<td>local</td>
<td></td>
<td>Authentication by local user DB</td>
</tr>
<tr>
<td>radius</td>
<td></td>
<td>Authentication by RADIUS server</td>
</tr>
<tr>
<td>ldap</td>
<td></td>
<td>Authentication by remote server</td>
</tr>
<tr>
<td>P-5</td>
<td>reject</td>
<td>Authentication is rejected / not allowed</td>
</tr>
<tr>
<td>local</td>
<td></td>
<td>Authentication by local user DB</td>
</tr>
<tr>
<td>radius</td>
<td></td>
<td>Authentication by RADIUS server</td>
</tr>
<tr>
<td>ldap</td>
<td></td>
<td>Authentication by remote server</td>
</tr>
<tr>
<td>P-6</td>
<td>reject</td>
<td>Authentication is rejected / not allowed</td>
</tr>
<tr>
<td>local</td>
<td></td>
<td>Authentication by local user DB</td>
</tr>
<tr>
<td>radius</td>
<td></td>
<td>Authentication by RADIUS server</td>
</tr>
<tr>
<td>ldap</td>
<td></td>
<td>Authentication by remote server</td>
</tr>
</tbody>
</table>

3.1.4 authlists enable

Activate a login authentication list.

Mode: Global Config Mode
Privilege Level: Administrator
Format: authlists enable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;authlist_name&gt; Name of an authentication list.</td>
</tr>
</tbody>
</table>
3.1.5 **authlists disable**
Deactivate a login authentication list.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** authlists disable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;authlist name&gt; Name of an authentication list.</td>
</tr>
</tbody>
</table>

3.2 **show**
Display device options and settings.

3.2.1 **show authlists**
Display the ordered methods for authentication lists.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Administrator
- **Format:** show authlists
4 Class Of Service

4.1 classofservice

Class of service configuration.

4.1.1 classofservice dot1p-mapping

Enter a VLAN priority and the traffic class it should be mapped to.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** classofservice dot1p-mapping <P-1> <P-2> <P-3>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..7</td>
<td>Enter the 802.1p priority.</td>
</tr>
<tr>
<td>P-2</td>
<td>0..7</td>
<td>Enter the Traffic Class value.</td>
</tr>
<tr>
<td>P-3</td>
<td>0..3</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

4.2 show

Display device options and settings.

4.2.1 show classofservice dot1p-mapping

Display a table containing the vlan priority to traffic class mappings.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show classofservice dot1p-mapping
5  Command Line Interface (CLI)

5.1  cli

Set the CLI preferences.

5.1.1  cli serial-timeout

Set login timeout for serial line connection to CLI. Setting to 0 will disable the timeout. The value is active after next login.

Mode: Privileged Exec Mode
Privilege Level: Operator
Format: cli serial-timeout <P-1>

<table>
<thead>
<tr>
<th>Parameter Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1 0..160</td>
<td>Enter a number in the given range. Setting to 0 will disable the timeout.</td>
</tr>
</tbody>
</table>

5.1.2  cli prompt

Change the system prompt. Following wildcards are allowed: %d date, %t time, %i IP address, %m MAC address, %p product name

Mode: Privileged Exec Mode
Privilege Level: Operator
Format: cli prompt <P-1>

<table>
<thead>
<tr>
<th>Parameter Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1 string</td>
<td>Enter a user-defined text, max. 128 characters. Following wildcards are allowed: %d date, %t time, %i IP address, %m MAC address, %p product name</td>
</tr>
</tbody>
</table>

5.1.3  cli numlines

Screen size for 'more' (23 = default). Enter a 0 will disable the feature. The value is only valid for the current session.

Mode: Command is in all modes available.
Privilege Level: Guest
Format: cli numlines <P-1>

<table>
<thead>
<tr>
<th>Parameter Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1 0..250</td>
<td>Screen size for 'more' (23 = default). Enter a 0 will disable the feature. The value is only valid for the current session.</td>
</tr>
</tbody>
</table>

5.1.4  cli banner operation

Enable or disable the CLI login banner.

Mode: Privileged Exec Mode
Privilege Level: Administrator
Format: cli banner operation

- no cli banner operation
  Disable the option
  Mode: Privileged Exec Mode
  Privilege Level: Administrator
  Format: no cli banner operation

5.1.5  cli banner text

Set the text for the CLI login banner (C printf format syntax allowed: ).

Mode: Privileged Exec Mode
Privilege Level: Administrator
Format: cli banner text <P-1>

<table>
<thead>
<tr>
<th>Parameter Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1 string</td>
<td>Enter a user-defined text, max. 1024 characters (allowed characters are from ASCII 32 to 127).</td>
</tr>
</tbody>
</table>
5.2 show

Display device options and settings.

5.2.1 show cli global

Display the CLI preferences.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show cli global

5.2.2 show cli command-tree

Display a list of every command.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show cli command-tree

5.3 logging

Logging configuration.

5.3.1 logging cli-command

Enable or disable the CLI command logging.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** logging cli-command

- **no logging cli-command**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no logging cli-command

5.4 show

Display device options and settings.

5.4.1 show logging cli-command

Display the CLI command logging preferences.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show logging cli-command
6 Clock

6.1 clock
Configure local and DST clock settings.

6.1.1 clock set
Edit current local time.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `clock set <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>YYYY-MM-DD</td>
<td>Local date (range: 2004-01-01 - 2037-12-31).</td>
</tr>
<tr>
<td>P-2</td>
<td>HH:MM:SS</td>
<td>Local time.</td>
</tr>
</tbody>
</table>

6.1.2 clock timezone offset
Local time offset (in minutes) with respect to UTC (positive values for locations east of Greenwich).
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `clock timezone offset <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>-780..840</td>
<td>Edit the timezone offset (in minutes).</td>
</tr>
</tbody>
</table>

6.1.3 clock timezone zone
Edit the timezone acronym (max. 4 characters).
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `clock timezone zone <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Edit the timezone acronym (max 4 characters).</td>
</tr>
</tbody>
</table>

6.2 show
Display device options and settings.

6.2.1 show clock
Display the current time information.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show clock [summer-time]`
  *[summer-time]: Display the summer-time parameters.*
7 Configuration

7.1 save
Save the configuration to the specified destination.

7.1.1 save profile
Save the configuration to the specific profile.
- Mode: All Privileged Modes
- Privilege Level: Operator
- Format: save profile <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
</tbody>
</table>

7.2 config
Configure the configuration saving settings.

7.2.1 config watchdog admin-state
Enable or disable the configuration undo feature.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: config watchdog admin-state

- no config watchdog admin-state
  Disable the option
  - Mode: Global Config Mode
  - Privilege Level: Operator
  - Format: no config watchdog admin-state

7.2.2 config watchdog timeout
Configure the configuration undo timeout (unit: seconds).
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: config watchdog timeout <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>30..600</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

7.2.3 config encryption password set
Set the configuration file password.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: config encryption password set [P-1] [P-2]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 64 characters.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 64 characters.</td>
</tr>
</tbody>
</table>

7.2.4 config encryption password clear
Clear the configuration file password.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: config encryption password clear [P-1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 64 characters.</td>
</tr>
</tbody>
</table>
7.2.5 config envm choose-active

Choose the active external non-volatile memory for copying firmware, logs, certificates etc. This does not affect loading and saving of the configuration.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** config envm choose-active <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>sd</td>
<td>SD-Card</td>
</tr>
<tr>
<td></td>
<td>usb</td>
<td>USB Storage Device</td>
</tr>
</tbody>
</table>

7.2.6 config envm log-device

Choose the active external non-volatile memory for persistent log files.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** config envm log-device <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>sd</td>
<td>SD-Card</td>
</tr>
<tr>
<td></td>
<td>usb</td>
<td>USB Storage Device</td>
</tr>
</tbody>
</table>

7.2.7 config envm auto-update

Allow automatic firmware updates with this memory device.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** config envm auto-update <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>sd</td>
<td>SD-Card</td>
</tr>
<tr>
<td></td>
<td>usb</td>
<td>USB Storage Device</td>
</tr>
</tbody>
</table>

- **no config envm auto-update**
  
  Disable the option
  
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no config envm auto-update <P-1>

7.2.8 config envm config-save

Allow the configuration to be saved to this memory device.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** config envm config-save <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>sd</td>
<td>SD-Card</td>
</tr>
<tr>
<td></td>
<td>usb</td>
<td>USB Storage Device</td>
</tr>
</tbody>
</table>

- **no config envm config-save**
  
  Disable the option
  
  - **Mode:** Global Config Mode
  - **Privilege Level:** Operator
  - **Format:** no config envm config-save <P-1>

7.2.9 config envm load-priority

Configure the order of configuration load attempts from memory devices at boot time. If one load is successful, then the device discards further attempts.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** config envm load-priority <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>sd</td>
<td>SD-Card</td>
</tr>
<tr>
<td></td>
<td>usb</td>
<td>USB Storage Device</td>
</tr>
<tr>
<td>P-2</td>
<td>disable</td>
<td>Config will not be loaded at all</td>
</tr>
<tr>
<td></td>
<td>first</td>
<td>Config will be loaded first. If successful, no other config will be tried.</td>
</tr>
<tr>
<td></td>
<td>second</td>
<td>Config will be loaded if first one does not succeed.</td>
</tr>
</tbody>
</table>
7.2.10 config profile select
Select a configuration profile to be the active configuration.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `config profile select <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>nvm</td>
<td>You can only select nvm for this command.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..20</td>
<td>Index of the profile entry.</td>
</tr>
</tbody>
</table>

7.2.11 config profile delete
Delete a specific configuration profile.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `config profile delete <P-1> num <P-2> profile <P-3>`
  - `num`: Select the index of a profile to delete.
  - `profile`: Select the name of a profile to delete.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>nvm</td>
<td>non-volatile memory</td>
</tr>
<tr>
<td></td>
<td>envm</td>
<td>external non-volatile memory device</td>
</tr>
<tr>
<td>P-2</td>
<td>1..20</td>
<td>Index of the profile entry.</td>
</tr>
<tr>
<td>P-3</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
</tbody>
</table>

7.2.12 config fingerprint verify nvm profile
Select the name of a profile to be verified.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `config fingerprint verify nvm profile <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter hash as 40 hexa-decimal characters.</td>
</tr>
</tbody>
</table>

7.2.13 config fingerprint verify nvm num
Select the index number of a profile to be verified.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `config fingerprint verify nvm num <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..20</td>
<td>Index of the profile entry.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter hash as 40 hexa-decimal characters.</td>
</tr>
</tbody>
</table>

7.2.14 config fingerprint verify envm profile
Select the name of a profile to be verified.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `config fingerprint verify envm profile <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter hash as 40 hexa-decimal characters.</td>
</tr>
</tbody>
</table>

7.2.15 config fingerprint verify envm num
Select the index number of a profile to be verified.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `config fingerprint verify envm num <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..20</td>
<td>Index of the profile entry.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter hash as 40 hexa-decimal characters.</td>
</tr>
</tbody>
</table>
7.3 copy

Copy different kinds of items.

7.3.1 copy sysinfo system envm

Copy the system information to external non-volatile memory.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** `copy sysinfo system envm [filename <P-1>]`

**Parameter** | **Value** | **Meaning**
--- | --- | ---
| P-1 | string | Enter a user-defined text, max. 32 characters.

7.3.2 copy sysinfoall system envm

Copy the system information and the event log from the device to external non-volatile memory.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** `copy sysinfoall system envm`

7.3.3 copy firmware envm

Copy a firmware image to the device from external non-volatile memory.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `copy firmware envm <P-1> system`

7.3.4 copy firmware remote

Copy a firmware image to the device from a server.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `copy firmware remote <P-1> system`

7.3.5 copy config running-config nvm

Copy the running-config to non-volatile memory.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** `copy config running-config nvm [profile <P-1>]`

7.3.6 copy config running-config remote

Copy the running-config to a file server.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `copy config running-config remote <P-1>`

7.3.7 copy config nvm

Load a configuration from non-volatile memory to the running-config.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `copy config nvm [profile <P-1>] running-config remote <P-2>`
running-config: (Re)-load a configuration from non-volatile memory to the running-config.
remote: Copy a configuration from non-volatile memory to a server.

### 7.3.8 copy config envm
Copy a configuration from external non-volatile memory to non-volatile memory.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `copy config envm [profile <P-1>] nvm`

**[profile]**: Copy a specific configuration profile from external non-volatile memory to non-volatile memory.

- **nvm:** Copy a specific profile from external non-volatile memory to non-volatile memory.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>

### 7.3.9 copy config remote
Copy a configuration file to the device from a server.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `copy config remote <P-1> nvm [profile <P-2>] running-config`

- **nvm:** Copy a configuration file from a server to non-volatile memory.
- **[profile]**: Copy a configuration from a server to a specific profile in non-volatile memory.
- **running-config:** Copy a configuration file from a server to the running-config.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>

### 7.4 clear
Clear several items.

#### 7.4.1 clear config
Clear the running configuration.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `clear config`

#### 7.4.2 clear factory
Set the device back to the factory settings (use with care).

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `clear factory`

#### 7.4.3 clear sfp-white-list
Clear the SFP WhiteList.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** `clear sfp-white-list`

### 7.5 show
Display device options and settings.
7.5.1 show running-config
Display the currently running configuration.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Administrator
- **Format:** show running-config

7.5.2 show running-config xml
Display the currently running configuration (XML file).
- **Mode:** Command is in all modes available.
- **Privilege Level:** Administrator
- **Format:** show running-config xml

7.6 show
Display device options and settings.

7.6.1 show config envm settings
Display the settings of the external non-volatile memory.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show config envm settings

7.6.2 show config envm properties
Display the properties of the external non-volatile memory.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show config envm properties

7.6.3 show config envm active
Display the active external non-volatile memory.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show config envm active

7.6.4 show config watchdog
Display the Auto Configuration Undo settings.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show config watchdog

7.6.5 show config encryption
Display the settings for configuration encryption.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show config encryption

7.6.6 show config profiles
Display the configuration profiles.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Administrator
- **Format:** show config profiles <P-1> [<P-2>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value 1</th>
<th>Value 2</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>nvm</td>
<td>envm</td>
<td>non-volatile memory</td>
</tr>
<tr>
<td>P-2</td>
<td>1..20</td>
<td></td>
<td>external non-volatile memory device</td>
</tr>
<tr>
<td>P-3</td>
<td></td>
<td></td>
<td>Index of the profile entry.</td>
</tr>
</tbody>
</table>
7.6.7  show config status
Display the synchronization status of the running configuration with the non-volatile memory and the ACA.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show config status

7.7  swap
Swap software images.

7.7.1  swap firmware system backup
Swap the main and backup images.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** swap firmware system backup
8 Device Monitoring

8.1 device-status
Configure various device conditions to be monitored.

8.1.1 device-status monitor link-failure
Enable or disable monitor state of network connection(s).
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** device-status monitor link-failure

**no device-status monitor link-failure**
Disable the option
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** no device-status monitor link-failure

8.1.2 device-status monitor temperature
Enable or disable monitoring of the device temperature.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** device-status monitor temperature

**no device-status monitor temperature**
Disable the option
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** no device-status monitor temperature

8.1.3 device-status monitor envm-removal
Enable or disable monitoring the presence of the external non-volatile memory.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** device-status monitor envm-removal

**no device-status monitor envm-removal**
Disable the option
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** no device-status monitor envm-removal

8.1.4 device-status monitor envm-not-in-sync
Enable or disable monitoring synchronization between the external non-volatile memory and the running configuration.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** device-status monitor envm-not-in-sync

**no device-status monitor envm-not-in-sync**
Disable the option
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** no device-status monitor envm-not-in-sync
8.1.5 device-status monitor power-supply

Enable or disable monitoring the condition of the power supply(s).

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** device-status monitor power-supply <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..2</td>
<td>Number of power supply.</td>
</tr>
</tbody>
</table>

- **no device-status monitor power-supply**
  - Disable the option
    - **Mode:** Global Config Mode
    - **Privilege Level:** Administrator
    - **Format:** no device-status monitor power-supply <P-1>

8.1.6 device-status trap

Configure the device to send a trap when the device status changes.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** device-status trap

- **no device-status trap**
  - Disable the option
    - **Mode:** Global Config Mode
    - **Privilege Level:** Administrator
    - **Format:** no device-status trap

8.2 device-status

Configure various device conditions to be monitored.

8.2.1 device-status link-alarm

Configure the monitor settings of the port link.

- **Mode:** Interface Range Mode
- **Privilege Level:** Administrator
- **Format:** device-status link-alarm

- **no device-status link-alarm**
  - Disable the option
    - **Mode:** Interface Range Mode
    - **Privilege Level:** Administrator
    - **Format:** no device-status link-alarm

8.3 show

Display device options and settings.

8.3.1 show device-status monitor

Display the device monitoring configurations.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show device-status monitor
8.3.2  **show device-status state**
Display the current state of the device.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show device-status state

8.3.3  **show device-status trap**
Display the device trap information and configurations.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show device-status trap

8.3.4  **show device-status events**
Display occurred device status events.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show device-status events

8.3.5  **show device-status link-alarm**
Display the monitor configurations of the network ports.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show device-status link-alarm

8.3.6  **show device-status all**
Display the configurable device status settings.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show device-status all
9 Device Security

9.1 security-status

Configure the security status settings.

9.1.1 security-status monitor pwd-change
Sets the monitoring of default password change for 'user' and 'admin'.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** security-status monitor pwd-change

- **no security-status monitor pwd-change**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no security-status monitor pwd-change

9.1.2 security-status monitor pwd-min-length
Sets the monitoring of minimum length of the password (smaller 8).
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** security-status monitor pwd-min-length

- **no security-status monitor pwd-min-length**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no security-status monitor pwd-min-length

9.1.3 security-status monitor pwd-policy-config
Sets the monitoring whether the minimum password policy is configured. The device changes the security status to the value "error" if the value for at least one of the following password rules is 0: "minimum upper cases", "minimum lower cases", "minimum numbers", "minimum special characters".
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** security-status monitor pwd-policy-config

- **no security-status monitor pwd-policy-config**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no security-status monitor pwd-policy-config

9.1.4 security-status monitor pwd-policy-inactive
Sets the monitoring whether at least one user is configured with inactive policy check. The device changes the security status to the value "error" if the function "policy check" is inactive for at least 1 user account.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** security-status monitor pwd-policy-inactive

- **no security-status monitor pwd-policy-inactive**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no security-status monitor pwd-policy-inactive
9.1.5 security-status monitor http-enabled
Sets the monitoring of the activation of http on the switch.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** security-status monitor http-enabled

- **no security-status monitor http-enabled**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no security-status monitor http-enabled

9.1.6 security-status monitor snmp-unsecure
Sets the monitoring of SNMP security (SNMP v1/v2 is enabled or v3 encryption is disabled).

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** security-status monitor snmp-unsecure

- **no security-status monitor snmp-unsecure**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no security-status monitor snmp-unsecure

9.1.7 security-status monitor sysmon-enabled
Sets the monitoring of the activation of System Monitor 1 on the switch.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** security-status monitor sysmon-enabled

- **no security-status monitor sysmon-enabled**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no security-status monitor sysmon-enabled

9.1.8 security-status monitor extnvm-upd-enabled
Sets the monitoring of activation of the configuration saving to external non volatile memory.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** security-status monitor extnvm-upd-enabled

- **no security-status monitor extnvm-upd-enabled**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no security-status monitor extnvm-upd-enabled

9.1.9 security-status monitor no-link-enabled
Sets the monitoring of no link detection.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** security-status monitor no-link-enabled

- **no security-status monitor no-link-enabled**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no security-status monitor no-link-enabled
Device Security
9.2 security-status

9.1.10 security-status monitor hidisc-enabled
Sets the monitoring of HiDiscovery.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** security-status monitor hidisc-enabled

- **no security-status monitor hidisc-enabled**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no security-status monitor hidisc-enabled

9.1.11 security-status monitor extnvm-load-unsecure
Sets the monitoring of security of the configuration loading from extnvm.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** security-status monitor extnvm-load-unsecure

- **no security-status monitor extnvm-load-unsecure**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no security-status monitor extnvm-load-unsecure

9.1.12 security-status monitor https-certificate
Sets the monitoring whether auto generated self-signed HTTPS certificate is in use.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** security-status monitor https-certificate

- **no security-status monitor https-certificate**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no security-status monitor https-certificate

9.1.13 security-status trap
Configure if a trap is sent when the security status changes.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** security-status trap

- **no security-status trap**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no security-status trap

9.2 security-status
Configure the security status interface settings.

9.2.1 security-status no-link
Configure the monitoring of the specific ports.

- **Mode:** Interface Range Mode
- **Privilege Level:** Administrator
- **Format:** security-status no-link
### 9.3 show

Display device options and settings.

#### 9.3.1 show security-status monitor

Display the security status monitoring settings.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show security-status monitor

#### 9.3.2 show security-status state

Display the current security status.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show security-status state

#### 9.3.3 show security-status no-link

Display the settings of the monitoring of the specific network ports.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show security-status no-link

#### 9.3.4 show security-status trap

Display the security status trap information and settings.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show security-status trap

#### 9.3.5 show security-status events

Display the occurred security status events.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show security-status events

#### 9.3.6 show security-status all

Display the security status settings.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show security-status all
10 Domain Name System (DNS)

10.1 dns
Set DNS parameters.

10.1.1 dns caching-server adminstate
Enable or disable the DNS Caching Server.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dns caching-server adminstate

```
no dns caching-server adminstate
```
Disable the option
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** no dns caching-server adminstate

10.1.2 dns caching-server flush
Flush the DNS cache.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dns caching-server flush <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>action</td>
<td>Flush the DNS cache.</td>
</tr>
</tbody>
</table>

10.1.3 dns client adminstate
Enable or disable DNS Client.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dns client adminstate

```
no dns client adminstate
```
Disable the option
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** no dns client adminstate

10.1.4 dns client cache adminstate
Enable or disable DNS client cache.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dns client cache adminstate

```
no dns client cache adminstate
```
Disable the option
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** no dns client cache adminstate

10.1.5 dns client servers add
Add a new DNS server.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dns client servers add <P-1> ip <P-2>
- **ip:** Enter the DNS server address.
### 10.1.6 dns client servers delete

Delete a DNS server.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `dns client servers delete <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>DNS Client servers index.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

### 10.1.7 dns client servers modify

Modify a DNS server entry.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `dns client servers modify <P-1> ip <P-2> status <P-3> operation <P-4>`
- **ip:** Change the DNS server address.
- **status:** Change the status of this DNS server.
- **operation:** Change the status of this DNS server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>DNS Client servers index.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-3</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
<tr>
<td>P-4</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

### 10.1.8 dns client servers enable

Activate a DNS server entry.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `dns client servers enable <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>DNS Client servers index.</td>
</tr>
</tbody>
</table>

### 10.1.9 dns client servers disable

Deactivate a DNS server entry.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `dns client servers disable <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>DNS Client servers index.</td>
</tr>
</tbody>
</table>

### 10.1.10 dns client timeout

Set the timeout before retransmitting a request to the server.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `dns client timeout <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..3600</td>
<td>The timeout before retransmitting a request to the server (default: 3).</td>
</tr>
</tbody>
</table>

### 10.1.11 dns client retry

Set the number of times the request is retransmitted.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `dns client retry <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..100</td>
<td>The number of times the request is retransmitted (default: 2).</td>
</tr>
</tbody>
</table>
10.2  show

Display device options and settings.

10.2.1  show dns caching-server info

Display the DNS Caching Server information.
► **Mode:** Command is in all modes available.
► **Privilege Level:** Guest
► **Format:** show dns caching-server info

10.2.2  show dns client hosts

Display the DNS Client hosts table.
► **Mode:** Command is in all modes available.
► **Privilege Level:** Guest
► **Format:** show dns client hosts

10.2.3  show dns client info

Display the DNS Client related information.
► **Mode:** Command is in all modes available.
► **Privilege Level:** Guest
► **Format:** show dns client info

10.2.4  show dns client servers

Display the DNS Client servers.
► **Mode:** Command is in all modes available.
► **Privilege Level:** Guest
► **Format:** show dns client servers
11 DoS Mitigation

11.1 dos

Manage DoS Mitigation

11.1.1 dos tcp-null

Enables TCP Null scan protection - all TCP flags and TCP sequence number zero.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dos tcp-null

- **no dos tcp-null**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Operator
  - **Format:** no dos tcp-null

11.1.2 dos tcp-xmas

Enables TCP XMAS scan protection - TCP FIN, URG, PSH equal 1 and SEQ equals 0.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dos tcp-xmas

- **no dos tcp-xmas**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Operator
  - **Format:** no dos tcp-xmas

11.1.3 dos tcp-syn-fin

Enables TCP SYN/FIN scan protection - TCP with SYN and FIN flags set.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dos tcp-syn-fin

- **no dos tcp-syn-fin**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Operator
  - **Format:** no dos tcp-syn-fin

11.1.4 dos tcp-min-header

Enables TCP minimal header size check.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dos tcp-min-header

- **no dos tcp-min-header**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Operator
  - **Format:** no dos tcp-min-header
11.1.5  **dos icmp-fragmented**
Enables fragmented ICMP protection.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dos icmp-fragmented

■ **no dos icmp-fragmented**
Disable the option
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** no dos icmp-fragmented

11.1.6  **dos icmp payload-check**
Enables ICMP max payload size protection for IPv4 and IPv6.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dos icmp payload-check

■ **no dos icmp payload-check**
Disable the option
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** no dos icmp payload-check

11.1.7  **dos icmp payload-size**
Configures maximum ICMP payload size (default: 512).
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dos icmp payload-size <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..1472</td>
<td>Max. ICMP payload size (default: 512)</td>
</tr>
</tbody>
</table>

11.1.8  **dos ip-land**
Enables LAND attack protection - source IP equals destination IP.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dos ip-land <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

11.1.9  **dos ip-src-route**
Enables Drop IP source route - Discard packets with Strict/Loose Source Routing Option set.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dos ip-src-route

■ **no dos ip-src-route**
Disable the option
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** no dos ip-src-route

11.1.10  **dos tcp-offset**
Enables TCP offset check - ingress TCP packets with fragment offset 1 are dropped.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dos tcp-offset
11.2 show

Display device options and settings.

11.2.1 show dos

Display the DoS Mitigation parameters.

- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show dos
12 Deep Packet Inspection (DPI)

12.1 dpi

Creation and configuration of DPI profiles.

12.1.1 dpi modbus commit

Writes all changes made in the DPI MODBUS profiles to the enforcer.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi modbus commit

12.1.2 dpi modbus addprofile

 Adds a profile to the DPI MODBUS profile table.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi modbus addprofile <P-1> [description <P-2>] [function-type <P-3>] [function-code-list <P-4>] [unit-identifier-list <P-5>] [sanity-check <P-6>] [exception <P-7>] [reset <P-8>]

  - [description]: Profile description/name for the DPI MODBUS profile.
  - [function-type]: Function type of corresponding function codes.
  - [function-code-list]: Function code list. A function code has the syntax 'val'. Function codes are separated by a comma. When more than one value for an function code is specified the values are separated by the pipe symbol ('|').
  - [unit-identifier-list]: Unit identifier list. A unit identifier has the syntax 'val'. To specify no options, the value 'none' must be given. Unit identifiers are separated by a comma.
  - [sanity-check]: Sanity check including format and specification.
  - [exception]: Device exception message.
  - [reset]: Reset connection message.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index 1 - 32</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Profile description/name</td>
</tr>
<tr>
<td>P-3</td>
<td>readonly</td>
<td>Read only function codes for function code list</td>
</tr>
<tr>
<td></td>
<td>readwrite</td>
<td>Read write function codes for function code list</td>
</tr>
<tr>
<td></td>
<td>programming</td>
<td>Programming function codes for function code list</td>
</tr>
<tr>
<td></td>
<td>all</td>
<td>All possible function codes for function code list (allow any function code)</td>
</tr>
<tr>
<td></td>
<td>advanced</td>
<td>Keeps the function code list from the previous selection and makes it editable by the user</td>
</tr>
</tbody>
</table>
12.1.3 dpi modbus modifyprofile

Modifies a profile in the DPI MODBUS profile table.

**Mode:** Global Config Mode

**Privilege Level:** Operator

**Format:**
```
dpi modbus modifyprofile <P-1> [description <P-2>] [function-type <P-3>] [function-code-list <P-4>] [unit-identifier-list <P-5>] [sanity-check <P-6>] [exception <P-7>] [reset <P-8>]
```

- **description**: Profile description/name for the DPI MODBUS profile.
- **function-type**: Function type of corresponding function codes.
- **function-code-list**: Function code list. A function code has the syntax 'val'. Function codes are separated by a comma. When more than one value for a function code is specified, the values are separated by the pipe symbol (`|`).
- **unit-identifier-list**: Unit identifier list. A unit identifier has the syntax 'val'. To specify no options, the value 'none' must be given. Unit identifiers are separated by a comma.
- **sanity-check**: Sanity check including format and specification.
- **exception**: Device exception message.
- **reset**: Reset connection message.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-4</td>
<td>1..255</td>
<td>Function codes 1 - 255</td>
</tr>
<tr>
<td>P-10</td>
<td>0-65535</td>
<td>Function code read coils, coil address range 0 - 65535</td>
</tr>
<tr>
<td>P-20</td>
<td>0-65535</td>
<td>Function code read discrete inputs, input address range 0 - 65535</td>
</tr>
<tr>
<td>P-30</td>
<td>0-65535</td>
<td>Function code read holding registers, register address range 0 - 65535</td>
</tr>
<tr>
<td>P-40</td>
<td>0-65535</td>
<td>Function code read input registers, register address range 0 - 65535</td>
</tr>
<tr>
<td>P-50</td>
<td>0-65535</td>
<td>Function code write single coil, coil address range 0 - 65535</td>
</tr>
<tr>
<td>P-60</td>
<td>0-65535</td>
<td>Function code write single register, register address range 0 - 65535</td>
</tr>
<tr>
<td>P-7</td>
<td></td>
<td>Function code read exception status</td>
</tr>
<tr>
<td>P-8</td>
<td></td>
<td>Function code diagnostic</td>
</tr>
<tr>
<td>P-11</td>
<td></td>
<td>Function code get com event counter</td>
</tr>
<tr>
<td>P-12</td>
<td></td>
<td>Function code get comm event log</td>
</tr>
<tr>
<td>P-13</td>
<td></td>
<td>Function code program (584/984)</td>
</tr>
<tr>
<td>P-14</td>
<td></td>
<td>Function code poll (584/984)</td>
</tr>
<tr>
<td>P-15</td>
<td>0-65535</td>
<td>Function code write multiple coils, coil address range 0 - 65535</td>
</tr>
<tr>
<td>P-16</td>
<td>0-65535</td>
<td>Function code write multiple registers, register address range 0 - 65535</td>
</tr>
<tr>
<td>P-17</td>
<td></td>
<td>Function code report slave id</td>
</tr>
<tr>
<td>P-20</td>
<td></td>
<td>Function code read file record</td>
</tr>
<tr>
<td>P-21</td>
<td></td>
<td>Function code write file record</td>
</tr>
<tr>
<td>P-22</td>
<td>0-65535</td>
<td>Function code mask write register, register address range 0 - 65535</td>
</tr>
<tr>
<td>P-23</td>
<td>0-65535</td>
<td>Function code read/write multiple registers, read address range 0 - 65535, write address range 0 - 65535</td>
</tr>
<tr>
<td>P-24</td>
<td>0-65535</td>
<td>Function code read fifo queue, pointer address range 0 - 65535</td>
</tr>
<tr>
<td>P-40</td>
<td></td>
<td>Function code program (concept)</td>
</tr>
<tr>
<td>P-42</td>
<td></td>
<td>Function code concept symbol table</td>
</tr>
<tr>
<td>P-43</td>
<td></td>
<td>Function code encapsulated interface transport</td>
</tr>
<tr>
<td>P-48</td>
<td></td>
<td>Function code advantech co. ltd. - management functions</td>
</tr>
<tr>
<td>P-66</td>
<td></td>
<td>Function code scan data inc. - expanded read holding registers</td>
</tr>
<tr>
<td>P-67</td>
<td></td>
<td>Function code scan data inc. - expanded write holding registers</td>
</tr>
<tr>
<td>P-90</td>
<td></td>
<td>Function code unity programming/ofs</td>
</tr>
<tr>
<td>P-100</td>
<td></td>
<td>Function code scattered register read</td>
</tr>
<tr>
<td>P-125</td>
<td></td>
<td>Function code schneider electric - firmware replacement</td>
</tr>
<tr>
<td>P-126</td>
<td></td>
<td>Function code schneider electric - program</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-5</td>
<td>0..255</td>
<td>Unit identifier 0 - 255</td>
</tr>
<tr>
<td>P-5 1</td>
<td>none</td>
<td>No unit identifier 'none'</td>
</tr>
<tr>
<td>P-6</td>
<td>yes</td>
<td>True</td>
</tr>
<tr>
<td>P-6 no</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>P-7</td>
<td>yes</td>
<td>True</td>
</tr>
<tr>
<td>P-7 no</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>P-8</td>
<td>yes</td>
<td>True</td>
</tr>
<tr>
<td>P-8 no</td>
<td>False</td>
<td></td>
</tr>
</tbody>
</table>
12.1.4 dpi modbus copyprofile

Copies a profile to another DPI MODBUS profile.

| Mode: | Global Config Mode |
| Privilege Level: | Operator |
| Format: | dpi modbus copyprofile <P-1> <P-2> |

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-3</td>
<td>readonly</td>
<td>Read only function codes for function code list</td>
</tr>
<tr>
<td></td>
<td>readwrite</td>
<td>Read write function codes for function code list</td>
</tr>
<tr>
<td></td>
<td>programming</td>
<td>Programming function codes for function code list</td>
</tr>
<tr>
<td></td>
<td>all</td>
<td>All possible function codes for function code list (allow any function code)</td>
</tr>
<tr>
<td></td>
<td>advanced</td>
<td>Keeps the function code list from the previous selection and makes it editable by the user</td>
</tr>
<tr>
<td>P-4</td>
<td>1..255</td>
<td>Function codes 1 - 255</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>0-65535</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>0-65535</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0-65535</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0-65535</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>0-65535</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>0-65535</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>Function code read exception status</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>Function code diagnostic</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>Function code get comm event counter</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>Function code get comm event log</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>Function code program (584/984)</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>Function code poll (584/984)</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>0-65535</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>0-65535</td>
</tr>
<tr>
<td></td>
<td>17</td>
<td>Function code report slave id</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>Function code read file record</td>
</tr>
<tr>
<td></td>
<td>21</td>
<td>Function code write file record</td>
</tr>
<tr>
<td></td>
<td>22</td>
<td>0-65535</td>
</tr>
<tr>
<td></td>
<td>23</td>
<td>0-65535</td>
</tr>
<tr>
<td></td>
<td>240</td>
<td>65535</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>Function code program (concept)</td>
</tr>
<tr>
<td></td>
<td>42</td>
<td>Function code concept symbol table</td>
</tr>
<tr>
<td></td>
<td>43</td>
<td>Function code encapsulated interface transport</td>
</tr>
<tr>
<td></td>
<td>48</td>
<td>Function code advantech co. ltd. - management functions</td>
</tr>
<tr>
<td></td>
<td>66</td>
<td>Function code scan data inc. - expanded read holding registers</td>
</tr>
<tr>
<td></td>
<td>67</td>
<td>Function code scan data inc. - expanded write holding registers</td>
</tr>
<tr>
<td></td>
<td>90</td>
<td>Function code unity programming/ofs</td>
</tr>
<tr>
<td></td>
<td>100</td>
<td>Function code scattered register read</td>
</tr>
<tr>
<td></td>
<td>125</td>
<td>Function code schneider electric - firmware replacement</td>
</tr>
<tr>
<td></td>
<td>126</td>
<td>Function code schneider electric - program</td>
</tr>
<tr>
<td>P-5</td>
<td>0..255</td>
<td>Unit identifier 0 - 255</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td>No unit identifier 'none'</td>
</tr>
<tr>
<td>P-6</td>
<td>yes</td>
<td>True</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>False</td>
</tr>
<tr>
<td>P-7</td>
<td>yes</td>
<td>True</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>False</td>
</tr>
<tr>
<td>P-8</td>
<td>yes</td>
<td>True</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>False</td>
</tr>
</tbody>
</table>

12.1.5 dpi modbus delprofile

Deletes a profile from the DPI MODBUS profile table. You cannot delete an active profile or if an enforcer mappings to it.

| Mode: | Global Config Mode |
| Privilege Level: | Operator |
| Format: | dpi modbus delprofile <P-1> |

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile source index 1 - 32</td>
</tr>
<tr>
<td>P-2</td>
<td>1..32</td>
<td>Profile destination index 1 - 32</td>
</tr>
</tbody>
</table>
12.1.6 dpi modbus enableprofile

Enables a profile in the DPI MODBUS profile table. A profile can only be activated when all required parameters are set. After activation modifications no longer possible.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi modbus enableprofile <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index 1 - 32</td>
</tr>
</tbody>
</table>

12.1.7 dpi modbus disableprofile

Disables a profile in the DPI MODBUS profile table. You cannot inactivate a profile if an active enforcer mappings to it.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi modbus disableprofile <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index 1 - 32</td>
</tr>
</tbody>
</table>

12.1.8 dpi opc commit

Writes all changes made in the DPI OPC profiles to the enforcer.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi opc commit

12.1.9 dpi opc addprofile

Adds a profile to the DPI OPC profile table.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi opc addprofile <P-1> [description <P-2>] [sanity-check <P-3>] [fragment-check <P-4>] [timeout-connect <P-5>]

- **description**: Profile description/name for the DPI OPC profile.
- **sanity-check**: Sanity check including format and specification.
- **fragment-check**: Fragment check.
- **timeout-connect**: Timeout at connect.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index 1 - 32</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Profile description/name</td>
</tr>
<tr>
<td>P-3</td>
<td>yes</td>
<td>True</td>
</tr>
<tr>
<td>no</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>P-4</td>
<td>yes</td>
<td>True</td>
</tr>
<tr>
<td>no</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>P-5</td>
<td>0..60</td>
<td>Timeout in seconds 0 - 60</td>
</tr>
</tbody>
</table>

12.1.10 dpi opc modifyprofile

Modifies a profile in the DPI OPC profile table.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi opc modifyprofile <P-1> [description <P-2>] [sanity-check <P-3>] [fragment-check <P-4>] [timeout-connect <P-5>]

- **description**: Profile description/name for the DPI OPC profile.
- **sanity-check**: Sanity check including format and specification.
- **fragment-check**: Fragment check.
- **timeout-connect**: Timeout at connect.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index 1 - 32</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Profile description/name</td>
</tr>
<tr>
<td>P-3</td>
<td>yes</td>
<td>True</td>
</tr>
<tr>
<td>no</td>
<td>False</td>
<td></td>
</tr>
</tbody>
</table>
12.1 dpi

12.1.11 dpi opc copyprofile
Copies a profile to another DPI OPC profile.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi opc copyprofile <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile source index 1 - 32</td>
</tr>
<tr>
<td>P-2</td>
<td>1..32</td>
<td>Profile destination index 1 - 32</td>
</tr>
</tbody>
</table>

12.1.12 dpi opc delprofile
Deleting a profile from the DPI OPC profile table. You cannot delete an active profile or if an enforcer mappings to it.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi opc delprofile <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index 1 - 32</td>
</tr>
</tbody>
</table>

12.1.13 dpi opc enableprofile
Enables a profile in the DPI OPC profile table. A profile can only be activated when all required parameters are set. After activation modifications no longer possible.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi opc enableprofile <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index 1 - 32</td>
</tr>
</tbody>
</table>

12.1.14 dpi opc disableprofile
Disables a profile in the DPI OPC profile table. You cannot inactivate a profile if an active enforcer mappings to it.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi opc disableprofile <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index 1 - 32</td>
</tr>
</tbody>
</table>

12.1.15 dpi iec104 commit
Writes all changes made in the DPI IEC104 profiles to the enforcer.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi iec104 commit

12.1.16 dpi iec104 add
Adds a profile to the DPI IEC104 profile table.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi iec104 add <P-1> [description <P-2>] [function-type <P-3>] [adv-type-id-list <P-4>] [transmission-size <P-5>] [originator-addr-list <P-6>] [common-addr-list <P-7>] [sanity-check <P-8>] [reset <P-9>] [debug <P-10>] [common-addr-size <P-11>] [io-addr-size <P-12>] [allow-101 <P-13>]

- **description:** Description/name for the DPI IEC104 profile.
- **function-type:** Function type.
- **adv-type-id-list:** Advanced type ID list.
- **transmission-size:** Set cause of transmission size.
- **originator-addr-list:** Originator address list (Configurable when cause of transmission size is 2).
- **common-addr-list:** Common address list (For common address size 1, range is 0-255 and for common address size 2, range is 0-65535).
[sanity-check]: Sanity check including format and specification.
[reset]: Reset connection message.
[debug]: Debug output in reset message.
[common-addr-size]: Set common address size.
[io-addr-size]: Set IO address size.
[allow-101]: Allow IEC101 type IDs.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index 1 - 32</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Profile description/name</td>
</tr>
<tr>
<td>P-3</td>
<td>readonly</td>
<td>Read only type IDs for type ID list.</td>
</tr>
<tr>
<td></td>
<td>readable</td>
<td>Read write type IDs for type ID list.</td>
</tr>
<tr>
<td></td>
<td>common</td>
<td>Common type IDs for type ID list.</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>All possible type IDs for type ID list (allow any type ID).</td>
</tr>
<tr>
<td></td>
<td>advanced</td>
<td>Lets the user specify customized type IDs for type ID list.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Meaning</td>
</tr>
<tr>
<td>-----------</td>
<td>-------</td>
<td>---------</td>
</tr>
<tr>
<td>P-4</td>
<td>1.255</td>
<td>Comma separated type ID e.g. 1,2,3.</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Single point information m-sp-na-1</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Single point information with time tag m-sp-ta-1</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Double point information m-dp-na-1</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Double point information with time tag m-dp-ta-1</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Step position information m-st-na-1</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>Step position information with time tag m-st-ta-1</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>Bit string of 32 bit m-bo-na-1</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>Bit string of 32 bit with time tag m-bo-ta-1</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>Measured value, normalized value m-me-na-1</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>Measured value, normalized value with time tag m-me-ta-1</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>Measured value, scaled value m-me-nb-1</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>Measured value, scaled value with time tag m-me-tb-1</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>Measured value, short floating point value m-me-nc-1</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>Measured value, short floating point value with time tag m-me-tc-1</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>Integrated totals m-it-na-1</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>Integrated totals with time tag m-it-ta-1</td>
</tr>
<tr>
<td></td>
<td>17</td>
<td>Event of protection equipment with time tag m-ep-na-1</td>
</tr>
<tr>
<td></td>
<td>18</td>
<td>Packed start events of protection equipment with time tag m-ep-ta-1</td>
</tr>
<tr>
<td></td>
<td>19</td>
<td>Packed output circuit information of protection equipment with time tag m-ep-tc-1</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>Packed single-point information with status change detection m-ps-na-1</td>
</tr>
<tr>
<td></td>
<td>21</td>
<td>Measured value, normalized value without quality descriptor m-me-nd-1</td>
</tr>
<tr>
<td></td>
<td>22</td>
<td>Single point information with time tag cp56time2a m-sp-tb-1</td>
</tr>
<tr>
<td></td>
<td>23</td>
<td>Double point information with time tag cp56time2a m-dp-tb-1</td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>Step position information with time tag cp56time2a m-st-tb-1</td>
</tr>
<tr>
<td></td>
<td>25</td>
<td>Bit string of 32 bit with time tag cp56time2a m-bo-tb-1</td>
</tr>
<tr>
<td></td>
<td>26</td>
<td>Measured value, normalized value with time tag cp56time2a m-me-tb-1</td>
</tr>
<tr>
<td></td>
<td>27</td>
<td>Measured value, scaled value with time tag cp56time2a m-me-te-1</td>
</tr>
<tr>
<td></td>
<td>28</td>
<td>Measured value, short floating point value with time tag cp56time2a m-me-tf-1</td>
</tr>
<tr>
<td></td>
<td>29</td>
<td>Integrated totals with time tag cp56time2a m-it-tb-1</td>
</tr>
<tr>
<td></td>
<td>30</td>
<td>Event of protection equipment with time tag cp56time2a m-ep-tb-1</td>
</tr>
<tr>
<td></td>
<td>31</td>
<td>Packed start events of protection equipment with time tag cp56time2a m-ep-te-1</td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>Packed output circuit information of protection equipment with time tag cp56time2a m-ep-tc-1</td>
</tr>
<tr>
<td></td>
<td>33</td>
<td>Single command c-sc-na-1</td>
</tr>
<tr>
<td></td>
<td>34</td>
<td>Double command c-sc-ta-1</td>
</tr>
<tr>
<td></td>
<td>35</td>
<td>Double command c-sc-tb-1</td>
</tr>
<tr>
<td></td>
<td>36</td>
<td>Double command c-sc-tc-1</td>
</tr>
<tr>
<td></td>
<td>37</td>
<td>Single command with time tag cp56time2a c-sc-ta-1</td>
</tr>
<tr>
<td></td>
<td>38</td>
<td>Double command with time tag cp56time2a c-sc-tb-1</td>
</tr>
<tr>
<td></td>
<td>39</td>
<td>Double command with time tag cp56time2a c-sc-tc-1</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>Setpoint command, normalized value c-se-na-1</td>
</tr>
<tr>
<td></td>
<td>41</td>
<td>Setpoint command, normalized value with time tag cp56time2a c-se-ta-1</td>
</tr>
<tr>
<td></td>
<td>42</td>
<td>Setpoint command, normalized value with time tag cp56time2a c-se-tb-1</td>
</tr>
<tr>
<td></td>
<td>43</td>
<td>Setpoint command, normalized value with time tag cp56time2a c-se-tc-1</td>
</tr>
<tr>
<td></td>
<td>44</td>
<td>Setpoint command, scaled value c-se-nb-1</td>
</tr>
<tr>
<td></td>
<td>45</td>
<td>Setpoint command, scaled value with time tag cp56time2a c-se-tb-1</td>
</tr>
<tr>
<td></td>
<td>46</td>
<td>Setpoint command, scaled value with time tag cp56time2a c-se-tc-1</td>
</tr>
<tr>
<td></td>
<td>47</td>
<td>Bit string 32 bit c-bo-na-1</td>
</tr>
<tr>
<td></td>
<td>48</td>
<td>Bit string 32 bit with time tag c-bo-ta-1</td>
</tr>
<tr>
<td></td>
<td>49</td>
<td>Bit string 32 bit with time tag c-bo-tb-1</td>
</tr>
<tr>
<td></td>
<td>50</td>
<td>Bit string 32 bit with time tag c-bo-tc-1</td>
</tr>
<tr>
<td></td>
<td>51</td>
<td>End of initialization m-ei-na-1</td>
</tr>
<tr>
<td></td>
<td>52</td>
<td>(General-) Interrogation command c-ic-na-1</td>
</tr>
<tr>
<td></td>
<td>53</td>
<td>Counter interrogation command c-ci-na-1</td>
</tr>
<tr>
<td></td>
<td>54</td>
<td>Read command c-rd-na-1</td>
</tr>
<tr>
<td></td>
<td>55</td>
<td>Clock synchronization command c-cs-na-1</td>
</tr>
<tr>
<td></td>
<td>56</td>
<td>(IEC 101) Test command c-ts-na-1</td>
</tr>
<tr>
<td></td>
<td>57</td>
<td>(IEC 101) Delay acquisition command c-cd-na-1</td>
</tr>
<tr>
<td></td>
<td>58</td>
<td>Test command with time tag cp56time2a c-ts-ta-1</td>
</tr>
<tr>
<td></td>
<td>59</td>
<td>Parameter of measured value, normalized value p-me-na-1</td>
</tr>
<tr>
<td></td>
<td>60</td>
<td>Parameter of measured value, normalized value with time tag p-me-ta-1</td>
</tr>
<tr>
<td></td>
<td>61</td>
<td>Parameter of measured value, scaled value p-me-nb-1</td>
</tr>
<tr>
<td></td>
<td>62</td>
<td>Parameter of measured value, scaled value with time tag p-me-tb-1</td>
</tr>
<tr>
<td></td>
<td>63</td>
<td>Parameter of measured value, short floating point value p-me-nc-1</td>
</tr>
<tr>
<td></td>
<td>64</td>
<td>Parameter of measured value, short floating point value with time tag p-me-tc-1</td>
</tr>
</tbody>
</table>
### 12.1.17 dpi iec104 modify

Modifies a profile in the DPI IEC104 profile table.

- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: `dpi iec104 modify <P-1> [description <P-2>] [function-type <P-3>] [adv-type-id-list <P-4>] [transmission-size <P-5>] [originator-addr-list <P-6>] [common-addr-list <P-7>] [sanity-check <P-8>] [reset <P-9>] [debug <P-10>] [common-addr-size <P-11>] [io-addr-size <P-12>] [allow-101 <P-13>]`

**[description]**: Description/name for the DPI IEC104 profile.

**[function-type]**: Function type.

**[adv-type-id-list]**: Advanced type ID list.

**[transmission-size]**: Set cause of transmission size.

**[originator-addr-list]**: Originator address list (Configurable when cause of transmission size is 2).

**[common-addr-list]**: Common address list (For common address size 1, range is 0-255 and for common address size 2, range is 0-65535).

**[sanity-check]**: Sanity check including format and specification.

**[reset]**: Reset connection message.

**[debug]**: Debug output in reset message.

**[io-addr-size]**: Set IO address size.

**[common-addr-size]**: Set Common Address Size.

**[allow-101]**: Allow IEC101 type IDs.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index 1 - 32</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Profile description/name</td>
</tr>
<tr>
<td>P-3</td>
<td>readonly</td>
<td>Read only type IDs for type ID list.</td>
</tr>
<tr>
<td></td>
<td>readwrite</td>
<td>Read write type IDs for type ID list.</td>
</tr>
<tr>
<td></td>
<td>common</td>
<td>Common type IDs for type ID list.</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>All possible type IDs for type ID list (allow any type ID).</td>
</tr>
<tr>
<td></td>
<td>advanced</td>
<td>Lets the user specify customized type IDs for type ID list.</td>
</tr>
</tbody>
</table>
Parameter | Value | Meaning
---|---|---
P-4 | 1.255 | Comma separated type ID e.g. 1,2,3.
1 | Single point information m-sp-na-1
2 | Single point information with time tag m-sp-ta-1
3 | Double point information m-dp-na-1
4 | Double point information with time tag m-dp-ta-1
5 | Step position information m-st-na-1
6 | Step position information with time tag m-st-ta-1
7 | Bit string of 32 bit m-bo-na-1
8 | Bit string of 32 bit with time tag m-bo-ta-1
9 | Measured value, normalized value m-me-na-1
10 | Measured value, normalized value with time tag m-me-ta-1
11 | Measured value, scaled value m-me-nb-1
12 | Measured value, short floating point value m-me-nc-1
13 | Measured value, short floating point value with time tag m-me-tc-1
14 | Integrated totals m-it-na-1
15 | Integrated totals with time tag m-it-ta-1
16 | Event of protection equipment with time tag m-ep-ta-1
17 | Packed start events of protection equipment with time tag m-ep-tb-1
18 | Packed output circuit information of protection equipment with time tag m-ep-tc-1
19 | Packed single point information with status change detection m-ps-na-1
20 | Measured value, normalized value without quality descriptor m-me-nd-1
21 | Single point information with time tag cp56time2a m-sp-tb-1
22 | Double point information with time tag cp56time2a m-dp-tb-1
23 | Step position information with time tag cp56time2a m-st-tb-1
24 | Bit string of 32 bit with time tag cp56time2a m-bo-tb-1
25 | Measured value, normalized value with time tag cp56time2a m-me-tb-1
26 | Measured value, scaled value with time tag cp56time2a m-me-te-1
27 | Measured value, short floating point value with time tag cp56time2a m-me-tf-1
28 | Integrated totals with time tag cp56time2a m-it-tb-1
29 | Event of protection equipment with time tag cp56time2a m-ep-td-1
30 | Packed start events of protection equipment with time tag cp56time2a m-ep-te-1
31 | Packed output circuit information of protection equipment with time tag cp56time2a m-ep-tc-1
32 | Single command c-sc-na-1
33 | Double command c-dc-na-1
34 | Regulating step command c-rc-na-1
35 | Setpoint command, normalized value c-se-na-1
36 | Setpoint command, scaled value c-se-nb-1
37 | Setpoint command, short floating point value c-se-nc-1
38 | Bit string 32 bit c-bo-na-1
39 | Single command with time tag cp56time2a c-sc-ta-1
40 | Double command with time tag cp56time2a c-dc-ta-1
41 | Regulating step command with time tag cp56time2a c-rc-ta-1
42 | Setpoint command, normalized value with time tag cp56time2a c-se-ta-1
43 | Setpoint command, scaled value with time tag cp56time2a c-se-tb-1
44 | Setpoint command, short floating point value with time tag cp56time2a c-se-tc-1
45 | Bit string 32 bit with time tag cp56time2a c-bo-ta-1
46 | End of initialization m-el-na-1
47 | (General-) Interrogation command c-ic-na-1
48 | Counter interrogation command c-ci-na-1
49 | Read command c-rd-na-1
50 | Clock synchronization command c-cs-na-1
51 | ( IEC 101 ) Test command c-ts-nb-1
52 | ( IEC 101 ) Delay acquisition command c-dl-na-1
53 | Test command with time tag cp56time2a c-ts-ta-1
54 | Parameter of measured value, normalized value p-me-na-1
55 | Parameter of measured value, scaled value p-me-nb-1
56 | Parameter of measured value, short floating point value p-me-nc-1
57 | Parameter activation p-act-na-1
58 | File ready f-fr-na-1
59 | Section ready f-sr-na-1
60 | Call directory, select file, call file, call section f-sc-na-1
12.1.18 dpi iec104 delete

Deletes a profile from the DPI IEC104 profile table. You cannot delete an active profile or if an enforcer maps to it.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `dpi iec104 delete <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-5</td>
<td>1..2</td>
<td>Specify the cause-of-transmission size.</td>
</tr>
</tbody>
</table>

12.1.19 dpi iec104 enable

Enables a profile in the DPI IEC104 profile table. A profile can only be activated when all required parameters are set. After activation no modifications are possible.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `dpi iec104 enable <P-1>`

12.1.20 dpi iec104 disable

Disables a profile in the DPI IEC104 profile table. You cannot deactivate a profile if an active enforcer maps to it.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `dpi iec104 disable <P-1>`

12.1.21 dpi iec104 copy

Copies a profile to another DPI IEC104 profile.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `dpi iec104 copy <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index 1 - 32</td>
</tr>
<tr>
<td>P-2</td>
<td>1..32</td>
<td>Profile destination index 1 - 32</td>
</tr>
</tbody>
</table>
12.1.22 dpi dnp3 profile add

Adds a profile to the DPI DNP3 profile table.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `dpi dnp3 profile add <P-1> [description <P-2>] [function-code-list <P-3>] [default-object-list <P-4>] [sanity-check <P-5>] [crc-check <P-6>] [outstation-packets-check <P-7>] [reset-tcp-check <P-8>]`

  - `[description]`: Profile description/name for the DPI DNP3 profile.
  - `[function-code-list]`: Function code list. A function code has the syntax 'val'. Function codes are separated by a comma.
  - `[default-object-list]`: Object entries to be included from Default white list.
  - `[sanity-check]`: Sanity check including format and specification.
  - `[crc-check]`: CRC verification for DNP3 data link layer frames.
  - `[outstation-packets-check]`: Check the DNP3 data packets originating at an outstation.
  - `[reset-tcp-check]`: Reset the TCP connection in case of a protocol violation or if the plausibility check leads to errors.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>DNP3 profile index.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Profile description/name for the DNP3 profile.</td>
</tr>
<tr>
<td>P-3</td>
<td>0..255</td>
<td>Function codes for the DNP3 profile.</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>Confirm</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Read</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Write</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Select</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Operate</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Direct Operate</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>Direct Operate-No Response Required</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>Freeze</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>Freeze-No Response Required</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>Freeze Clear</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>Freeze Clear-No Response Required</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>Freeze At Time</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>Freeze At Time-No Response Required</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>Cold Restart</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>Warm Restart</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>Initialize Data</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>Initialize Application</td>
</tr>
<tr>
<td></td>
<td>17</td>
<td>Start Application</td>
</tr>
<tr>
<td></td>
<td>18</td>
<td>Stop Application</td>
</tr>
<tr>
<td></td>
<td>19</td>
<td>Save Configuration</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>Enable Unsolicited Messages</td>
</tr>
<tr>
<td></td>
<td>21</td>
<td>Disable Unsolicited Messages</td>
</tr>
<tr>
<td></td>
<td>22</td>
<td>Assign Class</td>
</tr>
<tr>
<td></td>
<td>23</td>
<td>Delay Measurement</td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>Record Current Time</td>
</tr>
<tr>
<td></td>
<td>25</td>
<td>Open File</td>
</tr>
<tr>
<td></td>
<td>26</td>
<td>Close File</td>
</tr>
<tr>
<td></td>
<td>27</td>
<td>Delete File</td>
</tr>
<tr>
<td></td>
<td>28</td>
<td>Get File Information</td>
</tr>
<tr>
<td></td>
<td>29</td>
<td>Authenticate File</td>
</tr>
<tr>
<td></td>
<td>30</td>
<td>Abort File Transfer</td>
</tr>
<tr>
<td></td>
<td>31</td>
<td>Activate Configuration</td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>Authenticate Request</td>
</tr>
<tr>
<td></td>
<td>33</td>
<td>Authenticate Request-No Acknowledgement</td>
</tr>
<tr>
<td></td>
<td>129</td>
<td>Response</td>
</tr>
<tr>
<td></td>
<td>130</td>
<td>Unsolicited Response</td>
</tr>
<tr>
<td></td>
<td>131</td>
<td>Authentication Response</td>
</tr>
<tr>
<td>P-4</td>
<td>1..317</td>
<td>Comma separated index values e.g 1,2,3.</td>
</tr>
<tr>
<td>P-5</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>
12.1.23 dpi dnp3 profile modify

Modifies a profile to the DPI DNP3 profile table.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator

**Format:**
```
dpi dnp3 profile modify <P-1> [description <P-2>] [function-code-list <P-3>] [default-object-list <P-4>] [sanity-check <P-5>] [crc-check <P-6>] [outstation-packets-check <P-7>] [reset-tcp-check <P-8>]
```

- **[description]:** Profile description/name for the DPI DNP3 profile.
- **[function-code-list]:** Function code list. A function code has the syntax 'val'. Function codes are separated by a comma.
- **[default-object-list]:** Object entries to be included from Default white list.
- **[sanity-check]:** Sanity check including format and specification.
- **[crc-check]:** CRC verification for DNP3 data link layer frames.
- **[outstation-packets-check]:** Check the DNP3 data packets originating at an outstation.
- **[reset-tcp-check]:** Reset the TCP connection in case of a protocol violation or if the plausibility check leads to errors.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>DNP3 profile index.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Profile description/name for the DNP3 profile.</td>
</tr>
</tbody>
</table>
12.1.24 dpi dnp3 profile delete

Deletes a profile from the DPI DNP3 profile table. You cannot delete an active profile or if an enforcer mappings to it.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi dnp3 profile delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>DNP3 profile index.</td>
</tr>
</tbody>
</table>
12.1.25 dpi dnp3 profile enable

Enables a profile in the DPI DNP3 profile table. A profile can only be activated when all required parameters are set. After activation modifications no longer possible.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi dnp3 profile enable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>DNP3 profile index.</td>
</tr>
</tbody>
</table>

12.1.26 dpi dnp3 profile disable

Disables a profile in the DPI DNP3 profile table. You cannot inactivate a profile if an active enforcer mappings to it.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi dnp3 profile disable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>DNP3 profile index.</td>
</tr>
</tbody>
</table>

12.1.27 dpi dnp3 profile commit

Writes all changes made in the DPI DNP3 profiles to the enforcer.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi dnp3 profile commit

12.1.28 dpi dnp3 profile copy

Copies a profile to another DPI DNP3 profile.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi dnp3 profile copy <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Source index of DPI DNP3 profile.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..32</td>
<td>Destination index of DPI DNP3 profile.</td>
</tr>
</tbody>
</table>

12.1.29 dpi dnp3 object add

Adds an object to a DPI DNP3 rule.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi dnp3 object <P-1> add <P-2> object-type <P-3> group-number <P-4> variation-number <P-5> function-code <P-6> [function-name <P-7>] [function-length <P-8>] [qualifier-code-list <P-9>]

- **object-type:** Object type for DPI DNP3 object.
- **group-number:** Group number for DNP3 object ranging 0-255.
- **variation-number:** Variation number for DNP3 object could either be any integer between 0-255 or a range from 0-255.
- **function-code:** Function code for DNP3 object.
- **[function-name]:** Function name for DNP3 object.
- **[function-length]:** Function length for DNP3 Object.
- **[qualifier-code-list]:** Qualifier code list, hexadecimal numbers separated by a comma(e.g numbers ranging between 0x00 to 0xFF).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>DNP3 profile index.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..32</td>
<td>DNP3 Object index.</td>
</tr>
<tr>
<td>P-3</td>
<td>request</td>
<td>Request</td>
</tr>
<tr>
<td></td>
<td>response</td>
<td>Response</td>
</tr>
<tr>
<td>P-4</td>
<td>0..255</td>
<td>Group number for DNP3 object.</td>
</tr>
<tr>
<td>P-5</td>
<td>string</td>
<td>Variation Number for DNP3 object.</td>
</tr>
<tr>
<td>P-6</td>
<td>0..255</td>
<td>Function code for DNP3 object.</td>
</tr>
<tr>
<td>P-7</td>
<td>string</td>
<td>Function Name for DNP3 object.</td>
</tr>
<tr>
<td>P-8</td>
<td>string</td>
<td>Function Length for DNP3 object.</td>
</tr>
<tr>
<td>P-9</td>
<td>string</td>
<td>Qualifier code list, hexadecimal numbers separated by a comma(e.g numbers ranging between 0x00 to 0xFF).</td>
</tr>
</tbody>
</table>
12.1.30 dpi dnp3 object delete

Deletes an object from a DPI DNP3 rule.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi dnp3 object <P-1> delete <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>DNP3 profile index.</td>
</tr>
<tr>
<td>P-2</td>
<td>1.256</td>
<td>DNP3 Object index.</td>
</tr>
</tbody>
</table>

12.1.31 dpi amp profile add

Adds a profile to the DPI AMP profile table.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi amp profile add <P-1> [description <P-2>] [protocol <P-3>] [message-type <P-4>] [address-class <P-5>] [device-class <P-6>] [memory-address <P-7>] [data-word <P-8>] [task-code <P-9>] [task-code-data <P-10>] [error-check-characters <P-11>] [block-check-characters <P-12>] [debug <P-13>] [tcp-reset <P-14>] [sanity-check <P-15>]

  - **[description]:** Specify the description/name for the DPI AMP profile. The description consists of an alphanumeric ASCII character string with 0..32 characters
  - **[protocol]:** Specify the protocol type for the DPI AMP profile.
  - **[message-type]:** Specify the value for the message type which specifies the type of data in the message data area and also specifies if the message is a command or a response. The allowed message types are 02,03,04,05,06,07,08,09,FF,any.
  - **[address-class]:** Specify the particular type of the memory to be accessed, (total number of hexadecimal values can be specified up to 205).
  - **[device-class]:** Specify the value for the device class, (total number of hexadecimal values can be specified up to 205).
  - **[memory-address]:** Specify the beginning address of the memory to be read or written, (total number of hexadecimal values can be specified up to 205).
  - **[data-word]:** Specify the value for the data words to be read from the remote device, (total number of hexadecimal values can be specified up to 205).
  - **[task-code]:** Specify the value for the task code.
  - **[task-code-data]:** Specify the hexadecimal value 0..F in the field task code data. The maximum task code data length is up to 72 bytes
  - **[error-check-characters]:** Enable/disable the checking for the NITP error check characters (ECC) of the packets.
  - **[block-check-characters]:** Enable/disable the checking for the CAMP block check characters (BCC) of the AMP packets.
  - **[debug]:** Enable/disable the debugging in the DPI AMP profile, (if it is enabled then the reset connection message will contain the debug information).
  - **[tcp-reset]:** Enable/disable the resetting of the TCP connection, (if it is enabled then the TCP reset connection message will be sent in case a packet is dropped).
  - **[sanity-check]:** Enable/disable the sanity check including format and specification of all the AMP packets.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Profile description/name</td>
</tr>
<tr>
<td>P-3</td>
<td>camp</td>
<td>CAMP protocol</td>
</tr>
<tr>
<td></td>
<td>nitp</td>
<td>NITP protocol</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>The device applies the rule to every data packet without evaluating the protocol.</td>
</tr>
<tr>
<td>P-4</td>
<td>any</td>
<td>The device applies the rule to every data packet without evaluating the message type.</td>
</tr>
<tr>
<td></td>
<td>02-09,FF</td>
<td>Enter message type with hexadecimal values separated by a comma, for example, 02,03,FF.</td>
</tr>
<tr>
<td>P-5</td>
<td>any</td>
<td>The device applies the rule to every data packet without evaluating the address class.</td>
</tr>
<tr>
<td></td>
<td>0000-FFFF</td>
<td>Enter address class range with hexadecimal values connected by a hyphen, for example, 0000-000A.</td>
</tr>
<tr>
<td></td>
<td>0000-FFFF</td>
<td>Enter address class with hexadecimal values separated by a comma, for example, 0001,0003,FFFF.</td>
</tr>
<tr>
<td></td>
<td>0000-FFFF</td>
<td>Enter combination of address class and address class range, for example, 0001,0003,0004-000A.</td>
</tr>
</tbody>
</table>


Deep Packet Inspection (DPI)

12.1 dpi

### 12.1.32 dpi amp profile copy

Copies a profile to another DPI AMP profile.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi amp profile copy <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile source index</td>
</tr>
<tr>
<td>P-2</td>
<td>1..32</td>
<td>Profile destination index</td>
</tr>
</tbody>
</table>

### 12.1.33 dpi amp profile delete

Deletes a profile from the DPI AMP profile table. You cannot delete an active profile or if an enforcer mapped to it.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi amp profile delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index</td>
</tr>
</tbody>
</table>

### 12.1.34 dpi amp profile disable

Disables a profile in the DPI AMP profile table. You cannot deactivate a profile if an active enforcer mapped to it.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi amp profile disable <P-1>
Deep Packet Inspection (DPI)

12.1 dpi

12.1.35 dpi amp profile enable

Enables a profile in the DPI AMP profile table. A profile can only be activated when all required parameters are set. After activation no modifications are possible.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi amp profile enable <P-1>

```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index</td>
</tr>
</tbody>
</table>
```

12.1.36 dpi amp profile modify

Modifies a profile in the DPI AMP profile table.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi amp profile modify <P-1> [description <P-2>] [protocol <P-3>] [message-type <P-4>] [address-class <P-5>] [device-class <P-6>] [memory-address <P-7>] [data-word <P-8>] [task-code <P-9>] [task-code-data <P-10>] [error-check-characters <P-11>] [block-check-characters <P-12>] [debug <P-13>] [tcp-reset <P-14>] [sanity-check <P-15>]

- **description:** Specify the description/name for the DPI AMP profile. The description consists of an alphanumeric ASCII character string with 0..32 characters.
- **protocol:** Specify the protocol type for the DPI AMP profile.
- **message-type:** Specify the type of protocol, message includes the data in the message data area. Also specifies if the message is a command or a response. The allowed message types are 02,03,04,05,06,07,08,09,FF,any.
- **address-class:** Specify the particular type of the memory to be accessed, (total number of hexadecimal values can be specified upto 205).
- **device-class:** Specify the value for the device class, (total number of hexadecimal values can be specified upto 205).
- **memory-address:** Specify the beginning address of the memory to be read or written, (total number of hexadecimal values can be specified upto 205).
- **data-word:** Specify the value for the data words to be read from the remote device, (total number of hexadecimal values can be specified upto 205).
- **task-code:** Specify the value for the task code.
- **task-code-data:** Specify the hexadecimal value 0..F in the field task code data. The maximum task code data length is up to 72 bytes.
- **error-check-characters:** Enable/disable the checking for the NITP error check characters (ECC) of the packets.
- **block-check-characters:** Enable/disable the checking for the CAMP block check characters (BCC) of the AMP packets.
- **debug:** Enable/disable the debugging in the DPI AMP profile, (if it is enabled then the reset connection message will contain the debug information).
- **tcp-reset:** Enable/disable the resetting of the TCP connection, (if it is enabled then the TCP reset connection message will be sent in case a packet is dropped).
- **sanity-check:** Enable/disable the sanity check including format and specification of all the AMP packets.

```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>Profile index</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Profile description/name</td>
</tr>
<tr>
<td>P-3</td>
<td>camp</td>
<td>CAMP protocol</td>
</tr>
<tr>
<td></td>
<td>nitp</td>
<td>NITP protocol</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>The device applies the rule to every data packet without evaluating the protocol.</td>
</tr>
<tr>
<td>P-4</td>
<td>any</td>
<td>The device applies the rule to every data packet without evaluating the message type.</td>
</tr>
<tr>
<td></td>
<td>02-09,FF</td>
<td>Enter message type with hexadecimal values separated by a comma, for example, 02,03,FF.</td>
</tr>
</tbody>
</table>
```
12.1.37 dpi amp commit

Writes all changes made in the DPI AMP profiles to the enforcer.

- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: dpi amp commit

12.1.38 dpi amp task-code add

Add a value for the task code.

- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: dpi amp task-code add <P-1> [description <P-2>] [mode <P-3>]

- **description**: Specify the description for the task code. The description consists of an alphanumeric ASCII character string with 0..32 characters.
- **mode**: Specify the value for the task code mode (i.e. config or non-config).
Deep Packet Inspection (DPI)

12.2 show

Display device options and settings.

12.2.1 show dpi modbus profiletable

Display the DPI MODBUS profile table.

Parameter | Value | Meaning
---|---|---
P-2 | string | Enter the description for the task code.
P-3 | config | Specify the value config for the task code.
| non-config | Specify the value non-config for the task code.

**12.1.39 dpi amp task-code delete**

Delete a value for the task code.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi amp task-code delete <P-1>

Parameter | Value | Meaning
---|---|---
P-1 | 00-FF | Enter task code with hexadecinal value. The range is from 00 to FF.

**12.1.40 dpi amp task-code modify**

Modify a value for the task code.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi amp task-code modify <P-1> [description <P-2>] [mode <P-3>]

- **[description]:** Specify the description for the task code. The description consists of an alphanumeric ASCII character string with 0..32 characters.
- **[mode]:** Specify the value for the task code mode (i.e. config or non-config).

Parameter | Value | Meaning
---|---|---
P-1 | 00-FF | Enter task code with hexadecinal value. The range is from 00 to FF.
P-2 | string | Enter the description for the task code.
P-3 | config | Specify the value config for the task code.
| non-config | Specify the value non-config for the task code.

**12.1.41 dpi amp protect-mode**

Enable/disable the program and mode protect.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi amp protect-mode <P-1>

Parameter | Value | Meaning
---|---|---
P-1 | enable | Enable the option.
| disable | Disable the option.

**12.1.42 dpi amp digital-input**

Enable/disable the digital input.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** dpi amp digital-input <P-1>

Parameter | Value | Meaning
---|---|---
P-1 | enable | Enable the option.
| disable | Disable the option.

---
12.2.2  show dpi modbus pending
Display whether uncommitted changes for DPI MODBUS enforcer exist.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: show dpi modbus pending

12.2.3  show dpi opc profiletable
Display the DPI OPC profile table.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: show dpi opc profiletable

12.2.4  show dpi opc pending
Display whether uncommitted changes for DPI OPC enforcer exist.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: show dpi opc pending

12.2.5  show dpi iec104 profiletable
Display the DPI IEC104 profile table.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: show dpi iec104 profiletable

12.2.6  show dpi iec104 pending
Display whether uncommitted changes for DPI IEC104 enforcer exist.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: show dpi iec104 pending

12.2.7  show dpi dnp3 profiletable
Display the DPI DNP3 profile table.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: show dpi dnp3 profiletable

12.2.8  show dpi dnp3 pending
Display whether uncommitted changes for DPI DNP3 enforcer exist.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: show dpi dnp3 pending

12.2.9  show dpi dnp3 objectlist
Display the DPI DNP3 object list for a profile.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: show dpi dnp3 objectlist <P-1> [P-2>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..32</td>
<td>DNP3 profile index.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..256</td>
<td>DNP3 Object index.</td>
</tr>
</tbody>
</table>

12.2.10 show dpi amp global
Display the AMP global information and settings.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: show dpi amp global
12.2.11 show dpi amp profiletable
Display the DPI AMP profile table.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show dpi amp profiletable

12.2.12 show dpi amp taskcodetable
Display the DPI AMP task code table.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show dpi amp taskcodetable
13 Filtering Database (FDB)

13.1 mac-filter

13.1.1 mac-filter

Static MAC filter configuration.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `mac-filter <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>aa:bb:cc:dd:ee:ff</td>
<td>MAC address.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
</tbody>
</table>

**no mac-filter**

Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `no mac-filter <P-1> <P-2>`

13.2 bridge

Bridge configuration.

13.2.1 bridge aging-time

Aging time configuration.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `bridge aging-time <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>10..500000</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

13.3 show

Display device options and settings.

13.3.1 show mac-filter-table static

Display the MAC address filter table.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show mac-filter-table static`

13.4 show

Display device options and settings.

13.4.1 show bridge aging-time

Address aging time.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show bridge aging-time`
13.5  **show**

Display device options and settings.

### 13.5.1  **show mac-addr-table**

Display the MAC address table.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show mac-addr-table [<P-1>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>a:b:c:d:e:f</td>
<td>Enter a MAC address.</td>
</tr>
<tr>
<td></td>
<td>1..4042</td>
<td>Enter a VLAN ID.</td>
</tr>
</tbody>
</table>

13.6  **clear**

Clear several items.

### 13.6.1  **clear mac-addr-table**

Clears the MAC address table.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** `clear mac-addr-table`
14 Firewall Learning Mode (FLM)

14.1 flm
Configure the firewall learning mode.

14.1.1 flm operation
Enable/disable the firewall learning mode.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** flm operation <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>enable</td>
<td>Enable the firewall learning mode.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the firewall learning mode.</td>
</tr>
</tbody>
</table>

- **no flm operation**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Operator
  - **Format:** no flm operation <P-1>

14.1.2 flm action
Set the action for the firewall learning mode.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** flm action <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>start</td>
<td>Start a learning phase.</td>
</tr>
<tr>
<td></td>
<td>stop</td>
<td>Stop a learning phase.</td>
</tr>
<tr>
<td></td>
<td>continue</td>
<td>Continue the previous learning phase.</td>
</tr>
<tr>
<td></td>
<td>clear</td>
<td>Clear the learned data.</td>
</tr>
</tbody>
</table>

14.1.3 flm interface add
Add an interface to the firewall learning mode.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** flm interface add <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

14.1.4 flm interface delete
Delete an interface from the firewall learning mode.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** flm interface delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

14.2 show
Display device options and settings.
14.2.1 show flm global
Display the information and settings for the firewall learning mode.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show flm global

14.2.2 show flm interface
Display the interfaces selected for the firewall learning mode.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show flm interface
HiDiscovery

15 HiDiscovery

15.1 network
Configure the inband and outband connectivity.

15.1.1 network hidiscovery operation
Enable/disable the HiDiscovery protocol on this device.
- Mode: Privileged Exec Mode
- Privilege Level: Operator
- Format: network hidiscovery operation <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>enable</td>
<td>Enable the HiDiscovery protocol.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the HiDiscovery protocol.</td>
</tr>
</tbody>
</table>

no network hidiscovery operation
Disable the option
- Mode: Privileged Exec Mode
- Privilege Level: Operator
- Format: no network hidiscovery operation <P-1>

15.1.2 network hidiscovery mode
Set the access level for HiDiscovery.
- Mode: Privileged Exec Mode
- Privilege Level: Operator
- Format: network hidiscovery mode <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>read-write</td>
<td>Allow detection and configuration.</td>
</tr>
<tr>
<td></td>
<td>read-only</td>
<td>Allow only detection, no configuration.</td>
</tr>
</tbody>
</table>

15.1.3 network hidiscovery blinking
Enable/disable the HiDiscovery blinking sequence on this device. This preference is not saved in configuration
- Mode: Privileged Exec Mode
- Privilege Level: Operator
- Format: network hidiscovery blinking

no network hidiscovery blinking
Disable the option
- Mode: Privileged Exec Mode
- Privilege Level: Operator
- Format: no network hidiscovery blinking

15.2 show
Display device options and settings.

15.2.1 show network hidiscovery
Display the HiDiscovery settings.
- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show network hidiscovery
16 Hypertext Transfer Protocol (HTTP)

16.1 http
Set HTTP parameters.

16.1.1 http port
Set the HTTP port number.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** http port <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..65535</td>
<td>Port number of the HTTP server (default: 80).</td>
</tr>
</tbody>
</table>

16.1.2 http server
Enable or disable the HTTP server.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** http server

**no http server**
Disable the option
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** no http server

16.2 show
Display device options and settings.

16.2.1 show http
Display the HTTP server information.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show http
17 HTTP Secure (HTTPS)

17.1 https
Set HTTPS parameters.

17.1.1 https server
Enable or disable the HTTPS server.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: https server

no https server
Disable the option
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: no https server

17.1.2 https port
Set the HTTPS port number.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: https port <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..65535</td>
<td>Port number of the web server (default: 443).</td>
</tr>
</tbody>
</table>

17.1.3 https fingerprint-type
Configure fingerprint type.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: https fingerprint-type <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>sha1</td>
<td>Configure sha1 fingerprint</td>
</tr>
<tr>
<td></td>
<td>sha256</td>
<td>Configure sha256 fingerprint</td>
</tr>
</tbody>
</table>

17.1.4 https certificate
Generate/Delete HTTPS X509/PEM certificate.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: https certificate <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>generate</td>
<td>Generates the item</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td>Deletes the item</td>
</tr>
</tbody>
</table>

17.2 copy
Copy different kinds of items.

17.2.1 copy https cert remote
Copy X509/PEM certificate from a server to the specified destination.
- Mode: Privileged Exec Mode
- Privilege Level: Administrator
- Format: copy https cert remote <P-1> nvm
  nvm: Copy HTTPS certificate (PEM) from a server to the device.
### 17.3 show
Display device options and settings.

#### 17.3.1 show https
Display the HTTPS server information.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: show https

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>

---

**17.2.2 copy https cert envm**
Copy X509/PEM certificate from external non-volatile memory to the specified destination.
- **Mode**: Privileged Exec Mode
- **Privilege Level**: Administrator
- **Format**: copy https cert envm <P-1> nvm

nvm: Copy X509/PEM certificate from external non-volatile memory to the device.
18 Interface

18.1 shutdown

18.1.1 shutdown
Enable or disable the interface.
- Mode: Interface Range Mode
- Privilege Level: Operator
- Format: shutdown

no shutdown
Disable the option
- Mode: Interface Range Mode
- Privilege Level: Operator
- Format: no shutdown

18.2 auto-negotiate

18.2.1 auto-negotiate
Enable or disable automatic negotiation on the interface. The cable crossing settings have no effect if auto-negotiation is enabled. In this case cable crossing is always set to auto. Cable crossing is set to the value chosen by the user if auto-negotiation is disabled.
- Mode: Interface Range Mode
- Privilege Level: Operator
- Format: auto-negotiate

no auto-negotiate
Disable the option
- Mode: Interface Range Mode
- Privilege Level: Operator
- Format: no auto-negotiate

18.3 auto-power-down

18.3.1 auto-power-down
Set the auto-power-down mode on the interface.
- Mode: Interface Range Mode
- Privilege Level: Operator
- Format: auto-power-down <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>auto-power-save</td>
<td>The port goes in a low power mode.</td>
</tr>
<tr>
<td></td>
<td>no-power-save</td>
<td>The port does not use the automatic power save mode.</td>
</tr>
</tbody>
</table>
18.4 cable-crossing

18.4.1 cable-crossing

Cable crossing settings on the interface. The cable crossing settings have no effect if auto-negotiation is enabled. In this case cable crossing is always set to auto. Cable crossing is set to the value chosen by the user if auto-negotiation is disabled.

- **Mode**: Interface Range Mode
- **Privilege Level**: Operator
- **Format**: `cable-crossing <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>mdi</td>
<td>The port does not use the crossover mode.</td>
</tr>
<tr>
<td></td>
<td>mdix</td>
<td>The port uses the crossover mode.</td>
</tr>
<tr>
<td></td>
<td>auto-mdix</td>
<td>The port uses the auto crossover mode.</td>
</tr>
</tbody>
</table>

18.5 linktraps

18.5.1 linktraps

Enable/disable link up/down traps on the interface.

- **Mode**: Interface Range Mode
- **Privilege Level**: Operator
- **Format**: `linktraps`

- **no linktraps**

  Disable the option

  - **Mode**: Interface Range Mode
  - **Privilege Level**: Operator
  - **Format**: `no linktraps`

18.6 speed

18.6.1 speed

Sets the speed and duplex setting for the interface.

- **Mode**: Interface Range Mode
- **Privilege Level**: Operator
- **Format**: `speed <P-1> [P-2]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10</td>
<td>10 MBit/s.</td>
</tr>
<tr>
<td></td>
<td>100</td>
<td>100 MBit/s.</td>
</tr>
<tr>
<td></td>
<td>1000</td>
<td>1000 MBit/s.</td>
</tr>
<tr>
<td>P-2</td>
<td>full</td>
<td>full duplex.</td>
</tr>
<tr>
<td></td>
<td>half</td>
<td>half duplex.</td>
</tr>
</tbody>
</table>

18.7 name

18.7.1 name

Set or remove a descriptive name for the interface.

- **Mode**: Interface Range Mode
- **Privilege Level**: Operator
- **Format**: `name <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
</table>
|           | string| Enter a user-defined text, max. 64 characters.
18.8 power-state

18.8.1 power-state
Enable or disable the power state on the interface. The interface power state settings have no effect if the interface admin state is enabled.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** power-state

- **no power-state**
  Disable the option
  - **Mode:** Interface Range Mode
  - **Privilege Level:** Operator
  - **Format:** no power-state

18.9 mac-filter

18.9.1 mac-filter
static mac filter configuration

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** mac-filter <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>aa:bb:cc:dd:ee:ff</td>
<td>MAC address.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
</tbody>
</table>

- **no mac-filter**
  Disable the option
  - **Mode:** Interface Range Mode
  - **Privilege Level:** Operator
  - **Format:** no mac-filter <P-1> <P-2>

18.10 show

Display device options and settings.

18.10.1 show port

Display the interface parameters.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show port [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

18.11 show

Display device options and settings.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show
18.12 show

Display device options and settings.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show
19 Interface Statistics

19.1 utilization
Configure the interface utilization parameters.

19.1.1 utilization control-interval
Add interval time to monitor the bandwidth utilization of the interface.
- Mode: Interface Range Mode
- Privilege Level: Operator
- Format: utilization control-interval <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..3600</td>
<td>Add interval time to monitor the bandwidth utilization.</td>
</tr>
</tbody>
</table>

19.1.2 utilization alarm-threshold lower
Lower threshold value
- Mode: Interface Range Mode
- Privilege Level: Operator
- Format: utilization alarm-threshold lower <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..10000</td>
<td>Add alarm threshold lower value for monitoring bandwidth utilization in hundredths of a percent.</td>
</tr>
</tbody>
</table>

19.1.3 utilization alarm-threshold upper
Upper threshold value
- Mode: Interface Range Mode
- Privilege Level: Operator
- Format: utilization alarm-threshold upper <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..10000</td>
<td>Add alarm threshold upper value for monitoring bandwidth utilization in hundredths of a percent.</td>
</tr>
</tbody>
</table>

19.2 clear
Clear several items.

19.2.1 clear port-statistics
Clear all statistics counter.
- Mode: Privileged Exec Mode
- Privilege Level: Operator
- Format: clear port-statistics

19.3 show
Display device options and settings.

19.3.1 show interface counters
Display the interface counters.
- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show interface counters
19.3.2  show interface statistics
Display the summary interface statistics.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show interface statistics [P-1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

19.3.3  show interface ether-stats
Display the detailed interface statistics.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show interface ether-stats [P-1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>
20 Intern

20.1 help
Display the help text for various special keys.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** help

20.2 logout
Exit this session.
- **Mode:** Command is in all modes available.
- **Privilege Level:** any
- **Format:** logout

20.3 history
Display a list of previously run commands.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** history

20.4 vlan
Enter VLAN database mode.

20.4.1 vlan database
Enter VLAN database mode.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** vlan database

20.5 vlan-mode

20.5.1 vlan-mode
Enter VLAN Configuration Mode.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** vlan-mode <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>all</td>
<td>Select all VLAN configured.</td>
</tr>
<tr>
<td></td>
<td>vlan</td>
<td>Enter single VLAN.</td>
</tr>
<tr>
<td></td>
<td>vlan range</td>
<td>Enter VLAN range separated by hyphen e.g 1-4.</td>
</tr>
<tr>
<td></td>
<td>vlan list</td>
<td>Enter VLAN list separated by comma e.g 2,4,6,...</td>
</tr>
<tr>
<td></td>
<td>complex range</td>
<td>Enter VLAN range and several VLAN separated by comma for a list and hyphen for ranges e.g 2-4,6-9,11.</td>
</tr>
</tbody>
</table>
20.6 exit
Exit from vlan mode.
- Mode: VLAN Mode
- Privilege Level: Operator
- Format: exit

20.7 end
Exit to exec mode.
- Mode: Interface Range Mode
- Privilege Level: Operator
- Format: end

20.8 serviceshell
Enter system mode.

20.8.1 serviceshell start
Start serviceshell prompt
- Mode: Privileged Exec Mode
- Privilege Level: Administrator
- Format: serviceshell start

20.8.2 serviceshell deactivate
Disable the service shell access permanently (Cannot be undone).
- Mode: Privileged Exec Mode
- Privilege Level: Administrator
- Format: serviceshell deactivate

20.9 traceroute
Trace route to a specified host.

20.10 traceroute
Trace route to a specified host.

20.10.1 traceroute source
Source address for traceroute command.
- Mode: Privileged Exec Mode
- Privilege Level: Operator
- Format: traceroute <P-1> source <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>
**20.11 reboot**
Reset the device (cold start).
- **Mode:** All Privileged Modes
- **Privilege Level:** any
- **Format:** reboot

**20.12 ping**
Send ICMP echo packets to a specified IP address.

**20.12.1 ping count**
Number of retries.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** ping <P-1> count <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..255</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

**20.13 ping**
Send ICMP echo packets to a specified host or IP address.

**20.13.1 ping source**
Source address for ping command.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** ping <P-1> source <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

**20.14 show**
Display device options and settings.

**20.14.1 show serviceshell**
Display the service shell access.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show serviceshell
21 Intrusion Detection System (IDS)

21.1 ids
Configure the Intrusion Detection System feature.

21.1.1 ids operation
Enable/disable Intrusion Detection System feature.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ids operation
- **no ids operation**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no ids operation

21.1.2 ids user
Assign/Remove an existing administrator privilege user for Intrusion Detection System feature.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ids user <P-1>
- **Parameter | Value**
  | P-1 | string |
  |     | <user> User name (up to 32 characters).
- **no ids user**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no ids user

21.2 show
Display device options and settings.

21.2.1 show ids global
Display the information and settings for the intrusion detection system.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ids global
22 Open Shortest Path First (OSPF)

22.1 ip

Set IP parameters.

22.1.1 ip ospf area

Administer the OSPF areas. An area is a sub-division of an OSPF autonomous system. You identify an area by an area-id. OSPF networks, routers, and links that have the same area-id form a logical set.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip ospf area <P-1> range add <P-2> <P-3> <P-4> modify <P-5> <P-6> <P-7> <P-8> delete <P-9> <P-10> <P-11> add delete stub add <P-12> modify <P-13> summary lsa <P-14> default-cost <P-15> delete <P-16> virtual-link add <P-17> delete <P-18> modify <P-19> authentication type <P-20> key <P-21> key-id <P-22> hello-interval <P-23> dead-interval <P-24> transmit-delay <P-25> retransmit-interval <P-26> nssa add <P-27> delete <P-28> modify translator role <P-29> stability-interval <P-30> summary no-redistribute default-info originate [metric <P-31>] [metric-type <P-32>]

- **range:** Configure the range for the area. You summarize the networks within this range into a single routing domain.
  - add: Create an area.
  - modify: Modify the parameters of an existing area.
  - delete: Delete a specific area.
  - add: Create a new area.
  - delete: Delete an existing area.
- **stub:** Configure the preferences for a stub area. You shield stub areas from external route advertisements, but the area receives advertisements from networks that belong to other areas of the same autonomous system.
  - add: Create a stub area. The command also allows you to convert an existing area to a stub area.
  - modify: Modify the stub area parameters.
- **summary lsa:** Configure the summary LSA mode for a stub area. When enabled, the router both summarizes and propagates summary LSAs.
  - default-cost: Set the default cost for the stub area.
  - delete: Remove a stub area. After removal, the area receives external route advertisements.
- **virtual-link:** Configure a virtual link. You use the virtual link to connect the router to the backbone area (0.0.0.0) through a non-backbone area or to connect two parts of a partitioned backbone area (0.0.0.0) through a non-backbone area.
  - add: Add a virtual neighbor.
  - delete: Delete a virtual neighbor.
  - modify: Modify the parameters of a virtual neighbor.
- **authentication:** Configure the authentication type. The device authenticates the OSPF protocol exchanges in the OSPF packet header which includes an authentication type field.
  - type: Configure the authentication type. Authentication types are 0 for null authentication, 1 for simple password authentication, and 2 for cryptographic authentication.
  - key: Configure the authentication key.
  - key-id: Configure the authentication key-id for md5 authentication. This field identifies the algorithm and secret key used to create the message digest appended to the OSPF packet.
- **hello-interval:** Configure the OSPF hello-interval for the virtual link, in seconds. The hello timer controls the time interval between sending two consecutive hello packets. Set this value to the same hello-interval value of the virtual neighbors.
- **dead-interval:** Configure the OSPF dead-interval for the virtual link, in seconds. If the timer expires without the router receiving hello packets from a virtual neighbor, the router declares the neighbor router as down. Set the timer to at least four times the value of the hello-interval.
- **transmit-delay:** Configure the OSPF transmit-delay for the virtual link, in seconds. Transmit delay is the time that you estimate it takes to transmit a link-state update packet over the virtual link.
- **retransmit-interval:** Configure the OSPF retransmit-interval for the virtual link, in seconds. The retransmit interval is the time between two consecutive link-state advertisement transmissions. Link-state advertisements contain such information as database descriptions and link-state request packets for adjacencies belonging to virtual link.
**Open Shortest Path First (OSPF)**

22.1 ip

nssa: Configure a NSSA(Not-So-Stubby-Area).
add: Add a NSSA.
delete: Delete a NSSA.
modify: Modify the parameters of a NSSA.
translator: Configure the NSSA translator related parameters.
role: Configure the NSSA translator role.
stability-interval: Configure the translator stability interval for the NSSA, in seconds.
summary: Configure the import summary for the specified NSSA.
no-redistribute: Configure route redistribution for the specified NSSA.
default-info: Configure the nssa default information origination parameters.
origin: Configuration whether a Type-7 LSA should be originated into the NSSA.

**Parameter** | **Value** | **Meaning**
--- | --- | ---
P-1 | A.B.C.D | IP address.
P-2 | summary-link | Configure summary links LSDB type optional mode.
nssa-external-link | Configure nssa external link LSDB type optional mode.
P-3 | A.B.C.D | IPv4 address.
P-4 | A.B.C.D | IPv4 netmask address.
P-5 | summary-link | Configure summary links LSDB type optional mode.
nssa-external-link | Configure nssa external link LSDB type optional mode.
P-6 | A.B.C.D | IPv4 address.
P-7 | A.B.C.D | IPv4 netmask address.
P-8 | advertise | Set as advertise.
do-not-advertise | Set as do-not-advertise.
P-9 | summary-link | Configure summary links LSDB type optional mode.
nssa-external-link | Configure nssa external link LSDB type optional mode.
P-10 | A.B.C.D | IPv4 address.
P-11 | A.B.C.D | IPv4 netmask address.
P-12 | 0 | Configure the TOS (0 is for Normal Service).
P-13 | 0 | Configure the TOS (0 is for Normal Service).
P-14 | no-area-summary | Disable the router from sending area link state advertisement summaries.
send-area-summary | Enable the router to send area link state advertisement summaries. The router floods LSAs within the area using multicast. Every topology change starts a new flood of LSAs.
P-15 | 0.16777215 | Configure the default cost.
P-16 | 0 | Configure the TOS (0 is for Normal Service).
P-17 | A.B.C.D | IP address.
P-18 | A.B.C.D | IP address.
P-19 | A.B.C.D | IP address.
P-20 | none | Configure the authentication type as none (Key and key ID is not required).
simple | Configure the authentication type as simple (Key ID is not required).
md5 | Configure the authentication type as md5 for the interface.
P-21 | string | <key> Configure the authentication key.
P-22 | 0.255 | Enter a number in the given range.
P-23 | 1.65535 | Enter a number between 1 and 65535
P-24 | 1.65535 | Enter a number between 1 and 65535
P-25 | 0.3600 | Enter a number in the given range.
P-26 | 0.3600 | Enter a number in the given range.
P-27 | import-nssa | Configure the area as NSSA only.
P-28 | import-external | Change the area to support external LSAs also.
P-29 | always | Configure the NSSA translator role as always. When used as a border router, the router translates LSAs regardless of the translator states of the other NSSA border routers.
candidate | Configure the NSSA translator role as a candidate. When used as a border router, the router participates in the translator election process. The router maintains a list of reachable NSSA border routers.
P-30 | 0.65535 | Enter a number between 0 and 65535
P-31 | 1.16777214 | Configure the metric value.
P-32 | ospf-metric | Set the metric type as ospf Metric.
comparable-cost | Set the metric type as comparable cost.
non-comparable | Set the metric type as non-comparable.
## no ip ospf area
Disable the option
   - **Mode:** Global Config Mode
   - **Privilege Level:** Operator
   - **Format:** no ip ospf area <P-1> range add modify delete add delete stub add modify summary/lsa default-cost delete virtual-link add delete modify authentication type key key-id hello-interval dead-interval transmit-delay retransmit-interval nssa add delete modify translator role stability-interval summary no-re distribute default-info originate [metric] [metric-type]

### 22.1.2 ip ospf trapflags all
Set all trapflags at once.
   - **Mode:** Global Config Mode
   - **Privilege Level:** Operator
   - **Format:** ip ospf trapflags all <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>[cr]</td>
<td>Enable the Bit.</td>
</tr>
</tbody>
</table>

## no ip ospf trapflags all
Disable the option
   - **Mode:** Global Config Mode
   - **Privilege Level:** Operator
   - **Format:** no ip ospf trapflags all <P-1>

### 22.1.3 ip ospf operation
Enable or disable the OSPF admin mode. When enabled, the device initiates the OSPF process if the OSPF function is active on at least one interface.
   - **Mode:** Global Config Mode
   - **Privilege Level:** Operator
   - **Format:** ip ospf operation

## no ip ospf operation
Disable the option
   - **Mode:** Global Config Mode
   - **Privilege Level:** Operator
   - **Format:** no ip ospf operation

### 22.1.4 ip ospf 1583compatibility
Enable or disable the 1583compatibility for calculating routes external to the autonomous system. When enabled, the router is compatible with the preference rules defined in RFC1583, section 16.4.
   - **Mode:** Global Config Mode
   - **Privilege Level:** Operator
   - **Format:** ip ospf 1583compatibility

## no ip ospf 1583compatibility
Disable the option
   - **Mode:** Global Config Mode
   - **Privilege Level:** Operator
   - **Format:** no ip ospf 1583compatibility

### 22.1.5 ip ospf default-metric
Configure the default metric for re-distributed routes, when OSPF redistributes routes from other protocols.
   - **Mode:** Global Config Mode
   - **Privilege Level:** Operator
   - **Format:** ip ospf default-metric <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..16777214</td>
<td>Configure the default metric for redistributed routes.</td>
</tr>
</tbody>
</table>
22.1.6 ip ospf router-id
Configure the router ID to uniquely identify this OSPF router in the autonomous system. If a tie occurs during the designated router election, the router with the higher router ID is the designated router.

Parameter | Value | Meaning
--- | --- | ---
P-1 | A.B.C.D | IP address.

22.1.7 ip ospf external-lsdb-limit
Configure the OSPF external lsdb limitation, which is the maximum number of non-default AS-external-LSA entries that the router stores in the link-state database. When the value -1 is configured, you disable the limitation.

Parameter | Value | Meaning
--- | --- | ---
P-1 | -1..2147483647 | Configure the external lsdb limit.

22.1.8 ip ospf exit-overflow
Configure the OSPF exit overflow interval, in seconds. After the timer expires the router will attempt to leave the overflow-state. To disable the exit overflow interval function set the value to 0.

Parameter | Value | Meaning
--- | --- | ---
P-1 | 0..2147483647- | Configure the exit overflow interval.

22.1.9 ip ospf maximum-path
Configure the maximum number of paths that OSPF reports.

Parameter | Value | Meaning
--- | --- | ---
P-1 | 1..4 | Set the maximum path.

22.1.10 ip ospf spf-delay
Configure the SPF delay, in seconds. The Shortest Path First (SPF) delay is the time that the device waits for the network to stabilize before calculating the shortest path tree, after a topology change.

Parameter | Value | Meaning
--- | --- | ---
P-1 | 0..65535 | Enter a number between 0 and 65535

22.1.11 ip ospf spf-holdtime
Configure the minimum time between two consecutive SPF calculations, in seconds.

Parameter | Value | Meaning
--- | --- | ---
P-1 | 0..65535 | Enter a number between 0 and 65535
22.1.12 ip ospf auto-cost
Set the auto cost reference bandwidth of the router interfaces for ospf metric calculations. The default reference bandwidth is 100 Mbps.

- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip ospf auto-cost <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1.4294967</td>
<td>Configure the auto cost for OSPF calculation.</td>
</tr>
</tbody>
</table>

22.1.13 ip ospf distance intra
Enter the preference type as intra. Use intra-area routing when the device routes packets solely within an area, such as an internal router.

- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip ospf distance intra <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter the value.</td>
</tr>
</tbody>
</table>

22.1.14 ip ospf distance inter
Enter the preference type as inter. Use inter-area routing when the device routes packets into or out of an area, such as an area border router.

- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip ospf distance inter <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter the value.</td>
</tr>
</tbody>
</table>

22.1.15 ip ospf distance external
Enter the preference type as external. Use external-area routing when the device routes packets into or out of an autonomous system, such as an autonomous system boundary router (ASBR).

- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip ospf distance external <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter the value.</td>
</tr>
</tbody>
</table>

22.1.16 ip ospf re-distribute
Configure the OSPF route re-distribution. An ASBR is able to translate information from other OSPF processes in separate areas and routes from other sources, such as static routes or other dynamic routing protocols, into the OSPF protocol.

- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip ospf re-distribute <P-1> [metric <P-2>] [metric-type <P-3>] [tag <P-4>] [subnets <P-5>]
  [metric]: Configure the OSPF route re-distribution metric parameters.
  [metric-type]: Configure the OSPF route redistribution metric-type.
  [tag]: Configure the OSPF route redistribution tag parameters.
  [subnets]: Allow the router to redistribute subnets into OSPF.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>connected</td>
<td>Select the source protocol as connected.</td>
</tr>
<tr>
<td></td>
<td>static</td>
<td>Select the source protocol as static.</td>
</tr>
<tr>
<td>P-2</td>
<td>0..16777214</td>
<td>Configure the metric.</td>
</tr>
<tr>
<td>P-3</td>
<td>1..2</td>
<td>Configure the metric type.</td>
</tr>
<tr>
<td>P-4</td>
<td>0..4294967295</td>
<td>Configure the tag.</td>
</tr>
<tr>
<td>P-5</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>
22.2 ip

### no ip ospf re-distribute

Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `no ip ospf re-distribute <P-1> [metric] [metric-type] [tag] [subnets]`

#### 22.1.17 ip ospf distribute-list

Configure the distribute list for the routes from other source protocols.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `ip ospf distribute-list <P-1> <P-2> <P-3>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>out</td>
<td>Configure as out to re-distribute routes with ACL rules.</td>
</tr>
<tr>
<td>P-2</td>
<td>connected</td>
<td>Select the source protocol as connected.</td>
</tr>
<tr>
<td>P-3</td>
<td>static</td>
<td>Select the source protocol as static.</td>
</tr>
<tr>
<td></td>
<td>&lt;1000..1099&gt;</td>
<td>Enter the access list number.</td>
</tr>
</tbody>
</table>

### no ip ospf distribute-list

Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `no ip ospf distribute-list <P-1> <P-2> <P-3>`

#### 22.1.18 ip ospf default-info originate

Originate the OSPF default information.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `ip ospf default-info originate [always] [metric <P-1>] [metric-type <P-2>]
[always]: Always advertise the 0.0.0.0/0.0.0.0 route information.
[metric]: Configure the metric for default information.
[metric-type]: Configure the metric type for default information.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..16777214</td>
<td>Configure the metric value.</td>
</tr>
<tr>
<td>P-2</td>
<td>external-type1</td>
<td>Set the metric type for default information as external type-1. The type 1 value sets the metric to the sum of the internal and external OSPF metrics.</td>
</tr>
<tr>
<td>P-3</td>
<td>external-type2</td>
<td>Set the metric type for default information as external type-2. The type 2 value sets the metric to the sum of external OSPF metrics from the source AS to the destination AS.</td>
</tr>
</tbody>
</table>

### no ip ospf default-info originate

Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `no ip ospf default-info originate [always] [metric <P-1>] [metric-type]`

#### 22.2 ip

IP interface commands.

#### 22.2.1 ip ospf operation

Enable or disable OSPF on port.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip ospf operation`

### no ip ospf operation

Disable the option

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `no ip ospf operation`
22.2.2 ip ospf area-id
Configure the area ID that uniquely identifies the area to which the interface is connected.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip ospf area-id <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

22.2.3 ip ospf link-type
Configure the OSPF link type.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip ospf link-type <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>broadcast</td>
<td>Configure the link-type as broadcast for the interface. In broadcast networks, routers discover their neighbors dynamically using the OSPF hello protocol.</td>
</tr>
<tr>
<td></td>
<td>nbma</td>
<td>Configure the link-type as Non-Broadcast Multi-Access for the interface. The nbma mode, emulates OSPF operation over a broadcast network. The nbma mode is the most efficient way to run OSPF over non-broadcast networks, both in terms of the LSDB size and the amount of routing protocol traffic. However, this mode requires direct communication between every router in the nbma network.</td>
</tr>
<tr>
<td></td>
<td>point-to-point</td>
<td>Configure the link-type as point-to-point for the interface. Use the point-to-point link-type in a network that joins a single pair of routers.</td>
</tr>
<tr>
<td></td>
<td>point-to-multipoint</td>
<td>Configure the link-type as point-to-multipoint for the interface. In the point-to-multipoint mode, OSPF treats each router-to-router link over non-broadcast networks as if they were point-to-point links.</td>
</tr>
</tbody>
</table>

22.2.4 ip ospf priority
Configure the OSPF router priority which the router uses in multi-access networks for the designated router election algorithm. The router with the higher router priority is the designated router. A value of 0 declares the router as ineligible for designated router elections.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip ospf priority <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..255</td>
<td>Configure the priority.</td>
</tr>
</tbody>
</table>

22.2.5 ip ospf transmit-delay
Configure the OSPF transmit-delay for the interface, in seconds. The transmit-delay is the time that you estimate it takes to transmit a link-state update packet over the interface.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip ospf transmit-delay <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..3600</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

22.2.6 ip ospf retransmit-interval
Configure the OSPF retransmit-interval for the interface, in seconds. The retransmit-interval is the interval after which link-state advertisements containing database description and link-state request packets, are re-transmitted for adjacencies belonging to this interface.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip ospf retransmit-interval <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..3600</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

22.2.7 ip ospf hello-interval
Configure the OSPF hello-interval for the interface, in seconds. The hello timer controls the time interval between two consecutive hello packets. Set this value to the same hello-interval value of the neighbor.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip ospf hello-interval <P-1>
22.2.8 ip ospf dead-interval

Configure the OSPF dead-interval for the interface, in seconds. If the timer expires without the router receiving hello packets from the neighbor, the router declares the neighbor router as down. Set the timer to at least four times the value of the hello-interval.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip ospf dead-interval <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..65535</td>
<td>Enter a number between 1 and 65535</td>
</tr>
</tbody>
</table>

22.2.9 ip ospf cost

Configure the OSPF cost for the interface. The cost of a specific interface indicates the overhead required to send packets across the link. If set to 0, OSPF calculates the cost from the reference bandwidth and the interface speed.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip ospf cost <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..65535</td>
<td>Configure the cost for the specified interface.</td>
</tr>
<tr>
<td></td>
<td>auto</td>
<td>Automatic calculation from reference bandwidth and link speed.</td>
</tr>
</tbody>
</table>

22.2.10 ip ospf mtu-ignore

Enable/Disable OSPF MTU mismatch on interface.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip ospf mtu-ignore`

- **no ip ospf mtu-ignore**
  - Disable the option
    - **Mode:** Interface Range Mode
    - **Privilege Level:** Operator
    - **Format:** `no ip ospf mtu-ignore`

22.2.11 ip ospf authentication type

Configure authentication type.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip ospf authentication type <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>none</td>
<td>Configure the authentication type as none (Key and key ID is not required).</td>
</tr>
<tr>
<td></td>
<td>simple</td>
<td>Configure the authentication type as simple (Key ID is not required).</td>
</tr>
<tr>
<td></td>
<td>md5</td>
<td>Configure the authentication type as md5 for the interface.</td>
</tr>
</tbody>
</table>

22.2.12 ip ospf authentication key

Configure authentication key.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip ospf authentication key <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>&lt;key&gt;</td>
<td>Configure the authentication key.</td>
</tr>
</tbody>
</table>

22.2.13 ip ospf authentication key-id

Configure authentication key-id for md5 authentication.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip ospf authentication key-id <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..255</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>
22.3 show

Display device options and settings.

22.3.1 show ip ospf global

Display the OSPF global configurations.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip ospf global

22.3.2 show ip ospf area

Display the OSPF area related information.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip ospf area [P-1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

22.3.3 show ip ospf stub

Display the OSPF stub area related information.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip ospf stub

22.3.4 show ip ospf database internal

Display the internal LSA database information.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip ospf database internal

22.3.5 show ip ospf database external

Display the external LSA database information.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip ospf database external

22.3.6 show ip ospf range

Display the OSPF area range information.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip ospf range

22.3.7 show ip ospf interface

Display the OSPF interface related information.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip ospf interface [P-1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

22.3.8 show ip ospf virtual-link

Display the OSPF virtual-link related information.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip ospf virtual-link <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>
22.3.9 show ip ospf virtual-neighbor
Display the OSPF Virtual-link neighbor information.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip ospf virtual-neighbor

22.3.10 show ip ospf neighbor
Display the OSPF neighbor related information.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip ospf neighbor [P-1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

22.3.11 show ip ospf statistics
Display the OSPF statistics.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip ospf statistics

22.3.12 show ip ospf re-distribute
Display the OSPF re-distribute related information.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip ospf re-distribute P-1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>connected</td>
<td>Select the source protocol as connected.</td>
</tr>
<tr>
<td></td>
<td>static</td>
<td>Select the source protocol as static.</td>
</tr>
</tbody>
</table>

22.3.13 show ip ospf nssa
Display the OSPF NSSA related information.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip ospf nssa P-1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

22.3.14 show ip ospf route
Display the OSPF routes.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip ospf route
23  Virtual Router Redundancy Protocol (VRRP)

23.1  ip
Set IP parameters.

23.1.1  ip vrrp operation
Enables or disables VRRP globally on the device.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip vrrp operation

■ no ip vrrp operation
Disable the option
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: no ip vrrp operation

23.1.2  ip vrrp trap auth-failure
Enable or disable the sending of a trap if this router detects an authentication failure on any of its VRRP interfaces.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip vrrp trap auth-failure

■ no ip vrrp trap auth-failure
Disable the option
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: no ip vrrp trap auth-failure

23.1.3  ip vrrp trap new-master
Enable or disable the sending of a trap if this router becomes new master for any of its VRRP interfaces.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip vrrp trap new-master

■ no ip vrrp trap new-master
Disable the option
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: no ip vrrp trap new-master

23.2  ip
IP interface commands.

23.2.1  ip vrrp add
Create a new VRRP instance.
- Mode: Interface Range Mode
- Privilege Level: Operator
- Format: ip vrrp add <P-1> [priority <P-2>] [interval <P-3>]
  [priority]: Priority of the virtual router ..... default 100
  [interval]: Advertisement Interval in seconds .. default 1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1-255</td>
<td>Enter a virtual router ID.</td>
</tr>
</tbody>
</table>
Virtual Router Redundancy Protocol (VRRP)

23.2 ip

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-2</td>
<td>1..254</td>
<td>Enter a priority value.</td>
</tr>
<tr>
<td>P-3</td>
<td>1..255</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

### 23.2.2 ip vrrp modify
Modify parameters of a VRRP instance.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** ip vrrp modify <P-1> [priority <P-2>] [interval <P-3>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter a virtual router ID.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..254</td>
<td>Enter a priority value.</td>
</tr>
<tr>
<td>P-3</td>
<td>1..255</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

### 23.2.3 ip vrrp delete
Delete a VRRP instance.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** ip vrrp delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter a virtual router ID.</td>
</tr>
</tbody>
</table>

### 23.2.4 ip vrrp enable
Enable a VRRP instance.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** ip vrrp enable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter a virtual router ID.</td>
</tr>
</tbody>
</table>

### 23.2.5 ip vrrp disable
Disable a VRRP instance.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** ip vrrp disable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter a virtual router ID.</td>
</tr>
</tbody>
</table>

### 23.2.6 ip vrrp virtual-address add
Add a virtual address.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** ip vrrp virtual-address add <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter a virtual router ID.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

### 23.2.7 ip vrrp virtual-address delete
Delete a virtual address.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** ip vrrp virtual-address delete <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter a virtual router ID.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>
23.2.8 ip vrrp track add
Add a tracking object to the vrrp instance.
  ▶ Mode: Interface Range Mode
  ▶ Privilege Level: Operator
  ▶ Format: ip vrrp track add <P-1> <P-2> [decrement <P-3>]
    [decrement]: Configure the decrement value. Default is 20

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter a virtual router ID.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Track instance.</td>
</tr>
<tr>
<td>P-3</td>
<td>1..253</td>
<td>Enter the decrement value. The priority will be decremented by the configured value</td>
</tr>
</tbody>
</table>

23.2.9 ip vrrp track modify
Modify a tracking object to the vrrp instance.
  ▶ Mode: Interface Range Mode
  ▶ Privilege Level: Operator
  ▶ Format: ip vrrp track modify <P-1> <P-2> decrement <P-3>
    decrement: Configure the decrement value. Default is 20

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter a virtual router ID.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Track instance.</td>
</tr>
<tr>
<td>P-3</td>
<td>1..253</td>
<td>Enter the decrement value. The priority will be decremented by the configured value</td>
</tr>
</tbody>
</table>

23.2.10 ip vrrp track delete
Delete a tracking object to the vrrp instance.
  ▶ Mode: Interface Range Mode
  ▶ Privilege Level: Operator
  ▶ Format: ip vrrp track delete <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter a virtual router ID.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Track instance.</td>
</tr>
</tbody>
</table>

23.3 show
Display device options and settings.

23.3.1 show ip vrrp interface
Display the parameters of one VRRP instances.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show ip vrrp interface [<P-1> [<P-2>]]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>1..255</td>
<td>Enter a virtual router ID.</td>
</tr>
</tbody>
</table>

23.3.2 show ip vrrp global
Display the global VRRP parameters.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show ip vrrp global
24 Address Resolution Protocol (IP ARP)

24.1 ip

Set IP parameters.

24.1.1 ip arp add

Add a static arp entry.

- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: ip arp add <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

24.1.2 ip arp delete

Delete a static arp entry.

- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: ip arp delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

24.1.3 ip arp enable

Enable a static arp entry.

- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: ip arp enable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>a.b.c.d</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

24.1.4 ip arp disable

Disable a static arp entry.

- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: ip arp disable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>a.b.c.d</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

24.1.5 ip arp timeout

Configure ARP entry age-out time (in seconds).

- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: ip arp timeout <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>15..21600</td>
<td>Enter the arp response time.</td>
</tr>
</tbody>
</table>

24.1.6 ip arp response-time

Configure ARP request response timeout (in seconds).

- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: ip arp response-time <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..10</td>
<td>Enter the arp response time.</td>
</tr>
</tbody>
</table>
24.1.7  **ip arp retries**  
Configure ARP count of maximum requests for retries.  

- **Mode:** Global Config Mode  
- **Privilege Level:** Operator  
- **Format:** ip arp retries <P-1>  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..10</td>
<td>Enter the arp max retries.</td>
</tr>
</tbody>
</table>

24.2  **show**  
Display device options and settings.  

24.2.1  **show ip arp info**  
Display the ARP summary information.  

- **Mode:** Command is in all modes available.  
- **Privilege Level:** Guest  
- **Format:** show ip arp info  

24.2.2  **show ip arp table**  
Display the ARP cache entries.  

- **Mode:** Command is in all modes available.  
- **Privilege Level:** Guest  
- **Format:** show ip arp table  

24.2.3  **show ip arp static**  
Display the static ARP entries.  

- **Mode:** Command is in all modes available.  
- **Privilege Level:** Guest  
- **Format:** show ip arp static  

24.2.4  **show ip arp entry**  
Display the ARP cache entry.  

- **Mode:** Command is in all modes available.  
- **Privilege Level:** Guest  
- **Format:** show ip arp entry <P-1>  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

24.3  **clear**  
Clear several items.  

24.3.1  **clear ip arp-cache**  
Clear the router's ARP table (cache).  

- **Mode:** Privileged Exec Mode  
- **Privilege Level:** Operator  
- **Format:** clear ip arp-cache [gateway]  
[gateway]: Also clear gateway ARP entries.
25 Internet Protocol Version 4 (IPv4)

25.1 network
Configure the inband and outband connectivity.

25.1.1 network parms
Set network address, netmask and gateway

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** network parms <P-1> <P-2> [P-3>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IPv4 address.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IPv4 netmask address.</td>
</tr>
<tr>
<td>P-3</td>
<td>A.B.C.D</td>
<td>IPv4 gateway address.</td>
</tr>
</tbody>
</table>

25.2 clear
Clear several items.

25.2.1 clear arp-table-switch
Clear the agent's ARP table (cache).

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** clear arp-table-switch

25.3 show
Display device options and settings.

25.3.1 show network parms
Display the network settings.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show network parms

25.4 show
Display device options and settings.

25.4.1 show arp
Display the ARP table.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show arp
26 Link Layer Discovery Protocol (LLDP)

26.1 lldp

Configure of Link Layer Discovery Protocol.

26.1.1 lldp operation

Enable or disable the LLDP operational state.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** lldp operation

- **no lldp operation**

  Disable the option

  - **Mode:** Global Config Mode
  - **Privilege Level:** Operator
  - **Format:** no lldp operation

26.1.2 lldp config chassis admin-state

Enable or disable the LLDP operational state.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** lldp config chassis admin-state <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

26.1.3 lldp config chassis notification-interval

Enter the LLDP notification interval in seconds.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** lldp config chassis notification-interval <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5..3600</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

26.1.4 lldp config chassis re-init-delay

Enter the LLDP re-initialization delay in seconds.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** lldp config chassis re-init-delay <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1..10</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

26.1.5 lldp config chassis tx-delay

Enter the LLDP transmit delay in seconds (tx-delay smaller than \((0.25 \times \text{tx-interval})\))

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** lldp config chassis tx-delay <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1.8192</td>
<td>Enter a number in the given range (tx-delay smaller than ((0.25 \times \text{tx-interval})))</td>
</tr>
</tbody>
</table>

26.1.6 lldp config chassis tx-hold-multiplier

Enter the LLDP transmit hold multiplier.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** lldp config chassis tx-hold-multiplier <P-1>
26.2 show

Display device options and settings.

26.2.1 show lldp global

Display the LLDP global configurations.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>2..10</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

26.2.2 show lldp port

Display the port specific LLDP configurations.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

26.2.3 show lldp remote-data

Remote information collected with LLDP.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

26.3 lldp

Configure of Link Layer Discovery Protocol on a port.

26.3.1 lldp admin-state

Configure how the interface processes LLDP frames.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>tx-only</td>
<td>Interface will only transmit LLDP frames. Received frames are not processed.</td>
</tr>
<tr>
<td></td>
<td>rx-only</td>
<td>Interface will only receive LLDP frames. Frames are not transmitted.</td>
</tr>
<tr>
<td></td>
<td>tx-and-rx</td>
<td>Interface will transmit and receive LLDP frames. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Interface will neither transmit nor process received LLDP frames.</td>
</tr>
</tbody>
</table>
26.3.2 lldp fdb-mode
Configure the LLDP FDB mode for this interface.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `lldp fdb-mode <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>lldp-only</td>
<td>Collected remote data will be based on received LLDP frames only.</td>
</tr>
<tr>
<td></td>
<td>mac-only</td>
<td>Collected remote data will be based on the switch's FDB entries only.</td>
</tr>
<tr>
<td></td>
<td>both</td>
<td>Collected remote data will be based on received LLDP frames as well as on the switch's FDB entries.</td>
</tr>
<tr>
<td></td>
<td>auto-detect</td>
<td>As long as no LLDP frames are received, the collected remote data will be based on the switch's FDB entries only. After the first LLDP frame is received, the remote data will be based on received LLDP frames only. This is the default setting.</td>
</tr>
</tbody>
</table>

26.3.3 lldp max-neighbors
Enter the LLDP max neighbors for interface.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `lldp max-neighbors <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..50</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

26.3.4 lldp notification
Enable or disable the LLDP notification operation for interface.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `lldp notification`

- **no lldp notification**
  Disable the option
  - **Mode:** Interface Range Mode
  - **Privilege Level:** Operator
  - **Format:** `no lldp notification`

26.3.5 lldp tlv mac-phy-config-state
Enable or disable mac-phy-config-state TLV transmission.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `lldp tlv mac-phy-config-state <P-1>`

- **no lldp tlv mac-phy-config-state**
  Disable the option
  - **Mode:** Interface Range Mode
  - **Privilege Level:** Operator
  - **Format:** `no lldp tlv mac-phy-config-state <P-1>`

26.3.6 lldp tlv max-frame-size
Enable or disable max-frame-size TLV transmission.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `lldp tlv max-frame-size <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>[cr]</td>
<td>Enable the Bit.</td>
</tr>
</tbody>
</table>
26.3 lldp

- `no lldp tlv max-frame-size`
  - Disable the option
  - **Mode:** Interface Range Mode
  - **Privilege Level:** Operator
  - **Format:** `no lldp tlv max-frame-size <P-1>`

26.3.7 lldp tlv mgmt-addr

Enable or disable mgmt-addr TLV transmission.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `lldp tlv mgmt-addr`

- `no lldp tlv mgmt-addr`
  - Disable the option
  - **Mode:** Interface Range Mode
  - **Privilege Level:** Operator
  - **Format:** `no lldp tlv mgmt-addr`

26.3.8 lldp tlv port-desc

Enable or disable port description TLV transmission.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `lldp tlv port-desc <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>[cr]</td>
<td>Enable the Bit</td>
</tr>
</tbody>
</table>

- `no lldp tlv port-desc`
  - Disable the option
  - **Mode:** Interface Range Mode
  - **Privilege Level:** Operator
  - **Format:** `no lldp tlv port-desc <P-1>`

26.3.9 lldp tlv port-vlan

Enable or disable port-vlan TLV transmission.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `lldp tlv port-vlan`

- `no lldp tlv port-vlan`
  - Disable the option
  - **Mode:** Interface Range Mode
  - **Privilege Level:** Operator
  - **Format:** `no lldp tlv port-vlan`

26.3.10 lldp tlv protocol

Enable or disable protocol TLV transmission.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `lldp tlv protocol`

- `no lldp tlv protocol`
  - Disable the option
  - **Mode:** Interface Range Mode
  - **Privilege Level:** Operator
  - **Format:** `no lldp tlv protocol`
26.3.11 **lldp tlv sys-cap**
Enable or disable system capabilities TLV transmission.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `lldp tlv sys-cap <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>[cr]</td>
<td>Enable the Bit.</td>
</tr>
</tbody>
</table>

- **no lldp tlv sys-cap**
  Disable the option
  - **Mode:** Interface Range Mode
  - **Privilege Level:** Operator
  - **Format:** `no lldp tlv sys-cap <P-1>`

26.3.12 **lldp tlv sys-desc**
Enable or disable system description TLV transmission.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `lldp tlv sys-desc <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>[cr]</td>
<td>Enable the Bit.</td>
</tr>
</tbody>
</table>

- **no lldp tlv sys-desc**
  Disable the option
  - **Mode:** Interface Range Mode
  - **Privilege Level:** Operator
  - **Format:** `no lldp tlv sys-desc <P-1>`

26.3.13 **lldp tlv sys-name**
Enable or disable system name TLV transmission.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `lldp tlv sys-name <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>[cr]</td>
<td>Enable the Bit.</td>
</tr>
</tbody>
</table>

- **no lldp tlv sys-name**
  Disable the option
  - **Mode:** Interface Range Mode
  - **Privilege Level:** Operator
  - **Format:** `no lldp tlv sys-name <P-1>`

26.3.14 **lldp tlv vlan-name**
Enable or disable vlan name TLV transmission.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `lldp tlv vlan-name`

- **no lldp tlv vlan-name**
  Disable the option
  - **Mode:** Interface Range Mode
  - **Privilege Level:** Operator
  - **Format:** `no lldp tlv vlan-name`

26.3.15 **lldp tlv protocol-based-vlan**
Enable or disable protocol-based vlan TLV transmission.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `lldp tlv protocol-based-vlan`
no lldp tlv protocol-based-vlan

Disable the option

- **Mode**: Interface Range Mode
- **Privilege Level**: Operator
- **Format**: no lldp tlv protocol-based-vlan
27 Logging

27.1 logging

Logging configuration.

27.1.1 logging audit-trail

Add a comment for the audit trail.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `logging audit-trail <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 80 characters.</td>
</tr>
</tbody>
</table>

27.1.2 logging buffered severity

Configure the minimum severity level to be logged to the high priority buffer.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `logging buffered severity <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>emergency</td>
<td>System is unusable. System failure has occurred.</td>
</tr>
<tr>
<td></td>
<td>alert</td>
<td>Action must be taken immediately. Unrecoverable failure of a component. System failure likely.</td>
</tr>
<tr>
<td></td>
<td>critical</td>
<td>Recoverable failure of a component that may lead to system failure.</td>
</tr>
<tr>
<td></td>
<td>error</td>
<td>Error conditions. Recoverable failure of a component.</td>
</tr>
<tr>
<td></td>
<td>warning</td>
<td>Minor failure, e.g. misconfiguration of a component.</td>
</tr>
<tr>
<td></td>
<td>notice</td>
<td>Normal but significant conditions.</td>
</tr>
<tr>
<td></td>
<td>informational</td>
<td>Informational messages.</td>
</tr>
<tr>
<td></td>
<td>debug</td>
<td>Debug-level messages.</td>
</tr>
<tr>
<td>0</td>
<td></td>
<td>Same as emergency</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>Same as alert</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Same as critical</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>Same as error</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Same as warning</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>Same as notice</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>Same as informational</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>Same as debug</td>
</tr>
</tbody>
</table>

27.1.3 logging host add

Add a new logging host.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `logging host add <P-1> addr <P-2> [transport <P-3>] [port <P-4>] [severity <P-5>] [type <P-6>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1.8</td>
<td>Syslog server entry index</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-3</td>
<td>udp</td>
<td>The UDP-based transmission.</td>
</tr>
<tr>
<td></td>
<td>tls</td>
<td>The TLS-based transmission.</td>
</tr>
<tr>
<td>P-4</td>
<td>1.65535</td>
<td>Port number to be used</td>
</tr>
</tbody>
</table>
27.1 logging

27.1.4 logging host delete
Delete a logging host.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `logging host delete <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..8</td>
<td>Syslog server entry index</td>
</tr>
</tbody>
</table>

27.1.5 logging host enable
Enable a logging host.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `logging host enable <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..8</td>
<td>Syslog server entry index</td>
</tr>
</tbody>
</table>

27.1.6 logging host disable
Disable a logging host.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `logging host disable <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..8</td>
<td>Syslog server entry index</td>
</tr>
</tbody>
</table>

27.1.7 logging host modify
Modify an existing logging host.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `logging host modify <P-1> [addr <P-2>] [transport <P-3>] [port <P-4>] [severity <P-5>] [type <P-6>]`
  - `[addr]`: Enter the IP address of the server.
  - `[transport]`: Configure the type of transport used for syslog server transmission.
  - `[port]`: Enter the port used for syslog server transmission.
  - `[severity]`: Configure the minimum severity level to be sent to this syslog server.
  - `[type]`: Configure the type of log messages to be sent to the syslog server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..8</td>
<td>Syslog server entry index</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address</td>
</tr>
<tr>
<td>P-3</td>
<td>udp</td>
<td>The UDP-based transmission.</td>
</tr>
<tr>
<td></td>
<td>tls</td>
<td>The TLS-based transmission.</td>
</tr>
<tr>
<td>P-4</td>
<td>1..65535</td>
<td>Port number to be used</td>
</tr>
</tbody>
</table>
27.1.8 logging syslog operation

Enable or disable the syslog client.

- **Mode**: Global Config Mode
- **Privilege Level**: Administrator
- **Format**: `logging syslog operation`

- **no logging syslog operation**
  - Disable the option
    - **Mode**: Global Config Mode
    - **Privilege Level**: Administrator
    - **Format**: `no logging syslog operation`

27.1.9 logging current-console operation

Enable or disable logging messages to the current remote console.

- **Mode**: Global Config Mode
- **Privilege Level**: Administrator
- **Format**: `logging current-console operation`

- **no logging current-console operation**
  - Disable the option
    - **Mode**: Global Config Mode
    - **Privilege Level**: Administrator
    - **Format**: `no logging current-console operation`

27.1.10 logging current-console severity

Configure the minimum severity level to be sent to the current remote console.

- **Mode**: Global Config Mode
- **Privilege Level**: Administrator
- **Format**: `logging current-console severity <P-1>`
27.1 logging

27.1.11 logging console operation

Enable or disable logging to the local V.24 console.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** logging console operation

- **no logging console operation**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no logging console operation

27.1.12 logging console severity

Configure the minimum severity level to be logged to the V.24 console.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** logging console severity <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>emergency</td>
<td>System is unusable. System failure has occurred.</td>
</tr>
<tr>
<td></td>
<td>alert</td>
<td>Action must be taken immediately. Unrecoverable failure of a component. System failure likely.</td>
</tr>
<tr>
<td></td>
<td>critical</td>
<td>Recoverable failure of a component that may lead to system failure.</td>
</tr>
<tr>
<td></td>
<td>error</td>
<td>Error conditions. Recoverable failure of a component.</td>
</tr>
<tr>
<td></td>
<td>warning</td>
<td>Minor failure, e.g. misconfiguration of a component.</td>
</tr>
<tr>
<td></td>
<td>notice</td>
<td>Normal but significant conditions.</td>
</tr>
<tr>
<td></td>
<td>informational</td>
<td>Informational messages.</td>
</tr>
<tr>
<td></td>
<td>debug</td>
<td>Debug-level messages.</td>
</tr>
<tr>
<td>0</td>
<td>Same as emergency</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Same as alert</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Same as critical</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Same as error</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Same as warning</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Same as notice</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Same as informational</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Same as debug</td>
<td></td>
</tr>
</tbody>
</table>

27.1.13 logging persistent operation

Enable or disable persistent logging. This feature is only available when an ENVM is connected to the device. The logging information is saved on the selected ENVM.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** logging persistent operation
no logging persistent operation
Disable the option
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Administrator
  ▶ Format: no logging persistent operation

27.1.14 logging persistent numfiles
Enter the maximum number of log files.
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Administrator
  ▶ Format: logging persistent numfiles <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..25</td>
<td>number of logfiles</td>
</tr>
</tbody>
</table>

27.1.15 logging persistent filesize
Enter the maximum size of a log file.
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Administrator
  ▶ Format: logging persistent filesize <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..4096</td>
<td>Maximum persistent logfile size on the non-volatile memory in kBytes</td>
</tr>
</tbody>
</table>

27.1.16 logging persistent severity-level
Configure the minimum severity level to be logged into files.
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Administrator
  ▶ Format: logging persistent severity-level <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>emergency</td>
<td></td>
<td>System is unusable. System failure has occurred.</td>
</tr>
<tr>
<td>alert</td>
<td></td>
<td>Action must be taken immediately. Unrecoverable failure of a component. System failure likely.</td>
</tr>
<tr>
<td>critical</td>
<td></td>
<td>Recoverable failure of a component that may lead to system failure.</td>
</tr>
<tr>
<td>error</td>
<td></td>
<td>Error conditions. Recoverable failure of a component.</td>
</tr>
<tr>
<td>warning</td>
<td></td>
<td>Minor failure, e.g. misconfiguration of a component.</td>
</tr>
<tr>
<td>notice</td>
<td></td>
<td>Normal but significant conditions.</td>
</tr>
<tr>
<td>informational</td>
<td></td>
<td>Informational messages.</td>
</tr>
<tr>
<td>debug</td>
<td></td>
<td>Debug-level messages.</td>
</tr>
<tr>
<td>0</td>
<td></td>
<td>Same as emergency</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>Same as alert</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Same as critical</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>Same as error</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Same as warning</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>Same as notice</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>Same as informational</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>Same as debug</td>
</tr>
</tbody>
</table>

27.2 show
Display device options and settings.

27.2.1 show logging buffered
Display the buffered (in-memory) log entries.
  ▶ Mode: Command is in all modes available.
  ▶ Privilege Level: Guest
  ▶ Format: show logging buffered [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td></td>
<td>&lt;filter&gt; Enter a comma separated list of severity ranges, numbers or enum strings are allowed. Example: 0-1,informational-debug</td>
</tr>
</tbody>
</table>
Logging
27.3 copy

27.2.2 show logging traplogs
Display the trap log entries.
- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show logging traplogs

27.2.3 show logging console
Display the console logging configurations.
- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show logging console

27.2.4 show logging persistent
Display the persistent logging configurations.
- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show logging persistent [logfiles]
-logfiles: List the persistent log files.

27.2.5 show logging syslog
Display the current syslog operational setting.
- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show logging syslog

27.2.6 show logging host
Display a list of logging hosts currently configured.
- Mode: Command is in all modes available.
- Privilege Level: Guest
- Format: show logging host

27.3 copy
Copy different kinds of items.

27.3.1 copy eventlog buffered envm
Copy a buffered log from the device to external non-volatile memory.
- Mode: Privileged Exec Mode
- Privilege Level: Operator
- Format: copy eventlog buffered envm <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
</tbody>
</table>

27.3.2 copy eventlog buffered remote
Copy a buffered log from the device to a file server.
- Mode: Privileged Exec Mode
- Privilege Level: Operator
- Format: copy eventlog buffered remote <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>

27.3.3 copy eventlog persistent
Copy the persistent logs from the device to an envm or a file server.
- Mode: Privileged Exec Mode
- Privilege Level: Operator
- Format: copy eventlog persistent <P-1> envm <P-2> remote <P-3>
-envm: Copy the persistent log from the device to external non-volatile memory.
remote: Copy the persistent logs from the device to a file server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
<tr>
<td>P-3</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>

### 27.3.4 copy traplog system envm
Copy the traplog from the device to external non-volatile memory.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** `copy traplog system envm <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
</tbody>
</table>

### 27.3.5 copy traplog system remote
Copy the traplog from the device to a file server.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** `copy traplog system remote <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>

### 27.3.6 copy audittrail system envm
Copy the audit trail from the device to external non-volatile memory.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator, Auditor
- **Format:** `copy audittrail system envm <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
</tbody>
</table>

### 27.3.7 copy audittrail system remote
Copy the audit trail from the device to a file server.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator, Auditor
- **Format:** `copy audittrail system remote <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>

### 27.4 clear
Clear several items.

#### 27.4.1 clear logging buffered
Clear buffered log from memory.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `clear logging buffered`

#### 27.4.2 clear logging persistent
Clear persistent log from memory.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `clear logging persistent`
27.4.3 clear eventlog
Clear the event log entries from memory.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** clear eventlog
28 Management Access

28.1 network

Configure the inband and outband connectivity.

28.1.1 network management access web timeout

Set the web interface idle timeout.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `network management access web timeout <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..160</td>
<td>Idle timeout of a session in minutes (default: 5).</td>
</tr>
</tbody>
</table>

28.1.2 network management access add

Add a new entry with index.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `network management access add <P-1> [ip <P-2>] [mask <P-3>] [http <P-4>] [https <P-5>] [snmp <P-6>]`

- **[ip]**: Configure IP address which should have access to management.
- **[mask]**: Configure network mask to allow a subnet for management access.
- **[http]**: Configure if HTTP is allowed to have management access.
- **[https]**: Configure if HTTPS is allowed to have management access.
- **[snmp]**: Configure if SNMP is allowed to have management access.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..16</td>
<td>Pool entry index.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-3</td>
<td>0..32</td>
<td>Prefix length netmask.</td>
</tr>
<tr>
<td>P-4</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
<tr>
<td>P-5</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
<tr>
<td>P-6</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

28.1.3 network management access delete

Delete an entry with index.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `network management access delete <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..16</td>
<td>Pool entry index.</td>
</tr>
</tbody>
</table>

28.1.4 network management access modify

Modify an entry with index.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `network management access modify <P-1> ip <P-2> mask <P-3> http <P-4> https <P-5> snmp <P-6>`

- **ip**: Configure ip-address which should have access to management.
- **mask**: Configure network mask to allow a subnet for management access.
- **http**: Configure if HTTP is allowed to have management access.
- **https**: Configure if HTTPS is allowed to have management access.
- **snmp**: Configure if SNMP is allowed to have management access.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..16</td>
<td>Pool entry index.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>
28.2 show

Display device options and settings.

28.2.1 show network management access global

Display the global restricted management access preferences.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..16</td>
<td>Pool entry index.</td>
</tr>
</tbody>
</table>

28.2.2 show network management access rules

Display the restricted management access rules.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..16</td>
<td>Pool entry index.</td>
</tr>
</tbody>
</table>
29 Network Address Translation (NAT)

29.1 nat

Manage NAT rules

29.1.1 nat dnat commit

Commit pending changes for DNAT (commits all NAT changes).

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** nat dnat commit

29.1.2 nat dnat add

Add rule to DNAT

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** nat dnat add <P-1> [cfg <P-2> <P-3> <P-4> <P-5> <P-6> <P-7> <P-8> [<P-9>]]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>DNAT rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>Source IP address</td>
</tr>
<tr>
<td></td>
<td>a.b.c/d</td>
<td>CIDR mask</td>
</tr>
<tr>
<td></td>
<td>!a.b.c.d</td>
<td>Everything BUT this address</td>
</tr>
<tr>
<td></td>
<td>!a.b.c.d/n</td>
<td>Everything BUT this CIDR mask</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any</td>
</tr>
<tr>
<td>P-3</td>
<td>number</td>
<td>number UDP/TCP Source Port</td>
</tr>
<tr>
<td></td>
<td>nu-nu</td>
<td>nu-nu Port Range</td>
</tr>
<tr>
<td></td>
<td>nu.nu-nu</td>
<td>nu.nu-nu List of ports (or port ranges)</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any Any</td>
</tr>
<tr>
<td>P-4</td>
<td>a.b.c.d</td>
<td>Destination IP address</td>
</tr>
<tr>
<td></td>
<td>a.b.c/d</td>
<td>CIDR mask</td>
</tr>
<tr>
<td></td>
<td>!a.b.c.d</td>
<td>Everything BUT this address</td>
</tr>
<tr>
<td></td>
<td>!a.b.c.d/n</td>
<td>Everything BUT this CIDR mask</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any Any</td>
</tr>
<tr>
<td>P-5</td>
<td>number</td>
<td>number of the UDP/TCP Destination Port</td>
</tr>
<tr>
<td></td>
<td>nu-nu</td>
<td>nu-nu Port Range</td>
</tr>
<tr>
<td></td>
<td>number,number</td>
<td>nu.nu-nu List of ports (or port ranges)</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any Any Port (or protocol without a port)</td>
</tr>
<tr>
<td>P-6</td>
<td>a.b.c.d</td>
<td>New destination IP address</td>
</tr>
<tr>
<td>P-7</td>
<td>number</td>
<td>number of the UDP/TCP New Destination Port</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any Any Port (or protocol without a port)</td>
</tr>
<tr>
<td>P-8</td>
<td>icmp</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td></td>
<td>igmp</td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td></td>
<td>ipip</td>
<td>IP-within-IP Encapsulation Protocol</td>
</tr>
<tr>
<td></td>
<td>tcp</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td></td>
<td>udp</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td></td>
<td>esp</td>
<td>Encapsulating Security Protocol</td>
</tr>
<tr>
<td></td>
<td>ah</td>
<td>Authentication Header</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any of the above</td>
</tr>
<tr>
<td>P-9</td>
<td>string</td>
<td>Rule description/name</td>
</tr>
</tbody>
</table>

29.1.3 nat dnat modify

Configure single DNAT rule

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** nat dnat modify <P-1> <P-2> <P-3> <P-4> <P-5> <P-6> <P-7> <P-8> [<P-9>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>DNAT rule number</td>
</tr>
</tbody>
</table>
29.1 nat

29.1.4 nat dnat delete
Delete rule from DNAT

- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: nat dnat delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>DNAT rule number</td>
</tr>
</tbody>
</table>

29.1.5 nat dnat logtrap
Set log/trap for DNAT rule

- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: nat dnat logtrap <P-1> <P-2> <P-3>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>DNAT rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>no</td>
<td>Disable Logging</td>
</tr>
<tr>
<td></td>
<td>yes</td>
<td>Enable Logging</td>
</tr>
<tr>
<td>P-3</td>
<td>no</td>
<td>Disable SNMP Trap</td>
</tr>
<tr>
<td></td>
<td>yes</td>
<td>Enable SNMP Trap</td>
</tr>
</tbody>
</table>

29.1.6 nat dnat state
Enable/Disable specific DNAT rule

- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: nat dnat state <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>DNAT rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>
29.1.7 nat dnat if add
Add Interface
➤ Mode: Global Config Mode
➤ Privilege Level: Operator
➤ Format: nat dnat if add <P-1> <P-2> <P-3>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>1..255</td>
<td>DNAT rule number</td>
</tr>
<tr>
<td>P-3</td>
<td>0.4294967295</td>
<td>Priority</td>
</tr>
</tbody>
</table>

29.1.8 nat dnat if delete
Delete interface
➤ Mode: Global Config Mode
➤ Privilege Level: Operator
➤ Format: nat dnat if delete <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>1..255</td>
<td>DNAT rule number</td>
</tr>
</tbody>
</table>

29.1.9 nat 1to1nat commit
Commit pending changes for 1:1 NAT (commits every NAT change).
➤ Mode: Global Config Mode
➤ Privilege Level: Operator
➤ Format: nat 1to1nat commit

29.1.10 nat 1to1nat add
Add rule to 1:1 NAT
➤ Mode: Global Config Mode
➤ Privilege Level: Operator
➤ Format: nat 1to1nat add <P-1> [cfg <P-2> <P-3> <P-4>] [ingress <P-5>] [egress <P-6> [P-7]]
[cfg]: Configure the rule immediately
[ingress]: Configure ingress interface
[egress]: Configure egress interface

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>1:1 NAT rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>Virtual destination IP address</td>
</tr>
<tr>
<td></td>
<td>a.b.c.d/n</td>
<td>CIDR mask</td>
</tr>
<tr>
<td>P-3</td>
<td>a.b.c.d</td>
<td>Actual destination IP address</td>
</tr>
<tr>
<td></td>
<td>a.b.c.d/n</td>
<td>CIDR mask</td>
</tr>
<tr>
<td>P-4</td>
<td>0.4294967295</td>
<td>Priority</td>
</tr>
<tr>
<td>P-5</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-6</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-7</td>
<td>string</td>
<td>Rule description/name</td>
</tr>
</tbody>
</table>

29.1.11 nat 1to1nat modify
Configure single 1:1 NAT rule
➤ Mode: Global Config Mode
➤ Privilege Level: Operator
➤ Format: nat 1to1nat modify <P-1> <P-2> <P-3> <P-4> [ingress <P-5>] [egress <P-6> [P-7]]
[ingress]: Configure ingress interface
[egress]: Configure egress interface

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>1:1 NAT rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>Virtual destination IP address</td>
</tr>
<tr>
<td></td>
<td>a.b.c.d/n</td>
<td>CIDR mask</td>
</tr>
<tr>
<td>P-3</td>
<td>a.b.c.d</td>
<td>Actual destination IP address</td>
</tr>
<tr>
<td></td>
<td>a.b.c.d/n</td>
<td>CIDR mask</td>
</tr>
<tr>
<td>P-4</td>
<td>0.4294967295</td>
<td>Priority</td>
</tr>
<tr>
<td>P-5</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>
Network Address Translation (NAT)

29.1 nat

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-6</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-7</td>
<td>string</td>
<td>Rule description/name</td>
</tr>
</tbody>
</table>

### 29.1.12 nat 1to1nat delete
Delete the rule from 1:1 NAT

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** nat 1to1nat delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>1:1 NAT rule number</td>
</tr>
</tbody>
</table>

### 29.1.13 nat 1to1nat logtrap
Set log/trap for 1:1 NAT rule

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** nat 1to1nat logtrap <P-1> <P-2> <P-3>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>1:1 NAT rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>no</td>
<td>Disable Logging</td>
</tr>
<tr>
<td></td>
<td>yes</td>
<td>Enable Logging</td>
</tr>
<tr>
<td>P-3</td>
<td>no</td>
<td>Disable SNMP Trap</td>
</tr>
<tr>
<td></td>
<td>yes</td>
<td>Enable SNMP Trap</td>
</tr>
</tbody>
</table>

### 29.1.14 nat 1to1nat state
Enable/Disable specific 1:1 NAT rule

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** nat 1to1nat state <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>1:1 NAT rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

### 29.1.15 nat masq commit
Commit pending changes for Masquerading (commits every NAT change).

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** nat masq commit

### 29.1.16 nat masq add
Add rule to Masquerading

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** nat masq add <P-1> [cfg <P-2> <P-3> <P-4> [P-5]]

[cfg]: Configure the rule immediately

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..128</td>
<td>Masquerading rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>Source IP address</td>
</tr>
<tr>
<td></td>
<td>a.b.c.d/n</td>
<td>CIDR mask</td>
</tr>
<tr>
<td></td>
<td>!a.b.c.d</td>
<td>Everything BUT this address</td>
</tr>
<tr>
<td></td>
<td>!a.b.c.d/n</td>
<td>Everything BUT this CIDR mask</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any</td>
</tr>
<tr>
<td>P-3</td>
<td>number</td>
<td>number UDP/TCP Source Port</td>
</tr>
<tr>
<td></td>
<td>nu-nu</td>
<td>nu-nu Port Range</td>
</tr>
<tr>
<td></td>
<td>nu.nu-nu</td>
<td>List of ports (or port ranges)</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any port (or protocol without a port)</td>
</tr>
<tr>
<td>P-4</td>
<td>tcp</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td></td>
<td>udp</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any protocol at all</td>
</tr>
<tr>
<td>P-5</td>
<td>string</td>
<td>Rule description/name</td>
</tr>
</tbody>
</table>
29.1.17 nat masq modify
Configure single Masquerading rule
► Mode: Global Config Mode
► Privilege Level: Operator
► Format: nat masq modify <P-1> <P-2> <P-3> <P-4> [ <P-5> ]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..128</td>
<td>Masquerading rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>Source IP address</td>
</tr>
<tr>
<td></td>
<td>a.b.c.d/n</td>
<td>CIDR mask</td>
</tr>
<tr>
<td></td>
<td>![a.b.c.d]</td>
<td>Everything BUT this address</td>
</tr>
<tr>
<td></td>
<td>![a.b.c.d/n]</td>
<td>Everything BUT this CIDR mask</td>
</tr>
<tr>
<td>P-3</td>
<td>number</td>
<td>number UDP/TCP Source Port</td>
</tr>
<tr>
<td></td>
<td>nu-nu</td>
<td>nu-nu Port Range</td>
</tr>
<tr>
<td></td>
<td>nu-nu-nu</td>
<td>nu-nu-nu list of ports (or port ranges)</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>any Any</td>
</tr>
<tr>
<td>P-4</td>
<td>tcp</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td></td>
<td>udp</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any protocol at all</td>
</tr>
<tr>
<td>P-5</td>
<td>string</td>
<td>Rule description/name</td>
</tr>
</tbody>
</table>

29.1.18 nat masq delete
Delete rule from Masquerading
► Mode: Global Config Mode
► Privilege Level: Operator
► Format: nat masq delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..128</td>
<td>Masquerading rule number</td>
</tr>
</tbody>
</table>

29.1.19 nat masq logtrap
Set log/trap for Masquerading rule
► Mode: Global Config Mode
► Privilege Level: Operator
► Format: nat masq logtrap <P-1> <P-2> <P-3>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..128</td>
<td>Masquerading rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>no</td>
<td>Disable Logging</td>
</tr>
<tr>
<td></td>
<td>yes</td>
<td>Enable Logging</td>
</tr>
<tr>
<td>P-3</td>
<td>no</td>
<td>Disable SNMP Trap</td>
</tr>
<tr>
<td></td>
<td>yes</td>
<td>Enable SNMP Trap</td>
</tr>
</tbody>
</table>

29.1.20 nat masq ipsec-exempt
Exclude IPsec traffic from Masquerading rule
► Mode: Global Config Mode
► Privilege Level: Operator
► Format: nat masq ipsec-exempt <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..128</td>
<td>Masquerading rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>disabled</td>
<td>Apply rule to IPsec traffic</td>
</tr>
<tr>
<td></td>
<td>enabled</td>
<td>Do not apply rule to IPsec traffic</td>
</tr>
</tbody>
</table>

29.1.21 nat masq state
Enable/Disable specific Masquerading rule
► Mode: Global Config Mode
► Privilege Level: Operator
► Format: nat masq state <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..128</td>
<td>Masquerading rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>
Network Address Translation (NAT)
29.1 nat

29.1.22 nat masq if add
Add interface
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Operator
  ▶ Format: nat masq if add <P-1> <P-2> <P-3>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>1..128</td>
<td>Masquerading rule number</td>
</tr>
<tr>
<td>P-3</td>
<td>0..4294967295</td>
<td>Priority</td>
</tr>
</tbody>
</table>

29.1.23 nat masq if delete
Delete interface
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Operator
  ▶ Format: nat masq if delete <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>1..128</td>
<td>Masquerading rule number</td>
</tr>
</tbody>
</table>

29.1.24 nat doublenat commit
Commit pending changes for Double NAT (commits all NAT changes).
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Operator
  ▶ Format: nat doublenat commit

29.1.25 nat doublenat add
Add rule to Double NAT
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Operator
  ▶ Format: nat doublenat add <P-1> [cfg <P-2> <P-3> <P-4> <P-5> [<P-6>]]
[cfg]: Configure the rule immediately

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Double NAT rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>Local internal IP address</td>
</tr>
<tr>
<td>P-3</td>
<td>a.b.c.d</td>
<td>Local external IP address</td>
</tr>
<tr>
<td>P-4</td>
<td>a.b.c.d</td>
<td>Remote Internal IP Address</td>
</tr>
<tr>
<td>P-5</td>
<td>a.b.c.d</td>
<td>Remote External IP Address</td>
</tr>
<tr>
<td>P-6</td>
<td>string</td>
<td>Rule description/name</td>
</tr>
</tbody>
</table>

29.1.26 nat doublenat modify
Configure single Double NAT rule
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Operator
  ▶ Format: nat doublenat modify <P-1> <P-2> <P-3> <P-4> <P-5> [<P-6>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Double NAT rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>Local internal IP address</td>
</tr>
<tr>
<td>P-3</td>
<td>a.b.c.d</td>
<td>Local external IP address</td>
</tr>
<tr>
<td>P-4</td>
<td>a.b.c.d</td>
<td>Remote Internal IP Address</td>
</tr>
<tr>
<td>P-5</td>
<td>a.b.c.d</td>
<td>Remote External IP Address</td>
</tr>
<tr>
<td>P-6</td>
<td>string</td>
<td>Rule description/name</td>
</tr>
</tbody>
</table>

29.1.27 nat doublenat delete
Delete rule from Double NAT
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Operator
  ▶ Format: nat doublenat delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Double NAT rule number</td>
</tr>
</tbody>
</table>
29.1.28 nat doublenat logtrap
Set log/trap for Double NAT rule
▶ Mode: Global Config Mode
▶ Privilege Level: Operator
▶ Format: nat doublenat logtrap <P-1> <P-2> <P-3>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Double NAT rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>no</td>
<td>Disable Logging</td>
</tr>
<tr>
<td></td>
<td>yes</td>
<td>Enable Logging</td>
</tr>
<tr>
<td>P-3</td>
<td>no</td>
<td>Disable SNMP Trap</td>
</tr>
<tr>
<td></td>
<td>yes</td>
<td>Enable SNMP Trap</td>
</tr>
</tbody>
</table>

29.1.29 nat doublenat state
Enable/Disable specific Double NAT rule
▶ Mode: Global Config Mode
▶ Privilege Level: Operator
▶ Format: nat doublenat state <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Double NAT rule number</td>
</tr>
<tr>
<td>P-2</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

29.1.30 nat doublenat if add
Add Interface
▶ Mode: Global Config Mode
▶ Privilege Level: Operator
▶ Format: nat doublenat if add <P-1> <P-2> <P-3> <P-4>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td>Ingress</td>
</tr>
<tr>
<td>P-2</td>
<td>ingress</td>
<td>Egress</td>
</tr>
<tr>
<td></td>
<td>egress</td>
<td>Both</td>
</tr>
<tr>
<td></td>
<td>both</td>
<td></td>
</tr>
<tr>
<td>P-3</td>
<td>1..255</td>
<td>Double NAT rule number</td>
</tr>
<tr>
<td>P-4</td>
<td>0..4294967295</td>
<td>Priority</td>
</tr>
</tbody>
</table>

29.1.31 nat doublenat if delete
Delete interface
▶ Mode: Global Config Mode
▶ Privilege Level: Operator
▶ Format: nat doublenat if delete <P-1> <P-2> <P-3>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td>Ingress</td>
</tr>
<tr>
<td>P-2</td>
<td>ingress</td>
<td>Egress</td>
</tr>
<tr>
<td></td>
<td>egress</td>
<td>Both</td>
</tr>
<tr>
<td></td>
<td>both</td>
<td></td>
</tr>
<tr>
<td>P-3</td>
<td>1..255</td>
<td>Double NAT rule number</td>
</tr>
</tbody>
</table>

29.2 show
Display device options and settings.

29.2.1 show nat dnat global
Display the summary.
▶ Mode: Command is in all modes available.
▶ Privilege Level: Guest
▶ Format: show nat dnat global
29.2.2  show nat dnat rules
Display the DNAT rules.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show nat dnat rules [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>DNAT rule number</td>
</tr>
</tbody>
</table>

29.2.3  show nat dnat if
Display the DNAT interface configuration.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show nat dnat if

29.2.4  show nat dnat logtrap
Display the Log/Trap settings for the DNAT rules.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show nat dnat logtrap [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>DNAT rule number</td>
</tr>
</tbody>
</table>

29.2.5  show nat masq global
Display the summary.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show nat masq global

29.2.6  show nat masq rules
Display the masquerading rules.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show nat masq rules [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..128</td>
<td>Masquerading rule number</td>
</tr>
</tbody>
</table>

29.2.7  show nat masq logtrap
Display the Log/Trap settings for the masquerading rules.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show nat masq logtrap [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..128</td>
<td>Masquerading rule number</td>
</tr>
</tbody>
</table>

29.2.8  show nat masq if
Display the masquerading interface configuration.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show nat masq if

29.2.9  show nat 1to1nat global
Display the summary.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show nat 1to1nat global
### 29.2.10 show nat 1to1nat rules

Display the 1:1 NAT rules.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: `show nat 1to1nat rules [<P-1>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>1:1 NAT rule number</td>
</tr>
</tbody>
</table>

### 29.2.11 show nat 1to1nat logtrap

Display the Log/Trap settings for 1:1 NAT rules.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: `show nat 1to1nat logtrap [<P-1>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>1:1 NAT rule number</td>
</tr>
</tbody>
</table>

### 29.2.12 show nat doublenat global

Display the summary.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: `show nat doublenat global`

### 29.2.13 show nat doublenat rules

Display the Double NAT rules.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: `show nat doublenat rules [<P-1>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Double NAT rule number</td>
</tr>
</tbody>
</table>

### 29.2.14 show nat doublenat logtrap

Display the Log/Trap settings for the Double NAT rules.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: `show nat doublenat logtrap [<P-1>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Double NAT rule number</td>
</tr>
</tbody>
</table>

### 29.2.15 show nat doublenat if

Display the Double NAT interface configuration.
- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: `show nat doublenat if`
30 Network Time Protocol (NTP)

30.1 ntp

Configure NTP settings.

30.1.1 ntp client operation

Enable or disable the NTP client.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ntp client operation <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

30.1.2 ntp client operating-mode

Set the NTP client operating mode.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ntp client operating-mode <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>unicast</td>
<td>Enable NTP client in unicast operating mode.</td>
</tr>
<tr>
<td></td>
<td>broadcast</td>
<td>Enable NTP client in broadcast operating mode.</td>
</tr>
</tbody>
</table>

30.1.3 ntp server operation

Enable or disable the NTP server.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ntp server operation <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

30.1.4 ntp server operating-mode

Set the NTP server operating mode.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ntp server operating-mode <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>symmetric</td>
<td>Enable NTP server in symmetric operating mode.</td>
</tr>
<tr>
<td></td>
<td>client-server</td>
<td>Enable NTP server in client-server operating mode.</td>
</tr>
</tbody>
</table>

30.1.5 ntp server localclock-stratum

Set the stratum of the localclock.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ntp server localclock-stratum <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..16</td>
<td>Localclock stratum.</td>
</tr>
</tbody>
</table>

30.1.6 ntp peers add

Add a new peer.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ntp peers add <P-1> ip <P-2> [iburst <P-3>] [burst <P-4>] [prefer <P-5>]

  - ip: Set the peer address.
  - [iburst]: Speed up the initial synchronization (default: disabled). Used only when operating in client-unicast mode.
30.2 show

Display device options and settings.

30.2.1 show ntp client-status

Status of the NTP client connection.

Mode: Command is in all modes available.
Privilege Level: Guest
Format: show ntp client-status

30.2.2 show ntp server-status

Overall operational status of the NTP server.

Mode: Command is in all modes available.
Privilege Level: Guest
Format: show ntp server-status

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>NTP servers index.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-3</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
<tr>
<td>P-4</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
<tr>
<td>P-5</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>
31 Packet Filter

31.1 packet-filter

Creation and configuration of Firewall rules.

31.1.1 packet-filter l3 commit

Writes all changes made in the L3 firewall configuration to the device

- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: packet-filter l3 commit

31.1.2 packet-filter l3 defaultpolicy

Sets the default policy of the L3 and DynFw rule tables

- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: packet-filter l3 defaultpolicy <P-1>

31.1.3 packet-filter l3 checksum-validation

Configures the connection tracking checksum validation in Netfilter

- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: packet-filter l3 checksum-validation

- **no packet-filter l3 checksum-validation**

  Disable the option

  - **Mode**: Global Config Mode
  - **Privilege Level**: Operator
  - **Format**: no packet-filter l3 checksum-validation

31.1.4 packet-filter l3 addrule

Adds a rule to the L3 firewall table

- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: packet-filter l3 addrule <P-1> <P-2> <P-3> <P-4> <P-5> <P-6> <P-7> <P-8> [description <P-9>] [profile-index <P-10>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>accept</td>
<td>Accept packets</td>
</tr>
<tr>
<td></td>
<td>drop</td>
<td>Drop packets without notification</td>
</tr>
<tr>
<td></td>
<td>reject</td>
<td>Drop packets and notify source</td>
</tr>
</tbody>
</table>

### Parameter Value

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>accept</td>
<td>Accept packets</td>
</tr>
<tr>
<td></td>
<td>drop</td>
<td>Drop packets without notification</td>
</tr>
<tr>
<td></td>
<td>reject</td>
<td>Drop packets and notify source</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Source IP address/CIDR mask/'any'</td>
</tr>
<tr>
<td>P-3</td>
<td>string</td>
<td>Source port/port list with comma/port range with hyphen/'any'</td>
</tr>
<tr>
<td>P-4</td>
<td>string</td>
<td>Target IP address/CIDR mask/'any'</td>
</tr>
<tr>
<td>P-5</td>
<td>string</td>
<td>Target port/port list with comma/port range with hyphen/'any'</td>
</tr>
<tr>
<td>P-6</td>
<td>icmp</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td></td>
<td>igmp</td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td></td>
<td>igmp</td>
<td>IP-within-IP Encapsulation Protocol</td>
</tr>
<tr>
<td></td>
<td>tcp</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td></td>
<td>udp</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td></td>
<td>esp</td>
<td>Encapsulating Security Protocol</td>
</tr>
<tr>
<td></td>
<td>ah</td>
<td>Authentication Header</td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Any of the above</td>
</tr>
</tbody>
</table>


### 31.1.5 packet-filter l3 modifyrule

Modifies a rule to the L3 firewall table

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:**
  ```
  packet-filter l3 modifyrule <P-1> <P-2> <P-3> <P-4> <P-5> <P-6> <P-7> <P-8>
  [description <P-9>] [profile-index <P-10>]
  ```
- **Parameters:**
  - `P-1`: Rule index (1..2048)
  - `P-2`: Source IP address/CIDR mask/’any’
  - `P-3`: Source port/port list with comma/port range with hyphen/’any’
  - `P-4`: Target IP address/CIDR mask/’any’
  - `P-5`: Target port/port list with comma/port range with hyphen/’any’
  - `P-7`: Parameters for rule (or 'none')
  - `P-8`: Accept packets, Drop packets without notification, Drop packets and notify source
  - `P-9`: Rule description/name
  - `P-10`: Profile index 0 - 32

### 31.1.6 packet-filter l3 delrule

Deletes a rule from L3 rule table

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:**
  ```
  packet-filter l3 delrule <P-1>
  ```

### 31.1.7 packet-filter l3 enablerule

Enables a rule from L3 rule table. A rule can only be activated when all required parameters are set and at least one interface is mapped to the rule. You cannot activate a rule if an enforcer mappings to an inactive profile.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:**
  ```
  packet-filter l3 enablerule <P-1>
  ```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-7</td>
<td>string</td>
<td>Parameters for rule (or 'none')</td>
</tr>
<tr>
<td>P-8</td>
<td>accept</td>
<td>Accept packets</td>
</tr>
<tr>
<td></td>
<td>drop</td>
<td>Drop packets without notification</td>
</tr>
<tr>
<td></td>
<td>reject</td>
<td>Drop packets and notify source</td>
</tr>
<tr>
<td></td>
<td>enforce-modbus</td>
<td>Accept or drop packets by Modbus TCP/IP enforcer, protocol should be tcp or udp</td>
</tr>
<tr>
<td></td>
<td>enforce-opc</td>
<td>Accept or drop packets by opc enforcer, protocol should be tcp</td>
</tr>
<tr>
<td></td>
<td>enforce-iec104</td>
<td>Accept or drop packets by IEC104 enforcer, protocol should be tcp</td>
</tr>
<tr>
<td></td>
<td>enforce-dnp3</td>
<td>Accept or drop packets by DNP3 enforcer, protocol should be tcp</td>
</tr>
<tr>
<td>P-9</td>
<td>string</td>
<td>Rule description/name</td>
</tr>
<tr>
<td>P-10</td>
<td>0..32</td>
<td>Profile index 0 - 32</td>
</tr>
</tbody>
</table>
### 31.1.8 packet-filter l3 disablerule

Disables a rule from L3 rule table

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `packet-filter l3 disablerule <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..2048</td>
<td>Rule index</td>
</tr>
</tbody>
</table>

### 31.1.9 packet-filter l3 logmode

Set logmode for a rule from L3 rule table

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `packet-filter l3 logmode <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..2048</td>
<td>Rule index</td>
</tr>
<tr>
<td>P-2</td>
<td>log, trap, logtrap, none</td>
<td>Log when rule is applied, Send trap when rule is applied, Log and send trap when rule is applied, Disable log and trap</td>
</tr>
</tbody>
</table>

### 31.1.10 packet-filter l3 addif

Adds an interface to a L3 firewall rule

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `packet-filter l3 addif <P-1> <P-2> <P-3> <P-4>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>ingress, egress</td>
<td>Rule applies on ingress direction, Rule applies on egress direction,</td>
</tr>
<tr>
<td>P-3</td>
<td>1..2048</td>
<td>Rule index</td>
</tr>
<tr>
<td>P-4</td>
<td>0..4294967295</td>
<td>Priority</td>
</tr>
</tbody>
</table>

### 31.1.11 packet-filter l3 delif

Deletes an interface of a L3 firewall rule

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `packet-filter l3 delif <P-1> <P-2> <P-3>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>ingress, egress</td>
<td>Rule applies on ingress direction, Rule applies on egress direction,</td>
</tr>
<tr>
<td>P-3</td>
<td>1..2048</td>
<td>Rule index</td>
</tr>
</tbody>
</table>

### 31.1.12 packet-filter l3 enableif

Enables an interface of a L3 firewall rule

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `packet-filter l3 enableif <P-1> <P-2> <P-3>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>ingress, egress</td>
<td>Rule applies on ingress direction, Rule applies on egress direction,</td>
</tr>
<tr>
<td>P-3</td>
<td>1..2048</td>
<td>Rule index</td>
</tr>
</tbody>
</table>
31.1.13 packet-filter l3 disableif
Disables an interface of a L3 firewall rule

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** packet-filter l3 disableif <P-1> <P-2> <P-3>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>ingress</td>
<td>Rule applies on ingress direction.</td>
</tr>
<tr>
<td></td>
<td>egress</td>
<td>Rule applies on egress direction.</td>
</tr>
<tr>
<td>P-3</td>
<td>1..2048</td>
<td>Rule index</td>
</tr>
</tbody>
</table>

31.1.14 packet-filter l2 commit
Writes all changes made in the L2 firewall configuration to the device

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** packet-filter l2 commit

31.1.15 packet-filter l2 defaultpolicy
Sets the default policy of the L2 rule tables.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** packet-filter l2 defaultpolicy <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>accept</td>
<td>Accept packets.</td>
</tr>
<tr>
<td></td>
<td>drop</td>
<td>Drop packets without notification.</td>
</tr>
</tbody>
</table>

31.1.16 packet-filter l2 fcs-validation
Activates/Deactivates FCS validation

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** packet-filter l2 fcs-validation <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

31.1.17 packet-filter l2 rule add
Adds a rule to the L2 firewall table.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** packet-filter l2 rule add <P-1> action <P-2> [src-mac <P-3>] [dst-mac <P-4>] [src-ip <P-5>] [sourceport <P-6>] [dest-ip <P-7>] [destport <P-8>] [ethertype <P-9>] [proto <P-10>] [vlan <P-11>] [description <P-12>] [rule-limit <P-13> <P-14> <P-15>] [tos <P-16>] [log <P-17>] [trap <P-18>]

  **action:** Set Action
  - [src-mac]: Specify the source MAC address.
  - [dst-mac]: Specify the destination MAC address.
  - [src-ip]: Specify the source IP address/mask.
  - [sourceport]: Specify the source L4 port.
  - [dest-ip]: Specify the destination IP address/mask.
  - [destport]: Specify the destination L4 port.
  - [ethertype]: Specify the Ethertype.
  - [proto]: Specify the protocol for L2 firewall rule.
  - [vlan]: Specify the VLAN ID for L2 firewall rule.
  - [description]: Rule description/name for the L2 firewall rule.
  - [rule-limit]: Specify the rate limit and burst size.
  - [tos]: Specify TOS for L2 rule.
  - [log]: Set logging.
  - [trap]: Set sending SNMP traps.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1.999</td>
<td>Rule index</td>
</tr>
</tbody>
</table>
no packet-filter l2 rule add

Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** no packet-filter l2 rule add action [src-mac] [dst-mac] [src-ip] [sourceport] [dest-ip] [destport] [ethertype] [proto] [vlan] [description] [rate-limit] [tos] [log <P-17>] [trap <P-18>]
31.1.18 packet-filter l2 rule modify

Modifies a rule to the L2 firewall table.

- **Mode**: Global Config Mode
- **Privilege Level**: Operator
- **Format**: packet-filter l2 rule modify <P-1> action <P-2> [src-mac <P-3>] [dst-mac <P-4>] [src-ip <P-5>] [sourceport <P-6>] [dest-ip <P-7>] [destport <P-8>] [ethertype <P-9>] [proto <P-10>] [vlan <P-11>] [description <P-12>] [rate-limit <P-13> <P-14> <P-15>] [tos <P-16>] [log <P-17>] [trap <P-18>]

**action**
- **Set Action**

- **[src-mac]**: Specify the source MAC address.
- **[dst-mac]**: Specify the destination MAC address.
- **[src-ip]**: Specify the source IP address/mask.
- **[sourceport]**: Specify the source L4 port.
- **[dest-ip]**: Specify the destination IP address/mask.
- **[destport]**: Specify the destination L4 port.
- **[ethertype]**: Specify the Ethertype.
- **[proto]**: Specify the protocol for L2 firewall rule.
- **[vlan]**: Specify the VLAN ID for L2 firewall rule.
- **[description]**: Rule description/name for L2 firewall rule.
- **[rate-limit]**: Specify the rate limit and burst size.
- **[tos]**: Specify TOS for L2 rule.
- **[log]**: Set logging.
- **[trap]**: Set sending SNMP traps.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..999</td>
<td>Rule index</td>
</tr>
<tr>
<td>P-2</td>
<td>accept, drop</td>
<td>Accept packets, Drop packets without notification.</td>
</tr>
<tr>
<td>P-3</td>
<td>any</td>
<td>Enter any as a shortcut for the MAC address 00:00:00:00:00:00.</td>
</tr>
<tr>
<td></td>
<td>aa:bb:cc:dd:ee:ff</td>
<td>Enter the MAC address in hexadecimal format.</td>
</tr>
<tr>
<td>P-4</td>
<td>any</td>
<td>Enter any as a shortcut for the MAC address 00:00:00:00:00:00.</td>
</tr>
<tr>
<td></td>
<td>aa:bb:cc:dd:ee:ff</td>
<td>Enter the MAC address in hexadecimal format.</td>
</tr>
<tr>
<td>P-5</td>
<td>string</td>
<td>Source IP address/CIDR mask/’any’</td>
</tr>
<tr>
<td>P-6</td>
<td>any</td>
<td>any Any port/portless protocol</td>
</tr>
<tr>
<td></td>
<td>a-b Port Range</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a-b Port Range</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a-b,c-d List of Port Ranges (may be longer than two ranges)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 to 65535 Port Number</td>
<td></td>
</tr>
<tr>
<td>P-7</td>
<td>string</td>
<td>Target IP address/CIDR mask/’any’</td>
</tr>
<tr>
<td>P-8</td>
<td>any</td>
<td>any Any port/portless protocol</td>
</tr>
<tr>
<td></td>
<td>a-b Port Range</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a-b Port Range</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a-b,c-d List of Port Ranges (may be longer than two ranges)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 to 65535 Port Number</td>
<td></td>
</tr>
<tr>
<td>P-9</td>
<td>0x0600-0xffff</td>
<td>value Ethertype</td>
</tr>
<tr>
<td></td>
<td>apple Talk</td>
<td>AppleTalk</td>
</tr>
<tr>
<td></td>
<td>ibmsna</td>
<td>IBM SNA</td>
</tr>
<tr>
<td></td>
<td>ipv4</td>
<td>IPv4</td>
</tr>
<tr>
<td></td>
<td>ipv6</td>
<td>IPv6</td>
</tr>
<tr>
<td></td>
<td>ipx-old</td>
<td>IPX-OLD</td>
</tr>
<tr>
<td></td>
<td>mpls-mcast</td>
<td>MPLS Multicast</td>
</tr>
<tr>
<td></td>
<td>mpls-ucast</td>
<td>MPLS Unicast</td>
</tr>
<tr>
<td></td>
<td>netbios</td>
<td>NetBIOS</td>
</tr>
<tr>
<td></td>
<td>novell</td>
<td>NOVELL</td>
</tr>
<tr>
<td></td>
<td>pppoe-disc</td>
<td>PPPoEDISC</td>
</tr>
<tr>
<td></td>
<td>rarp</td>
<td>RARP</td>
</tr>
<tr>
<td></td>
<td>pppoe-session</td>
<td>PPPoESESS</td>
</tr>
<tr>
<td></td>
<td>ipxnew</td>
<td>IPXNEW</td>
</tr>
<tr>
<td></td>
<td>profinet</td>
<td>PROFINET</td>
</tr>
<tr>
<td></td>
<td>powerlink</td>
<td>POWERLINK</td>
</tr>
<tr>
<td></td>
<td>ethercat</td>
<td>ETHERCAT</td>
</tr>
<tr>
<td></td>
<td>vlan8021q</td>
<td>IEEE802_1Q VLAN</td>
</tr>
</tbody>
</table>
### Packet Filter

#### 31.1 packet-filter

**no packet-filter l2 rule modify**

Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** 
  ```
  no packet-filter l2 rule modify action [src-mac] [dst-mac] [src-ip] [sourceport] [dest-ip] [destport] [ethertype] [proto] [vlan] [description] [rate-limit] [tos] [log enable|disable] [trap enable|disable]
  ```

#### 31.1.19 packet-filter l2 rule delete

Deletes a rule from L2 rule table.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** 
  ```
  packet-filter l2 rule delete <P-1>
  ```

#### 31.1.20 packet-filter l2 rule enable

Enables a rule from L2 rule table.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** 
  ```
  packet-filter l2 rule enable <P-1>
  ```

#### 31.1.21 packet-filter l2 rule disable

Disables a rule from L2 rule table.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** 
  ```
  packet-filter l2 rule disable <P-1>
  ```

#### 31.1.22 packet-filter l2 if add

Adds an interface to a L2 firewall rule.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** 
  ```
  packet-filter l2 if add <P-1> <P-2> <P-3> <P-4> <P-5>
  ```

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-10</td>
<td>icmp</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td></td>
<td>igmp</td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td></td>
<td>ipip</td>
<td>IP-within-IP Encapsulation Protocol</td>
</tr>
<tr>
<td></td>
<td>tcp</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td></td>
<td>udp</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td></td>
<td>esp</td>
<td>Encapsulating Security Protocol</td>
</tr>
<tr>
<td></td>
<td>ah</td>
<td>Authentication Header</td>
</tr>
<tr>
<td>any</td>
<td>Any of the above</td>
<td></td>
</tr>
<tr>
<td>P-11</td>
<td>1..4042</td>
<td>Enter a VLAN ID in the given range.</td>
</tr>
<tr>
<td>P-12</td>
<td>string</td>
<td>Rule description/name</td>
</tr>
<tr>
<td>P-13</td>
<td>0..1000000</td>
<td>Committed rate value, specified in kbps or pps.</td>
</tr>
<tr>
<td>P-14</td>
<td>0..128</td>
<td>Committed burst size value, specified in kbytes or pps.</td>
</tr>
<tr>
<td>P-15</td>
<td>pps</td>
<td>Packets per second.</td>
</tr>
<tr>
<td></td>
<td>kbps</td>
<td>kbytes per second.</td>
</tr>
<tr>
<td>P-16</td>
<td>0..255</td>
<td>Specify the IP TOS bits to match.</td>
</tr>
<tr>
<td>P-17</td>
<td>enable</td>
<td>Enable logging when applying the rule</td>
</tr>
<tr>
<td>disalbe</td>
<td>Do not log applying the rule</td>
<td></td>
</tr>
<tr>
<td>P-18</td>
<td>enable</td>
<td>Enable sending a trap when applying the rule</td>
</tr>
<tr>
<td>disalbe</td>
<td>Do not send a trap when applying the rule</td>
<td></td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..999</td>
<td>Rule index</td>
</tr>
<tr>
<td>P-2</td>
<td>port</td>
<td>Interface type to use is physical interface.</td>
</tr>
<tr>
<td></td>
<td>vian</td>
<td>Interface type to use is L2 VLAN.</td>
</tr>
<tr>
<td></td>
<td>1..4042</td>
<td>Interface ID for rule assignment.</td>
</tr>
</tbody>
</table>
31.2 clear

Clear several items.

31.2.1 clear fw-state-table

Clear Firewall connection tracking table.

Mode: Privileged Exec Mode

Format: clear fw-state-table
31.3  show
Display device options and settings.

31.3.1  show packet-filter l3 global
Display the packet-filter global information and settings.
  Mode: Command is in all modes available.
  Privilege Level: Guest
  Format: show packet-filter l3 global

31.3.2  show packet-filter l3 maxrules
Max. number of allowed rules in L3 rule table
  Mode: Command is in all modes available.
  Privilege Level: Guest
  Format: show packet-filter l3 maxrules

31.3.3  show packet-filter l3 defaultpolicy
Default policy (accept(1), drop(2), reject(3))
  Mode: Command is in all modes available.
  Privilege Level: Guest
  Format: show packet-filter l3 defaultpolicy

31.3.4  show packet-filter l3 ruletable
Display the L3 rule table.
  Mode: Command is in all modes available.
  Privilege Level: Guest
  Format: show packet-filter l3 ruletable

31.3.5  show packet-filter l3 iftable
Display the L3 interface mapping table.
  Mode: Command is in all modes available.
  Privilege Level: Guest
  Format: show packet-filter l3 iftable

31.3.6  show packet-filter l3 pending
Display whether uncommitted changes for L3 exist.
  Mode: Command is in all modes available.
  Privilege Level: Guest
  Format: show packet-filter l3 pending

31.3.7  show packet-filter l2 global
Display the packet-filter global information and settings.
  Mode: Command is in all modes available.
  Privilege Level: Guest
  Format: show packet-filter l2 global

31.3.8  show packet-filter l2 rule
Display the L2 rule table.
  Mode: Command is in all modes available.
  Privilege Level: Guest
  Format: show packet-filter l2 rule

31.3.9  show packet-filter l2 if
Display the L2 interface mapping table.
  Mode: Command is in all modes available.
  Privilege Level: Guest
  Format: show packet-filter l2 if
32 Password Management

32.1 passwords

Manage password policies and options.

32.1.1 passwords min-length

Set minimum password length for user passwords.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: passwords min-length <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..64</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

32.1.2 passwords max-login-attempts

Set maximum login attempts for the users.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: passwords max-login-attempts <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..5</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

32.1.3 passwords min-uppercase-chars

Set minimum upper case characters for user passwords.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: passwords min-uppercase-chars <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..16</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

32.1.4 passwords min-lowercase-chars

Set minimum lower case characters for user passwords.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: passwords min-lowercase-chars <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..16</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

32.1.5 passwords min-numeric-chars

Set minimum numeric characters for user passwords.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: passwords min-numeric-chars <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..16</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

32.1.6 passwords min-special-chars

Set minimum special characters for user passwords.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: passwords min-special-chars <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..16</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>
32.1.7  **passwords login-attempt-period**

The time period [minutes] in which the number of failed authentication attempts is counted. Value 0 disables this functionality.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `passwords login-attempt-period <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0</td>
<td>Disables the counting.</td>
</tr>
<tr>
<td></td>
<td>1..60</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

### 32.2  **show**

Display device options and settings.

#### 32.2.1  **show passwords**

Display the password policies and options.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Administrator
- **Format:** `show passwords`
33 Radius

33.1 radius

Configure RADIUS parameters.

33.1.1 radius server attribute 4

Specifies the RADIUS client to use the NAS-IP Address attribute in the RADIUS requests.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** radius server attribute 4 <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

33.1.2 radius server auth add

Add a RADIUS authentication server.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** radius server auth add <P-1> ip <P-2> [name <P-3>] [port <P-4>]

  - ip: RADIUS authentication server IP address.
  - [name]: RADIUS authentication server name.
  - [port]: RADIUS authentication server port (default: 1812).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1.8</td>
<td>Next RADIUS server valid index (it can be seen with '#show radius global' command).</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Hostname or IP address.</td>
</tr>
<tr>
<td>P-3</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
<tr>
<td>P-4</td>
<td>1.65535</td>
<td>Enter port number between 1 and 65535</td>
</tr>
</tbody>
</table>

33.1.3 radius server auth delete

Delete a RADIUS authentication server.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** radius server auth delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1.8</td>
<td>RADIUS server index.</td>
</tr>
</tbody>
</table>

33.1.4 radius server auth modify

Change a RADIUS authentication server parameters.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** radius server auth modify <P-1> [name <P-2>] [port <P-3>] [msgauth <P-4>] [primary <P-5>] [status <P-6>] [secret [ <P-7>]] [encrypted <P-8>]

  - [name]: RADIUS authentication server name.
  - [port]: RADIUS authentication server port (default: 1812).
  - [msgauth]: Enable or disable the message authenticator attribute for this server.
  - [primary]: Configure the primary RADIUS server.
  - [status]: Enable or disable a RADIUS authentication server entry.
  - [secret]: Configure the shared secret for the RADIUS authentication server.
  - [encrypted]: Configure the encrypted shared secret.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1.8</td>
<td>RADIUS server index.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
<tr>
<td>P-3</td>
<td>1.65535</td>
<td>Enter port number between 1 and 65535</td>
</tr>
<tr>
<td>P-4</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
<tr>
<td>P-5</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>
33.2 show

Display device options and settings.

33.2.1 show radius global

Display the global RADIUS configuration.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show radius global

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..15</td>
<td>Maximum number of retransmissions (default: 4).</td>
</tr>
</tbody>
</table>

33.2.2 show radius auth servers

Display the configured RADIUS authentication servers.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show radius auth servers [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..8</td>
<td>RADIUS server index.</td>
</tr>
</tbody>
</table>

33.2.3 show radius auth statistics

Display the RADIUS authentication server statistics.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show radius auth statistics <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..8</td>
<td>RADIUS server index.</td>
</tr>
</tbody>
</table>

33.3 clear

Clear several items.
33.3.1 clear radius

Clear the RADIUS statistics.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** clear radius <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>statistics</td>
<td>Clear the RADIUS statistics.</td>
</tr>
</tbody>
</table>
34 Remote Authentication

34.1 ldap
Configure LDAP settings.

34.1.1 ldap operation
Enable or disable the remote authentication operation.
   - Mode: Global Config Mode
   - Privilege Level: Administrator
   - Format: ldap operation

   **no ldap operation**
   Disable the option
   - Mode: Global Config Mode
   - Privilege Level: Administrator
   - Format: no ldap operation

34.1.2 ldap cache-timeout
Configure LDAP user cache entry timeout.
   - Mode: Global Config Mode
   - Privilege Level: Administrator
   - Format: ldap cache-timeout <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..1440</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

34.1.3 ldap flush-user-cache
Flush LDAP user cache.
   - Mode: Global Config Mode
   - Privilege Level: Administrator
   - Format: ldap flush-user-cache <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>action</td>
<td>Flush the LDAP user cache.</td>
</tr>
</tbody>
</table>

34.1.4 ldap role-policy
Configure LDAP user role selection policy.
   - Mode: Global Config Mode
   - Privilege Level: Administrator
   - Format: ldap role-policy <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>highest</td>
<td>Use the role mapping with the highest user role.</td>
</tr>
<tr>
<td></td>
<td>first</td>
<td>Use the first matching role mapping table entry.</td>
</tr>
</tbody>
</table>

34.1.5 ldap basedn
Base distinguished name for LDAP query at the external AD server.
   - Mode: Global Config Mode
   - Privilege Level: Administrator
   - Format: ldap basedn <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 255 characters.</td>
</tr>
</tbody>
</table>

34.1.6 ldap search-attr
Search attribute for LDAP query at the external AD server.
   - Mode: Global Config Mode
   - Privilege Level: Administrator
   - Format: ldap search-attr <P-1>
34.1.7 ldap bind-user
Bind-account user name for LDAP query at the external AD server.

- **Mode**: Global Config Mode
- **Privilege Level**: Administrator
- **Format**: ldap bind-user <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 64 characters.</td>
</tr>
</tbody>
</table>

34.1.8 ldap bind-passwd
Bind-account user password for LDAP query at the external AD server.

- **Mode**: Global Config Mode
- **Privilege Level**: Administrator
- **Format**: ldap bind-passwd <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 255 characters.</td>
</tr>
</tbody>
</table>

34.1.9 ldap default-domain
Default domain used for users without a domain name.

- **Mode**: Global Config Mode
- **Privilege Level**: Administrator
- **Format**: ldap default-domain <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 64 characters.</td>
</tr>
</tbody>
</table>

34.1.10 ldap client server add
Add a LDAP client server connection.

- **Mode**: Global Config Mode
- **Privilege Level**: Administrator
- **Format**: ldap client server add <P-1> <P-2> [port <P-3>] [security <P-4>] [description <P-5>]
  - **[port]**: Set the port number of the external LDAP server.
  - **[security]**: Set the security settings for the connection to external LDAP server.
  - **[description]**: Description of the external LDAP server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>Enter a number in the given range.</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-3</td>
<td>1..65535</td>
<td>Port number of LDAP Server.</td>
</tr>
<tr>
<td>P-4</td>
<td>none, ssl, startTLS</td>
<td></td>
</tr>
<tr>
<td>P-5</td>
<td>string</td>
<td>Enter a user-defined text, max. 100 characters.</td>
</tr>
</tbody>
</table>

34.1.11 ldap client server delete
Delete a LDAP client server connection.

- **Mode**: Global Config Mode
- **Privilege Level**: Administrator
- **Format**: ldap client server delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

34.1.12 ldap client server enable
Enable a LDAP client server connection.

- **Mode**: Global Config Mode
- **Privilege Level**: Administrator
- **Format**: ldap client server enable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>
34.1.13 ldap client server disable

Disable a LDAP client server connection.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ldap client server disable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

34.1.14 ldap client server modify

Modify a LDAP client server connection.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ldap client server modify <P-1> [addr <P-2>] [port <P-3>] [security <P-4>] [description <P-5>]
  - [addr]: Modify the host address of the external LDAP server.
  - [port]: Modify the port number of the external LDAP server.
  - [security]: Modify the security settings for the connection to external LDAP server.
  - [description]: Modify the description of the external LDAP server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>Enter a number in the given range.</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-3</td>
<td>1.65535</td>
<td>Port number of LDAP Server.</td>
</tr>
<tr>
<td>P-4</td>
<td>none</td>
<td>Enter a user-defined text, max. 100 characters.</td>
</tr>
<tr>
<td></td>
<td>ssl</td>
<td>Enter a user-defined text, max. 100 characters.</td>
</tr>
<tr>
<td></td>
<td>startTLS</td>
<td>Enter a user-defined text, max. 100 characters.</td>
</tr>
</tbody>
</table>

34.1.15 ldap mapping add

Add a LDAP mapping entry.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ldap mapping add <P-1> access-role <P-2> mapping-type <P-3> mapping-parameter <P-4>
  - access-role: Access role type.
  - mapping-type: Role mapping type.
  - mapping-parameter: Role mapping parameter.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..64</td>
<td>Enter a number in the given range.</td>
</tr>
<tr>
<td>P-2</td>
<td>slot no./port no.</td>
<td>Enter a user-defined text, max. 255 characters.</td>
</tr>
<tr>
<td>P-3</td>
<td>attribute</td>
<td>Enter a user-defined text, max. 255 characters.</td>
</tr>
<tr>
<td></td>
<td>group</td>
<td>Enter a user-defined text, max. 255 characters.</td>
</tr>
</tbody>
</table>

34.1.16 ldap mapping delete

Delete a LDAP role mapping entry.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ldap mapping delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..64</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

34.1.17 ldap mapping enable

Activate a LDAP role mapping entry.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ldap mapping enable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..64</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>
### 34.1.18 ldap mapping disable
Deactivate a LDAP role mapping entry.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ldap mapping disable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..64</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

### 34.2 show
Display device options and settings.

#### 34.2.1 show ldap global
Display the LDAP configuration parameters and information.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Administrator
- **Format:** show ldap global

#### 34.2.2 show ldap client server
Display the LDAP client server connections.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Administrator
- **Format:** show ldap client server [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

#### 34.2.3 show ldap mapping
Display the LDAP role mapping entries.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Administrator
- **Format:** show ldap mapping [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..64</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

### 34.3 copy
Copy different kinds of items.

#### 34.3.1 copy ldapcacert remote
Copy CA certificate file (*.pem) from the remote AD server to the specified destination.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** copy ldapcacert remote <P-1> nvm [<P-2>]

nvm: Copy CA certificate file (*.pem) from the remote AD server to the device.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 100 characters.</td>
</tr>
</tbody>
</table>

#### 34.3.2 copy ldapcacert envm
Copy CA certificate file (*.pem) from external non-volatile memory to the specified destination.
- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** copy ldapcacert envm <P-1> nvm [<P-2>]

nvm: Copy CA certificate file (*.pem) from external non-volatile memory to the device.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 100 characters.</td>
</tr>
</tbody>
</table>
35 Remote Monitoring (RMON)

35.1 show

Display device options and settings.

35.1.1 show rmon statistics

Show RMON statistics configuration.

- **Mode**: Command is in all modes available.
- **Privilege Level**: Guest
- **Format**: show rmon statistics [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>
36 Script File

36.1 script

CLI Script File.

36.1.1 script apply

Executes the CLI script file available in the device.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** script apply <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
</tbody>
</table>

36.1.2 script validate

Only validates the CLI script file available in the device.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** script validate <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
</tbody>
</table>

36.1.3 script list system

List all the script files available in the device memory.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** script list system

36.1.4 script list envm

List all the script files available in external non-volatile memory.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** script list envm

36.1.5 script delete

Delete the CLI script files.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** script delete [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
</tbody>
</table>

36.2 copy

Copy different kinds of items.

36.2.1 copy script envm

Copy script file from external non-volatile memory to specified destination.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** copy script envm <P-1> running-config nvm <P-2>

- **running-config:** Copy script file from external non-volatile memory to the running-config.
- **nvm:** Copy script file from external non-volatile memory to the non-volatile memory.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
</tbody>
</table>
36.2.2 copy script remote
Copy script file from server to specified destination.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `copy script remote <P-1> running-config nvms <P-2>`

  - `running-config:` Copy script file from file server to running-config.
  - `nvms:` Copy script file to non-volatile memory.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
</tbody>
</table>

36.2.3 copy script nvms
Copy Script file from non-volatile memory to the specified destination.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `copy script nvms <P-1> running-config envms <P-2> remote <P-3>`

  - `running-config:` Copy Script file from non-volatile system memory to running-config.
  - `envms:` Copy Script file to external non-volatile memory device.
  - `remote:` Copy Script file to file server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
<tr>
<td>P-3</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>

36.3 show
Display device options and settings.

36.3.1 show script envms
Display the content of the CLI script file present in the envms.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Administrator
- **Format:** `show script envms <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
</tbody>
</table>

36.3.2 show script system
Display the content of the CLI script file present in the device.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Administrator
- **Format:** `show script system <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Filename.</td>
</tr>
</tbody>
</table>
37 Selftest

37.1 selftest

Configure the selftest settings.

37.1.1 selftest action

Configure the action that a selftest component should take.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `selftest action <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>task</td>
<td>Configure the action for task errors.</td>
</tr>
<tr>
<td></td>
<td>resource</td>
<td>Configure the action for lack of resources.</td>
</tr>
<tr>
<td></td>
<td>software</td>
<td>Configure the action for broken software integrity.</td>
</tr>
<tr>
<td></td>
<td>hardware</td>
<td>Configure the action for detected hardware errors.</td>
</tr>
<tr>
<td>P-2</td>
<td>log-only</td>
<td>Write a message to the logging file.</td>
</tr>
<tr>
<td></td>
<td>send-trap</td>
<td>Send a trap to the management station.</td>
</tr>
<tr>
<td></td>
<td>reboot</td>
<td>Reboot the device.</td>
</tr>
</tbody>
</table>

37.1.2 selftest ramtest

Enable or disable the RAM selftest on cold start of the device. When disabled the device booting time is reduced.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `selftest ramtest`

- **no selftest ramtest**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** `no selftest ramtest`

37.1.3 selftest system-monitor

Enable or disable the System Monitor 1 access during the boot phase. Please note: If the System Monitor is disabled it is possible to loose access to the device permanently in case of loosing administrator password or misconfiguration.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `selftest system-monitor`

- **no selftest system-monitor**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** `no selftest system-monitor`

37.1.4 selftest boot-default-on-error

Enable or disable loading of the default configuration in case there is any error loading the configuration during boot phase. If disabled the system will be halted.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `selftest boot-default-on-error`

- **no selftest boot-default-on-error**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** `no selftest boot-default-on-error`
37.2  show
Display device options and settings.

37.2.1  show selftest action
Display the actions the device takes if an error occurs.
► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show selftest action

37.2.2  show selftest settings
Display the selftest settings.
► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show selftest settings
38 Small Form-factor Pluggable (SFP)

38.1 show
Display device options and settings.

38.1.1 show sfp
Display the information about the plugged SFP modules.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show sfp [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>
39 Signal Contact

39.1 signal-contact

Configure the signal contact settings.

39.1.1 signal-contact mode

Configure the Signal Contact mode setting.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: signal-contact <P-1> mode <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>signal contact no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>manual</td>
<td>The signal contact's status is determined by the associated manual setting (subcommand 'state').</td>
</tr>
<tr>
<td></td>
<td>monitor</td>
<td>The signal contact's status is determined by the associated monitor settings.</td>
</tr>
<tr>
<td></td>
<td>device-status</td>
<td>The signal contact's status is determined by the device status.</td>
</tr>
<tr>
<td></td>
<td>security-status</td>
<td>The signal contact's status is determined by the security status.</td>
</tr>
<tr>
<td></td>
<td>dev-sec-status</td>
<td>The signal contact's status is determined by the device status and security status.</td>
</tr>
</tbody>
</table>

39.1.2 signal-contact monitor link-failure

Sets the monitoring of the network connection(s).

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: signal-contact <P-1> monitor link-failure

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>signal contact no.</td>
<td></td>
</tr>
</tbody>
</table>

- no signal-contact monitor link-failure
  Disable the option
  - Mode: Global Config Mode
  - Privilege Level: Administrator
  - Format: no signal-contact <P-1> monitor link-failure

39.1.3 signal-contact monitor envm-not-in-sync

Sets the monitoring whether the external non-volatile memory device is in sync with the running configuration.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: signal-contact <P-1> monitor envm-not-in-sync

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>signal contact no.</td>
<td></td>
</tr>
</tbody>
</table>

- no signal-contact monitor envm-not-in-sync
  Disable the option
  - Mode: Global Config Mode
  - Privilege Level: Administrator
  - Format: no signal-contact <P-1> monitor envm-not-in-sync

39.1.4 signal-contact monitor envm-removal

Sets the monitoring of the external non-volatile memory device removal.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: signal-contact <P-1> monitor envm-removal

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>signal contact no.</td>
<td></td>
</tr>
</tbody>
</table>
39.1 signal-contact

- **no signal-contact monitor envm-removal**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** `no signal-contact <P-1> monitor envm-removal`

### 39.1.5 signal-contact monitor temperature

Sets the monitoring of the device temperature.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `signal-contact <P-1> monitor temperature`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>signal contact no.</td>
<td></td>
</tr>
</tbody>
</table>

- **no signal-contact monitor temperature**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** `no signal-contact <P-1> monitor temperature`

### 39.1.6 signal-contact monitor power-supply

Sets the monitoring of the power supply(s).
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `signal-contact <P-1> monitor power-supply <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>signal contact no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>1..2</td>
<td>Number of power supply.</td>
</tr>
</tbody>
</table>

- **no signal-contact monitor power-supply**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** `no signal-contact <P-1> monitor power-supply <P-2>`

### 39.1.7 signal-contact state

Configure the Signal Contact manual state (only takes immediate effect in manual mode).
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `signal-contact <P-1> state <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>signal contact no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>open</td>
<td>Open the signal contact (only takes effect in the manual mode).</td>
</tr>
<tr>
<td></td>
<td>close</td>
<td>Close the signal contact (only takes effect in the manual mode).</td>
</tr>
</tbody>
</table>

### 39.1.8 signal-contact trap

Configure if a trap is sent when the Signal Contact changes state (in monitor mode).
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `signal-contact <P-1> trap`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>signal contact no.</td>
<td></td>
</tr>
</tbody>
</table>

- **no signal-contact trap**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** `no signal-contact <P-1> trap`
39.2 signal-contact
Configure the signal contact interface settings.

39.2.1 signal-contact link-alarm
Configure the monitoring of the specific network ports.
- **Mode:** Interface Range Mode
- **Privilege Level:** Administrator
- **Format:** `signal-contact <P-1> link-alarm`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>signal contact no.</td>
<td></td>
</tr>
</tbody>
</table>

■ no signal-contact link-alarm
Disable the option
- **Mode:** Interface Range Mode
- **Privilege Level:** Administrator
- **Format:** `no signal-contact <P-1> link-alarm`

39.3 show
Display device options and settings.

39.3.1 show signal-contact
Display the signal contact settings.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show signal-contact <P-1> mode monitor state trap link-alarm events all mode` Display the signal contact mode.
  - `monitor`: Display the signal contact monitor settings.
  - `state`: Display the signal contact state (open/close). Note: This covers the signal contact’s administrative setting as well as its actual state.
  - `trap`: Display the signal contact trap information and settings.
  - `link-alarm`: Display the settings of the monitoring of the specific network ports.
  - `events`: Display the occurred device status events.
  - `all`: Display the signal contact settings for the specified signal contact.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>signal contact no.</td>
<td></td>
</tr>
</tbody>
</table>
40 Simple Network Management Protocol (SNMP)

40.1 snmp
Configure of SNMP versions and traps.

40.1.1 snmp access version v1
Enable or disable SNMP version V1.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** snmp access version v1

- **no snmp access version v1**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no snmp access version v1

40.1.2 snmp access version v2
Enable or disable SNMP version V2.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** snmp access version v2

- **no snmp access version v2**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no snmp access version v2

40.1.3 snmp access version v3
Enable or disable SNMP version V3.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** snmp access version v3

- **no snmp access version v3**
  Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no snmp access version v3

40.1.4 snmp access port
Configure the SNMP access port.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** snmp access port <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1-65535</td>
<td>Port number of the SNMP server (default: 161).</td>
</tr>
</tbody>
</table>

40.2 show
Display device options and settings.
40.2.1  show snmp access

Display the SNMP access configuration settings.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show snmp access
41 SNMP Community

41.1 snmp
Configure of SNMP versions and traps.

41.1.1 snmp community ro
SNMP v1/v2 read-only community.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: snmp community ro

41.1.2 snmp community rw
SNMP v1/v2 read-write community.
- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: snmp community rw

41.2 show
Display device options and settings.

41.2.1 show snmp community
Display the SNMP v1/2 community.
- Mode: Command is in all modes available.
- Privilege Level: Administrator
- Format: show snmp community
42 SNMP Logging

42.1 logging

Logging configuration.

42.1.1 logging snmp-request get operation

Enable or disable logging of SNMP GET or SET requests.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: logging snmp-request get operation <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>enable</td>
<td>Enable logging of SNMP GET or SET requests.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable logging of SNMP GET or SET requests.</td>
</tr>
</tbody>
</table>

42.1.2 logging snmp-request get severity

Define severity level.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: logging snmp-request get severity <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>emergency</td>
<td>System is unusable. System failure has occurred.</td>
</tr>
<tr>
<td></td>
<td>alert</td>
<td>Action must be taken immediately. Unrecoverable failure of a component. System failure likely.</td>
</tr>
<tr>
<td></td>
<td>critical</td>
<td>Recoverable failure of a component that may lead to system failure.</td>
</tr>
<tr>
<td></td>
<td>error</td>
<td>Error conditions. Recoverable failure of a component.</td>
</tr>
<tr>
<td></td>
<td>warning</td>
<td>Minor failure, e.g. misconfiguration of a component.</td>
</tr>
<tr>
<td></td>
<td>notice</td>
<td>Normal but significant conditions.</td>
</tr>
<tr>
<td></td>
<td>informational</td>
<td>Informational messages.</td>
</tr>
<tr>
<td></td>
<td>debug</td>
<td>Debug-level messages.</td>
</tr>
<tr>
<td>0</td>
<td>Same as emergency</td>
<td>Same as emergency.</td>
</tr>
<tr>
<td>1</td>
<td>Same as alert</td>
<td>Same as alert.</td>
</tr>
<tr>
<td>2</td>
<td>Same as critical</td>
<td>Same as critical.</td>
</tr>
<tr>
<td>3</td>
<td>Same as error</td>
<td>Same as error.</td>
</tr>
<tr>
<td>4</td>
<td>Same as warning</td>
<td>Same as warning.</td>
</tr>
<tr>
<td>5</td>
<td>Same as notice</td>
<td>Same as notice.</td>
</tr>
<tr>
<td>6</td>
<td>Same as informational</td>
<td>Same as informational.</td>
</tr>
<tr>
<td>7</td>
<td>Same as debug</td>
<td>Same as debug.</td>
</tr>
</tbody>
</table>

42.1.3 logging snmp-request set operation

Enable or disable logging of SNMP GET or SET requests.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: logging snmp-request set operation <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>enable</td>
<td>Enable logging of SNMP GET or SET requests.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable logging of SNMP GET or SET requests.</td>
</tr>
</tbody>
</table>

42.2 no logging snmp-request set operation

Disable the option.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: no logging snmp-request set operation <P-1>
42.1.4 logging snmp-request set severity

Define severity level.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** logging snmp-request set severity <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>emergency</td>
<td>System is unusable. System failure has occurred.</td>
<td></td>
</tr>
<tr>
<td>alert</td>
<td>Action must be taken immediately. Unrecoverable failure of a component. System failure likely.</td>
<td></td>
</tr>
<tr>
<td>critical</td>
<td>Recoverable failure of a component that may lead to system failure.</td>
<td></td>
</tr>
<tr>
<td>error</td>
<td>Error conditions. Recoverable failure of a component.</td>
<td></td>
</tr>
<tr>
<td>warning</td>
<td>Minor failure, e.g. misconfiguration of a component.</td>
<td></td>
</tr>
<tr>
<td>notice</td>
<td>Normal but significant conditions.</td>
<td></td>
</tr>
<tr>
<td>informational</td>
<td>Informational messages.</td>
<td></td>
</tr>
<tr>
<td>debug</td>
<td>Debug-level messages.</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>Same as emergency</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Same as alert</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Same as critical</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Same as error</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Same as warning</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Same as notice</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Same as informational</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Same as debug</td>
<td></td>
</tr>
</tbody>
</table>

42.2 show

Display device options and settings.

42.2.1 show logging snmp

Display the SNMP logging settings.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show logging snmp
43 Secure Shell (SSH)

43.1 ssh
Set SSH parameters.

43.1.1 ssh server
Enable or disable the SSH server.
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Administrator
  ▶ Format: ssh server

  no ssh server
  Disable the option
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Administrator
  ▶ Format: no ssh server

43.1.2 ssh timeout
Set the SSH connection idle timeout in minutes (default: 5).
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Administrator
  ▶ Format: ssh timeout <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0.160</td>
<td>Idle timeout of a session in minutes (default: 5).</td>
</tr>
</tbody>
</table>

43.1.3 ssh port
Set the SSH server port number (default: 22).
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Administrator
  ▶ Format: ssh port <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1.65535</td>
<td>Port number of the SSH server (default: 22).</td>
</tr>
</tbody>
</table>

43.1.4 ssh max-sessions
Set the maximum number of concurrent SSH sessions (default: 5).
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Administrator
  ▶ Format: ssh max-sessions <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1.5</td>
<td>Maximum number of concurrent SSH sessions.</td>
</tr>
</tbody>
</table>

43.1.5 ssh key rsa
Generate or delete RSA key
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Administrator
  ▶ Format: ssh key rsa <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>generate</td>
<td>Generates the item</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td>Deletes the item</td>
</tr>
</tbody>
</table>

43.1.6 ssh key fingerprint-type
Configure fingerprint type
  ▶ Mode: Global Config Mode
  ▶ Privilege Level: Administrator
  ▶ Format: ssh key fingerprint-type <P-1>
Secure Shell (SSH)

43.2 copy

Copy different kinds of items.

**43.2.1 copy sshkey remote**

Copy the SSH key from a server to the specified destination.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `copy sshkey remote <P-1> nvm`

nvm: Copy the SSH key from a server to non-volatile memory.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>md5</td>
<td>Configure md5 fingerprint of the existing SSH host key</td>
</tr>
<tr>
<td></td>
<td>sha256</td>
<td>Configure sha256 fingerprint of the existing SSH host key</td>
</tr>
</tbody>
</table>

**43.2.2 copy sshkey envm**

Copy the SSH key from external non-volatile memory to the specified destination.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Administrator
- **Format:** `copy sshkey envm <P-1> nvm`

nvm: Copy the SSH key from external non-volatile memory to non-volatile memory.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters</td>
</tr>
</tbody>
</table>

**43.3 show**

Display device options and settings.

**43.3.1 show ssh**

Display the SSH server and client information.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show ssh`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters</td>
</tr>
</tbody>
</table>
44 Storm Control

44.1 storm-control
Configure the global storm-control settings.

44.1.1 storm-control flow-control
Enable or disable flow control globally.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: storm-control flow-control

no storm-control flow-control
Disable the option
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: no storm-control flow-control

44.2 storm-control
Storm control commands

44.2.1 storm-control flow-control
Enable or disable flow control (802.3x) for this port.
- Mode: Interface Range Mode
- Privilege Level: Operator
- Format: storm-control flow-control

no storm-control flow-control
Disable the option
- Mode: Interface Range Mode
- Privilege Level: Operator
- Format: no storm-control flow-control

44.2.2 storm-control ingress unit
Set unit.
- Mode: Interface Range Mode
- Privilege Level: Operator
- Format: storm-control ingress unit <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>percent</td>
<td>Metering unit expressed in percentage of bandwidth.</td>
</tr>
<tr>
<td></td>
<td>pps</td>
<td>Metering unit expressed in packets per second.</td>
</tr>
</tbody>
</table>

44.2.3 storm-control ingress unicast operation
Enable/disable ingress storm control for unicast frames with unknown destination.
- Mode: Interface Range Mode
- Privilege Level: Operator
- Format: storm-control ingress unicast operation

no storm-control ingress unicast operation
Disable the option
- Mode: Interface Range Mode
- Privilege Level: Operator
- Format: no storm-control ingress unicast operation
44.2.4 storm-control ingress unicast threshold
Set the threshold value for unicast frames with unknown destination.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `storm-control ingress unicast threshold <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..14880000</td>
<td>Enter a number in the given range. If the configured unit is percent enter a number in (0..100) range.</td>
</tr>
</tbody>
</table>

44.2.5 storm-control ingress multicast operation
Enable/disable ingress storm control for multicast frames.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `storm-control ingress multicast operation`

- **no storm-control ingress multicast operation**
  Disable the option
  - **Mode:** Interface Range Mode
  - **Privilege Level:** Operator
  - **Format:** `no storm-control ingress multicast operation`

44.2.6 storm-control ingress multicast threshold
Set the threshold value for multicast frames.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `storm-control ingress multicast threshold <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..14880000</td>
<td>Enter a number in the given range. If the configured unit is percent enter a number in (0..100) range.</td>
</tr>
</tbody>
</table>

44.2.7 storm-control ingress broadcast operation
Enable/disable ingress storm control for broadcast frames.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `storm-control ingress broadcast operation`

- **no storm-control ingress broadcast operation**
  Disable the option
  - **Mode:** Interface Range Mode
  - **Privilege Level:** Operator
  - **Format:** `no storm-control ingress broadcast operation`

44.2.8 storm-control ingress broadcast threshold
Set the threshold value for broadcast frames.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `storm-control ingress broadcast threshold <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..14880000</td>
<td>Enter a number in the given range. If the configured unit is percent enter a number in (0..100) range.</td>
</tr>
</tbody>
</table>

44.3 show
Display device options and settings.
44.3.1  **show storm-control flow-control**
Global flow control status.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show storm-control flow-control`

44.3.2  **show storm-control ingress**
Display the storm control ingress parameters.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show storm-control ingress [P-1]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>
45 System

45.1 system

Set system related values e.g. name of the device, location of the device, contact data for the person responsible for the device, and pre-login banner text.

45.1.1 system name

Edit the name of the device. The system name consists of an alphanumeric ASCII character string with 0..255 characters.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** system name <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 255 characters.</td>
</tr>
</tbody>
</table>

45.1.2 system location

Edit the location of the device. The system location consists of an alphanumeric ASCII character string with 0..255 characters.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** system location <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 255 characters.</td>
</tr>
</tbody>
</table>

45.1.3 system contact

Edit the contact information for the person responsible for the device. The contact data consists of an alphanumeric ASCII character string with 0..255 characters.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** system contact <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 255 characters.</td>
</tr>
</tbody>
</table>

45.1.4 system pre-login-banner operation

Enable or disable the pre-login banner. You use the pre-login banner to display a greeting or information to users before they login to the device.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** system pre-login-banner operation

- no system pre-login-banner operation
  
  Disable the option
  
  - **Mode:** Global Config Mode
  - **Privilege Level:** Administrator
  - **Format:** no system pre-login-banner operation

45.1.5 system pre-login-banner text

Edit the text for the pre-login banner (C printf format syntax allowed: \n\t) The device allows you to edit an alphanumeric ASCII character string with up to 512 characters.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** system pre-login-banner text <P>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 512 characters (allowed characters are from ASCII 32 to 127).</td>
</tr>
</tbody>
</table>
45.1.6 system resources operation
Enable or disable the measurement operation.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** system resources operation

```
no system resources operation
```
Disable the option
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** no system resources operation

### 45.2 temperature
Configure the upper and lower temperature limits of the device. The device allows you to set the threshold as an integer from -99 through 99. You configure the temperatures in degrees Celsius.

#### 45.2.1 temperature upper-limit
Configure the upper temperature limit.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** temperature upper-limit <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>-99..99</td>
<td>Upper temperature threshold [(C], default 70).</td>
</tr>
</tbody>
</table>

#### 45.2.2 temperature lower-limit
Configure the lower temperature limit.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** temperature lower-limit <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>-99..99</td>
<td>Lower temperature threshold [(C], default 0).</td>
</tr>
</tbody>
</table>

### 45.3 show
Display device options and settings.

#### 45.3.1 show eventlog
Display the event log notice and warning entries with time stamp.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show eventlog

#### 45.3.2 show system info
Display the system related information.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show system info

#### 45.3.3 show system pre-login-banner
Display the pre-login banner status and text.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show system pre-login-banner
45.3.4  show system flash-status
Display the flash memory statistics of the device.
  Mode: Command is in all modes available.
  Privilege Level: Guest
  Format: show system flash-status

45.3.5  show system temperature limits
Display the temperature limits.
  Mode: Command is in all modes available.
  Privilege Level: Guest
  Format: show system temperature limits

45.3.6  show system temperature extremes
Display the minimum and maximum recorded temperature.
  Mode: Command is in all modes available.
  Privilege Level: Guest
  Format: show system temperature extremes

45.3.7  show system temperature histogram
Display the temperature histogram of the device.
  Mode: Command is in all modes available.
  Privilege Level: Guest
  Format: show system temperature histogram

45.3.8  show system temperature counters
Display number of 20 centigrade C variations in maximum one hour period.
  Mode: Command is in all modes available.
  Privilege Level: Guest
  Format: show system temperature counters

45.3.9  show system resources
Display the system resources information (CPU utilization, memory and network CPU utilization).
  Mode: Command is in all modes available.
  Privilege Level: Guest
  Format: show system resources

45.3.10 show hardware by-pass
Display state of hardware by-pass.
  Mode: Command is in all modes available.
  Privilege Level: Guest
  Format: show hardware by-pass
46 Tracking

46.1 track
Configure tracking instances on the device.

46.1.1 track add
Create a tracking instance.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** track add <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>interface</td>
<td>interface tracking</td>
</tr>
<tr>
<td></td>
<td>ping</td>
<td>ping tracking</td>
</tr>
<tr>
<td></td>
<td>logical</td>
<td>logical tracking</td>
</tr>
<tr>
<td>P-2</td>
<td>1..256</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

46.1.2 track delete
Delete a tracking instance.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** track delete <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>interface</td>
<td>interface tracking</td>
</tr>
<tr>
<td></td>
<td>ping</td>
<td>ping tracking</td>
</tr>
<tr>
<td></td>
<td>logical</td>
<td>logical tracking</td>
</tr>
<tr>
<td>P-2</td>
<td>1..256</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

46.1.3 track enable
Activate a tracking instance.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** track enable <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>interface</td>
<td>interface tracking</td>
</tr>
<tr>
<td></td>
<td>ping</td>
<td>ping tracking</td>
</tr>
<tr>
<td></td>
<td>logical</td>
<td>logical tracking</td>
</tr>
<tr>
<td>P-2</td>
<td>1..256</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

46.1.4 track disable
Deactivate a tracking instance.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** track disable <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>interface</td>
<td>interface tracking</td>
</tr>
<tr>
<td></td>
<td>ping</td>
<td>ping tracking</td>
</tr>
<tr>
<td></td>
<td>logical</td>
<td>logical tracking</td>
</tr>
<tr>
<td>P-2</td>
<td>1..256</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

46.1.5 track trap
Enable / Disable the StateChange trap for the corresponding tracking instance.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** track trap <P-1> <P-2>
46.1.6 track description

Set the description for the corresponding tracking instance.

Mode: Global Config Mode
Privilege Level: Operator
Format: track description <P-1> <P-2> <P-3>

Parameter | Value | Meaning
--- | --- | ---
P-1 | interface | interface tracking
ping | ping tracking
logical | logical tracking
P-2 | 1..256 | Enter a number in the given range.
P-3 | string | Enter a user-defined text, max. 255 characters.

46.1.7 track modify interface

Modify the configuration of an interface tracking instance.

Mode: Global Config Mode
Privilege Level: Operator
Format: track modify interface <P-1> [interface <P-2>] [linkup-delay <P-3>] [linkdown-delay <P-4>]

interface: Set the interface number of the interface tracking instance.
linkup-delay: Set the linkup-delay of the interface tracking instance.
linkdown-delay: Set the linkdown-delay of the interface tracking instance.

Parameter | Value | Meaning
--- | --- | ---
P-1 | slot no./port no. | 
P-2 | slot no./port no. | 
P-3 | 0..255 | Enter a number in the given range.
P-4 | 0..255 | Enter a number in the given range.

46.1.8 track modify ping

Modify the configuration of a ping tracking instance.

Mode: Global Config Mode
Privilege Level: Operator
Format: track modify ping <P-1> <P-2> [interface <P-3>] [address <P-4>] [interval <P-5>] [success <P-6>] [timeout <P-7>] [ttl <P-8>]

interface: Set the source interface number of the ping tracking instance.
address: Set the address of the router to be monitored.
interval: Set the number of milliseconds between the pings to the target router address.
miss: Set the number of consecutive ping misses until the tracked object is considered to be down.
success: Set the number of consecutive ping successes until the tracked object is considered to be up.
timeout: Set the timeout in milliseconds for a ping reply.
ttl: Set the time to live for a ping request packet.

Parameter | Value | Meaning
--- | --- | ---
P-1 | slot no./port no. | 
P-2 | slot no./port no. | 
P-3 | a.b.c.d | IP address.
P-4 | 100..20000 | value for ping tracking interval range between 100 and 20000.
P-5 | 1..10 | value for ping tracking interval range between 1 and 10.
P-6 | 1..10 | value for ping tracking range between 1 and 10.
P-7 | 10..10000 | value for ping tracking time range between 10 and 10000.
P-8 | 1..255 | Enter a number in the given range.
46.1.9  track modify logical
Modify the configuration of a logical tracking instance.
▶ Mode: Global Config Mode
▶ Privilege Level: Operator
▶ Format: track modify logical <P-1> <P-2> <P-3> <P-4>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Track instance.</td>
</tr>
<tr>
<td>P-3</td>
<td>and</td>
<td>AND operator</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td>OR operator</td>
</tr>
<tr>
<td>P-4</td>
<td>string</td>
<td>Track instance.</td>
</tr>
</tbody>
</table>

46.2  show
Display device options and settings.

46.2.1  show track overview
Display the information and settings for the tracking instances.
▶ Mode: Command is in all modes available.
▶ Privilege Level: Guest
▶ Format: show track overview

46.2.2  show track interface
Display the information and settings for the interface tracking instances.
▶ Mode: Command is in all modes available.
▶ Privilege Level: Guest
▶ Format: show track interface [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

46.2.3  show track ping
Display the information and settings for the ping tracking instances.
▶ Mode: Command is in all modes available.
▶ Privilege Level: Guest
▶ Format: show track ping [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

46.2.4  show track logical
Display the information and settings for the logical tracking instances.
▶ Mode: Command is in all modes available.
▶ Privilege Level: Guest
▶ Format: show track logical [<P-1>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

46.2.5  show track application
Display the information on tracking application registrations.
▶ Mode: Command is in all modes available.
▶ Privilege Level: Guest
▶ Format: show track application
## 47 L3 Relay

### 47.1 ip

Set IP parameters.

#### 47.1.1 ip udp-helper operation

Enable or disable the IP helper and DHCP relay.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip udp-helper operation

```bash
no ip udp-helper operation
```

Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** no ip udp-helper operation

#### 47.1.2 ip udp-helper server add

Add a global relay agent to process DHCP client requests and UDP broadcast packets received on any interface.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip udp-helper server add <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>67_hmcliList_IpHelperUdpPorts</td>
<td>DHCP server port number.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

#### 47.1.3 ip udp-helper server delete

Delete a global relay agent.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip udp-helper server delete <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>67_hmcliList_IpHelperUdpPorts</td>
<td>DHCP server port number.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

#### 47.1.4 ip udp-helper server enable

Enable a global relay agent to process DHCP client requests and UDP broadcast packets received on any interface.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip udp-helper server enable <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>67_hmcliList_IpHelperUdpPorts</td>
<td>DHCP server port number.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

#### 47.1.5 ip udp-helper server disable

Disable a global relay agent from processing DHCP client requests and UDP broadcast packets received on any interface.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip udp-helper server disable <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>67_hmcliList_IpHelperUdpPorts</td>
<td>DHCP server port number.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>
47.1.6 ip udp-helper maxhopcount
Configure the DHCP relay maximum hop count.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip udp-helper maxhopcount <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..16</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

47.1.7 ip udp-helper minwaittime
Configure DHCP relay minimum wait time in seconds.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip udp-helper minwaittime <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..100</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

47.1.8 ip udp-helper cidoptmode
Enable or disable DHCP relay circuit id option mode.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip udp-helper cidoptmode

- **no ip udp-helper cidoptmode**
  - Disable the option
  - **Mode:** Global Config Mode
  - **Privilege Level:** Operator
  - **Format:** no ip udp-helper cidoptmode

47.2 ip
IP interface commands.

47.2.1 ip udp-helper server add
Add a relay agent to process DHCP client requests and UDP broadcast packets received on a specific interface.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** ip udp-helper server add <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>67_hmcliList_ipHelpersDHCP server port number. rUdpPorts</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

47.2.2 ip udp-helper server delete
Delete a relay agent from a specific interface.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** ip udp-helper server delete <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>67_hmcliList_ipHelpersDHCP server port number. rUdpPorts</td>
<td></td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>
47.2.3  **ip udp-helper server enable**

Enable a relay agent to process DHCP client requests and UDP broadcast packets received on a specific interface.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip udp-helper server enable <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>67_hmcliList_IpHelperUdpPorts</td>
<td>DHCP server port number.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

47.2.4  **ip udp-helper server disable**

Disable a relay agent from processing DHCP client requests and UDP broadcast packets received on a specific interface.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip udp-helper server disable <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>67_hmcliList_IpHelperUdpPorts</td>
<td>DHCP server port number.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

47.3  **show**

Display device options and settings.

47.3.1  **show ip udp-helper status**

Display the IP helper and DHCP relay status information.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show ip udp-helper status`

47.3.2  **show ip udp-helper global**

Display the DHCP and UDP relays defined globally.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show ip udp-helper global`

47.3.3  **show ip udp-helper interface**

Display the DHCP and UDP relays defined for specific interfaces.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show ip udp-helper interface [<P-1>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

47.3.4  **show ip udp-helper statistics**

Display the IP helper and DHCP relay statistics.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** `show ip udp-helper statistics`

47.4  **clear**

Clear several items.
47.4.1 clear ip udp-helper
Reset IP helper and DHCP relay statistics.

- **Mode:** Privileged Exec Mode
- **Privilege Level:** Operator
- **Format:** clear ip udp-helper
48 Traps

48.1 snmp
Configure of SNMP versions and traps.

48.1.1 snmp trap operation
Global enable/disable SNMP trap.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `snmp trap operation`

**no snmp trap operation**
Disable the option
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `no snmp trap operation`

48.1.2 snmp trap mode
Enable/disable SNMP trap entry.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `snmp trap mode <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;name&gt; Trap name (1 to 32 characters)</td>
</tr>
</tbody>
</table>

**no snmp trap mode**
Disable the option
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `no snmp trap mode <P-1>`

48.1.3 snmp trap delete
Delete SNMP trap entry.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `snmp trap delete <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;name&gt; Trap name (1 to 32 characters)</td>
</tr>
</tbody>
</table>

48.1.4 snmp trap add
Add SNMP trap entry.
- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `snmp trap add <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;name&gt; Trap name (1 to 32 characters)</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>a.b.c.d Single IP address.</td>
</tr>
<tr>
<td></td>
<td>a.b.c.d:n</td>
<td>a.b.c.d:n Address with port.</td>
</tr>
</tbody>
</table>

48.2 show
Display device options and settings.
48.2.1 show snmp traps
Display the SNMP traps.
► **Mode:** Command is in all modes available.
► **Privilege Level:** Guest
► **Format:** show snmp traps
49 Unicast Routing

49.1 routing
Create routing on VLAN.

49.1.1 routing add
Enable routing on VLAN
- Mode: VLAN Database Mode
- Privilege Level: Operator
- Format: routing add <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
</tbody>
</table>

49.1.2 routing delete
Disable routing on VLAN
- Mode: VLAN Database Mode
- Privilege Level: Operator
- Format: routing delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
</tbody>
</table>

49.2 ip
Set IP parameters.

49.2.1 ip routing
Enables or disables Routing globally on the device.
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip routing

- no ip routing
  Disable the option
  - Mode: Global Config Mode
  - Privilege Level: Operator
  - Format: no ip routing

49.2.2 ip proxy-arp max-delay
Configure the maximum time a Proxy ARP response can be delayed
- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip proxy-arp max-delay <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..1000</td>
<td>Enter Proxy ARP max response delay ms</td>
</tr>
</tbody>
</table>

49.3 show
Display device options and settings.
49.3.1 **show ip global**
Display the summary information of the IP, including the ICMP rate limit configuration and the global ICMP Redirect configuration.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip global

49.4 **show**
Display device options and settings.

49.4.1 **show ip interface**
Display the interface parameters.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip interface [P-1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

49.4.2 **show ip statistics**
Display the global IP statistics.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip statistics

49.5 **ip**
IP interface commands.

49.5.1 **ip routing**
This command enables/disables routing for an interface.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** ip routing

```
no ip routing
```
Disable the option
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** no ip routing

49.5.2 **ip proxy-arp operation**
Enables or disables Proxy ARP on the interface.
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** ip proxy-arp operation

```
no ip proxy-arp operation
```
Disable the option
- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** no ip proxy-arp operation
49.5.3  **ip address secondary**
Designates whether an IP Address is a secondary address on this interface.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip address secondary <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>IP subnet mask.</td>
</tr>
</tbody>
</table>

- **no ip address secondary**
  Disable the option
  - **Mode:** Interface Range Mode
  - **Privilege Level:** Operator
  - **Format:** `no ip address secondary <P-1>`

49.5.4  **ip address primary**
Designates whether an IP Address is a primary address on this interface.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip address primary <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-2</td>
<td>a.b.c.d</td>
<td>IP subnet mask.</td>
</tr>
</tbody>
</table>

- **no ip address primary**
  Disable the option
  - **Mode:** Interface Range Mode
  - **Privilege Level:** Operator
  - **Format:** `no ip address primary`

49.5.5  **ip mtu**
Set MTU size for IP protocol

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip mtu <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>68..12266</td>
<td>Set the MTU value.</td>
</tr>
</tbody>
</table>

49.5.6  **ip icmp redirects**
Enables or disables the generation of ICMP Redirect messages.

- **Mode:** Interface Range Mode
- **Privilege Level:** Operator
- **Format:** `ip icmp redirects`

- **no ip icmp redirects**
  Disable the option
  - **Mode:** Interface Range Mode
  - **Privilege Level:** Operator
  - **Format:** `no ip icmp redirects`

49.6  **ip**
Set IP parameters.
49.6.1  ip route add
Add a static route entry.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `ip route add <P-1> <P-2> <P-3> [preference <P-4>]`
  - `[preference]: Change the preference value of a route.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IPv4 address.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IPv4 netmask address.</td>
</tr>
<tr>
<td>P-3</td>
<td>A.B.C.D</td>
<td>Next hop IP address.</td>
</tr>
<tr>
<td>P-4</td>
<td>1..255</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

49.6.2  ip route modify
Modify a static route entry.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `ip route modify <P-1> <P-2> <P-3> [preference <P-4>]`
  - `[preference]: Change the preference value of a route.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IPv4 address.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IPv4 netmask address.</td>
</tr>
<tr>
<td>P-3</td>
<td>A.B.C.D</td>
<td>Next hop IP address.</td>
</tr>
<tr>
<td>P-4</td>
<td>1..255</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

49.6.3  ip route delete
Delete a static route entry.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `ip route delete <P-1> <P-2> <P-3>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IPv4 address.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IPv4 netmask address.</td>
</tr>
<tr>
<td>P-3</td>
<td>A.B.C.D</td>
<td>Next hop IP address.</td>
</tr>
</tbody>
</table>

49.6.4  ip route distance
Default preference for static routes.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `ip route distance <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..255</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

49.6.5  ip route track add
Add a track-id for a static route entry.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `ip route track add <P-1> <P-2> <P-3> <P-4>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IPv4 address.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IPv4 netmask address.</td>
</tr>
<tr>
<td>P-3</td>
<td>A.B.C.D</td>
<td>Next hop IP address.</td>
</tr>
<tr>
<td>P-4</td>
<td>string</td>
<td>Track instance.</td>
</tr>
</tbody>
</table>

49.6.6  ip route track delete
Remove a track-id for a static route entry.

- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** `ip route track delete <P-1> <P-2> <P-3>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IPv4 address.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IPv4 netmask address.</td>
</tr>
</tbody>
</table>
Unicast Routing

49.6 ip

49.6.7 ip default-route add
Add a static default route entry.

- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip default-route add <P-1> [preference <P-2>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..255</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

49.6.8 ip default-route modify
Modify a static default route entry.

- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip default-route modify <P-1> preference <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..255</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

49.6.9 ip default-route delete
Delete a static default route entry.

- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip default-route delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

49.6.10 ip default-route track add
Add a track-id for a static route entry.

- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip default-route track add <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Track instance.</td>
</tr>
</tbody>
</table>

49.6.11 ip default-route track delete
Remove a track-id for a static route entry.

- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip default-route track delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>

49.6.12 ip loopback add
Enable a loopback interface.

- Mode: Global Config Mode
- Privilege Level: Operator
- Format: ip loopback add <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..8</td>
<td>Enter the loopback id in the given range.</td>
</tr>
</tbody>
</table>
49.6.13 ip loopback delete
Disable a loopback interface.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip loopback delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..8</td>
<td>Enter the loopback id in the given range.</td>
</tr>
</tbody>
</table>

49.6.14 ip icmp redirects
Enables or disables the generation of ICMP Redirect messages.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip icmp redirects

**no ip icmp redirects**
Disable the option
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** no ip icmp redirects

49.6.15 ip icmp echo-reply
Enables or disables the generation of ICMP Echo Reply messages.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip icmp echo-reply

**no ip icmp echo-reply**
Disable the option
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** no ip icmp echo-reply

49.6.16 ip icmp rate-limit interval
Configure ICMP rate limit interval in milliseconds.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip icmp rate-limit interval <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..2147483647</td>
<td>configure the interval.</td>
</tr>
</tbody>
</table>

49.6.17 ip icmp rate-limit burst-size
Configure ICMP rate limit burst size.
- **Mode:** Global Config Mode
- **Privilege Level:** Operator
- **Format:** ip icmp rate-limit burst-size <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..200</td>
<td>configure the burst-size.</td>
</tr>
</tbody>
</table>

49.7 show
Display device options and settings.

49.7.1 show ip route all
Display the static, dynamic and local routes.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ip route all
49.7.2  show ip route local
Display the local routes.
► **Mode:** Command is in all modes available.
► **Privilege Level:** Guest
► **Format:** show ip route local

49.7.3  show ip route static
Display the static routes.
► **Mode:** Command is in all modes available.
► **Privilege Level:** Guest
► **Format:** show ip route static

49.7.4  show ip route entry
Display the router route entry information.
► **Mode:** Command is in all modes available.
► **Privilege Level:** Guest
► **Format:** show ip route entry <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IPv4 address.</td>
</tr>
<tr>
<td>P-2</td>
<td>A.B.C.D</td>
<td>IPv4 netmask address.</td>
</tr>
</tbody>
</table>

49.7.5  show ip route tracking
Display the tracking information for static routes.
► **Mode:** Command is in all modes available.
► **Privilege Level:** Guest
► **Format:** show ip route tracking

49.7.6  show ip entry
Display the router route entry information.
► **Mode:** Command is in all modes available.
► **Privilege Level:** Guest
► **Format:** show ip entry <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>A.B.C.D</td>
<td>IP address.</td>
</tr>
</tbody>
</table>
50 Users

50.1 users

Manage Users and User Accounts.

50.1.1 users add
Add a new user.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: users add <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;user&gt; User name (up to 32 characters).</td>
</tr>
</tbody>
</table>

50.1.2 users delete
Delete an existing user.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: users delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;user&gt; User name (up to 32 characters).</td>
</tr>
</tbody>
</table>

50.1.3 users enable
Enable user.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: users enable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;user&gt; User name (up to 32 characters).</td>
</tr>
</tbody>
</table>

50.1.4 users disable
Disable user.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: users disable <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;user&gt; User name (up to 32 characters).</td>
</tr>
</tbody>
</table>

50.1.5 users password
Change user password.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: users password <P-1> [<P-2>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;user&gt; User name (up to 32 characters).</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 64 characters.</td>
</tr>
</tbody>
</table>

50.1.6 users snmpv3 authentication
Specify authentication setting for a user.

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: users snmpv3 authentication <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;user&gt; User name (up to 32 characters).</td>
</tr>
<tr>
<td>P-2</td>
<td>md5</td>
<td>MD5 as SNMPv3 user authentication mode.</td>
</tr>
<tr>
<td></td>
<td>sha1</td>
<td>SHA1 as SNMPv3 user authentication mode.</td>
</tr>
</tbody>
</table>
**50.1.7 users snmpv3 encryption**

Specify encryption settings for a user.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `users snmpv3 encryption <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;user&gt; User name (up to 32 characters).</td>
</tr>
<tr>
<td>P-2</td>
<td>none</td>
<td>SNMPv3 encryption method is none.</td>
</tr>
<tr>
<td></td>
<td>des</td>
<td>DES as SNMPv3 encryption method.</td>
</tr>
<tr>
<td></td>
<td>aescfb128</td>
<td>AES-128 as SNMPv3 encryption method.</td>
</tr>
</tbody>
</table>

**50.1.8 users access-role**

Specify snmpv3 access role for a user.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `users access-role <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;user&gt; User name (up to 32 characters).</td>
</tr>
<tr>
<td>P-2</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

**50.1.9 users lock-status**

Set the lockout status of a specified user.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `users lock-status <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;user&gt; User name (up to 32 characters).</td>
</tr>
<tr>
<td>P-2</td>
<td>unlock</td>
<td>Unlock specific user. User can login again.</td>
</tr>
</tbody>
</table>

**50.1.10 users password-policy-check**

Set password policy check option. The device checks the "minimum password length", regardless of the setting for this option.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** `users password-policy-check <P-1> <P-2>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>&lt;user&gt; User name (up to 32 characters).</td>
</tr>
<tr>
<td>P-2</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

**50.2 show**

Display device options and settings.

**50.2.1 show users**

Display the users and user accounts information.

- **Mode:** Command is in all modes available.
- **Privilege Level:** Administrator
- **Format:** `show users`
51 Virtual LAN (VLAN)

51.1 name

51.1.1 name
Assign a name to a VLAN
► Mode: VLAN Database Mode
► Privilege Level: Operator
► Format: name <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 32 characters.</td>
</tr>
</tbody>
</table>

51.2 vlan
Creation and configuration of VLANS.

51.2.1 vlan add
Create a VLAN
► Mode: VLAN Database Mode
► Privilege Level: Operator
► Format: vlan add <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
</tbody>
</table>

51.2.2 vlan delete
Delete a VLAN
► Mode: VLAN Database Mode
► Privilege Level: Operator
► Format: vlan delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4042</td>
<td>Enter the VLAN ID. VLAN ID 1 can not be deleted or created</td>
</tr>
</tbody>
</table>

51.3 vlan
Configure 802.1Q port parameters for VLANs.

51.3.1 vlan acceptframe
Configure how to handle tagged/untagged frames received.
► Mode: Interface Range Mode
► Privilege Level: Operator
► Format: vlan acceptframe <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>all</td>
<td>Untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port.</td>
</tr>
<tr>
<td></td>
<td>vlanonly</td>
<td>Only frames received with a VLAN tag will be forwarded. All other frames will be dropped.</td>
</tr>
</tbody>
</table>

51.3.2 vlan ingressfilter
Enable/Disable application of Ingress Filtering Rules.
► Mode: Interface Range Mode
► Privilege Level: Operator
► Format: vlan ingressfilter
51.3.3 vlan priority

Configure the priority for untagged frames.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..7</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>

51.3.4 vlan pvid

Configure the VLAN id for a specific port.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
</tbody>
</table>

51.3.5 vlan tagging

Enable or disable tagging for a specific VLAN port.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
</tbody>
</table>

51.3.6 vlan participation include

vlan participation to include

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
</tbody>
</table>

51.3.7 vlan participation exclude

vlan participation to exclude

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
</tbody>
</table>

51.3.8 vlan participation auto

vlan participation to auto

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
</tbody>
</table>
51.4 show
Display device options and settings.

51.4.1 show vlan id
Display the configuration of a single specified VLAN.
► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show vlan id <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
</tbody>
</table>

51.4.2 show vlan brief
Display the general VLAN parameters.
► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show vlan brief

51.4.3 show vlan port
Display the VLAN configuration of a single port.
► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show vlan port [P-1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>slot no./port no.</td>
<td></td>
</tr>
</tbody>
</table>

51.4.4 show vlan member current
Display the membership of ports in static VLAN or dynamically created.
► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show vlan member current

51.4.5 show vlan member static
Display the membership of ports in static VLAN.
► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show vlan member static

51.5 network
Configure the inband and outband connectivity.

51.5.1 network management vlan
Configure the management VLAN ID of the switch.
► Mode: Privileged Exec Mode
► Privilege Level: Operator
► Format: network management vlan <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..4042</td>
<td>Enter the VLAN ID.</td>
</tr>
</tbody>
</table>

51.5.2 network management priority dot1p
Configure the management VLAN priority of the switch.
► Mode: Privileged Exec Mode
► Privilege Level: Operator
► Format: network management priority dot1p <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..7</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>
51.5.3 network management priority ip-dscp

Configure the management VLAN ip-dscp priority of the switch.

- **Mode**: Privileged Exec Mode
- **Privilege Level**: Operator
- **Format**: `network management priority ip-dscp <P-1>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>0..63</td>
<td>Enter a number in the given range.</td>
</tr>
</tbody>
</table>
52 Virtual Private Network (VPN)

52.1 ipsec

Configure IPsec VPN settings.

52.1.1 ipsec certificate delete
Delete a certificate uploaded to the device.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ipsec certificate delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..100</td>
<td>Certificate Table Index.</td>
</tr>
</tbody>
</table>

52.1.2 ipsec certificate upload passphrase
Passphrase that will be used to decrypt the next uploaded file, before storing on the device (note: will not be stored after the next upload, no matter if it is used or not!)

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ipsec certificate upload passphrase <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>

52.1.3 ipsec connection add
Add an IPsec VPN connection (use next free index if none submitted).

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ipsec connection add <P-1> [name <P-2>] [name]: IPsec VPN connection name.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>VPN connection index.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
</tbody>
</table>

52.1.4 ipsec connection modify
Modify an IPsec VPN connection (index in connection is mandatory).

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ipsec connection modify <P-1> name <P-2> certificate ca add <P-3> clear local <P-4> [remote <P-5>] [privkey <P-6>] [passphrase <P-7>] debug informational <P-8> not-handled <P-9> access [method <P-10>] [pre-shared-key <P-11>] [local-type <P-12>] [local-id <P-13>] [remote-type <P-14>] [remote-id <P-15>] key-exchange mode [protocol <P-16>] [startup <P-17>] [dpd-timeout <P-18>] [lifetime <P-19>] [exchange-mode <P-20>] [margintime <P-21>] [re-authenticate <P-22>] algorithms [key-agreement <P-23>] [identity <P-24>] [encryption <P-25>] endpoints [local-address <P-26>] [remote-address <P-27>] data-exchange mode [lifetime <P-28>] algorithms [key-agreement <P-29>] [identity <P-30>] [encryption <P-31>]

**name:** IPsec VPN connection name.

**certificate:** Manage certificates for this connection.

**ca:** Set the CA certificate file name(s). Also supports comma-separated chains.

**clear:** Add a CA file name to the current connection.

**local:** Remove all the CA file names added to the current connection.

**remote:** Set the file name of the certificate that will identify the current device.

**[privkey]:** Set the file name of the private key (if it is encrypted and cannot be automatically matched to the certificate).

**[passphrase]:** Set the passphrase to be used with an encrypted private key or PKCS12 encrypted container (warning: will be stored in the config!).

**debug:** IPsec VPN connection additional debugging information to event log.
### Virtual Private Network (VPN)

52.1 ipsec

**informational:** Enable or disable debug of informational messages.

**not-handled:** Enable or disable debug of not handled messages.

**access:** IPsec VPN access.

**[method]:** Authentication method to be used.

**[pre-shared-key]:** Preshared key (passphrase).

**[local-type]:** Type of local peer identifier.

**[local-id]:** Local peer identifier.

**[remote-type]:** Type of remote peer identifier.

**[remote-id]:** Remote peer identifier.

**key-exchange:** Key exchange parameters.

**mode:** Key exchange mode.

**[protocol]:** Version of the key exchange protocol.

**[startup]:** Key exchange at startup.

**[dpd-timeout]:** Dead peer detection timeout.

**[lifetime]:** IKE security association lifetime.

**[exchange-mode]:** IKE exchange mode.

**[margintime]:** IKE and IPsec margintime for re-keying before timeout.

**[re-authenticate]:** Re-authenticate at end of IKE lifetime (IKEv2 only).

**algorithms:** Key exchange algorithms.

**[key-agreement]:** Key agreement algorithm to be used.

**[integrity]:** Integrity (MAC) algorithm to be used in IKEv2.

**[encryption]:** Encryption algorithm to be used.

**endpoints:** IPsec VPN tunnel endpoints.

**[local-address]:** Address of local security gateway.

**[remote-address]:** Address of remote security gateway.

**data-exchange:** Data exchange parameters.

**mode:** Data exchange mode.

**[lifetime]:** Lifetime of IPsec SA.

**algorithms:** Data exchange algorithms.

**[key-agreement]:** Key agreement algorithm to be used.

**[integrity]:** Integrity (MAC) algorithm to be used in IPsec.

**[encryption]:** Algorithm to be used for IPsec payload encryption.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1-256</td>
<td>VPN connection index.</td>
</tr>
<tr>
<td>P-2</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
<tr>
<td>P-3</td>
<td>string</td>
<td>Filename.</td>
</tr>
<tr>
<td>P-4</td>
<td>string</td>
<td>Filename.</td>
</tr>
<tr>
<td>P-5</td>
<td>string</td>
<td>Filename.</td>
</tr>
<tr>
<td>P-6</td>
<td>string</td>
<td>Filename.</td>
</tr>
<tr>
<td>P-7</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
<tr>
<td>P-8</td>
<td>debug_inform</td>
<td>debug informational</td>
</tr>
<tr>
<td>P-9</td>
<td>debug_unhandled</td>
<td>debug unhandled</td>
</tr>
<tr>
<td>P-10</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>psk</td>
<td>Pre-shared key.</td>
</tr>
<tr>
<td></td>
<td>x509rsa</td>
<td>Individual X.509 RSA certificates.</td>
</tr>
<tr>
<td></td>
<td>pkcs12</td>
<td>Single PKCS12 file with all certificates (including CA).</td>
</tr>
<tr>
<td>P-11</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
<tr>
<td>P-12</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>default</td>
<td>Local IPv4 address.</td>
</tr>
<tr>
<td></td>
<td>address</td>
<td>IPv4 address or host name (use from address field).</td>
</tr>
<tr>
<td></td>
<td>id</td>
<td>Use identifier.</td>
</tr>
<tr>
<td>P-13</td>
<td>string</td>
<td>Enter a user-defined text, max. 255 characters.</td>
</tr>
<tr>
<td>P-14</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>any</td>
<td>Not checked.</td>
</tr>
<tr>
<td></td>
<td>address</td>
<td>IPv4 address or host name (use from address field).</td>
</tr>
<tr>
<td></td>
<td>id</td>
<td>Use identifier.</td>
</tr>
<tr>
<td>P-15</td>
<td>string</td>
<td>Enter a user-defined text, max. 255 characters.</td>
</tr>
<tr>
<td>P-16</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>auto</td>
<td>Accept IKEv1/v2 as responder, start with IKEv2 as initiator.</td>
</tr>
<tr>
<td></td>
<td>v1</td>
<td>IKE version 1 (ISAKMP).</td>
</tr>
<tr>
<td></td>
<td>v2</td>
<td>IKE version 2.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Meaning</td>
</tr>
<tr>
<td>-----------</td>
<td>-------</td>
<td>---------</td>
</tr>
<tr>
<td>P-17</td>
<td>initiator</td>
<td>Initiates an IKE at startup.</td>
</tr>
<tr>
<td></td>
<td>responder</td>
<td>Peer starts the IKE initiation.</td>
</tr>
<tr>
<td>P-18</td>
<td>0..86400</td>
<td>Interval between liveness messages in seconds, 0 to disable.</td>
</tr>
<tr>
<td>P-19</td>
<td>300..86400</td>
<td>Lifetime of IKE SA in seconds (Max. 24h).</td>
</tr>
<tr>
<td>P-20</td>
<td>main</td>
<td>Initiates or Accepts main mode only.</td>
</tr>
<tr>
<td></td>
<td>aggressive</td>
<td>Initiates or Accepts aggressive mode.</td>
</tr>
<tr>
<td>P-21</td>
<td>1..1800</td>
<td>Margintime for re-keying before timeout.</td>
</tr>
<tr>
<td>P-22</td>
<td>true</td>
<td>True</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>False</td>
</tr>
<tr>
<td>P-23</td>
<td>any</td>
<td>Accept all algorithms as responder, use default as initiator.</td>
</tr>
<tr>
<td></td>
<td>modp1024</td>
<td>RSA with 1024 bits modulus (DH Group 2).</td>
</tr>
<tr>
<td></td>
<td>modp1536</td>
<td>RSA with 1536 bits modulus (DH Group 5).</td>
</tr>
<tr>
<td></td>
<td>modp2048</td>
<td>RSA with 2048 bits modulus (DH Group 14).</td>
</tr>
<tr>
<td></td>
<td>modp3072</td>
<td>RSA with 3072 bits modulus (DH Group 15).</td>
</tr>
<tr>
<td></td>
<td>modp4096</td>
<td>RSA with 4096 bits modulus (DH Group 16).</td>
</tr>
<tr>
<td></td>
<td>ecp256</td>
<td>NIST Elliptic Curve with 256 bits (DH Group 19).</td>
</tr>
<tr>
<td></td>
<td>ecp384</td>
<td>NIST Elliptic Curve with 384 bits (DH Group 20).</td>
</tr>
<tr>
<td></td>
<td>ecp521</td>
<td>NIST Elliptic Curve with 521 bits (DH Group 21).</td>
</tr>
<tr>
<td>P-24</td>
<td>any</td>
<td>Accept all algorithms as responder, use default as initiator.</td>
</tr>
<tr>
<td></td>
<td>hmacmd5</td>
<td>HMAC-MD5</td>
</tr>
<tr>
<td></td>
<td>hmacsha1</td>
<td>HMAC-SHA1</td>
</tr>
<tr>
<td></td>
<td>hmacsha256</td>
<td>HMAC-SHA256</td>
</tr>
<tr>
<td></td>
<td>hmacsha384</td>
<td>HMAC-SHA384</td>
</tr>
<tr>
<td></td>
<td>hmacsha512</td>
<td>HMAC-SHA512</td>
</tr>
<tr>
<td>P-25</td>
<td>any</td>
<td>Accept all algorithms as responder, use default as initiator.</td>
</tr>
<tr>
<td></td>
<td>des</td>
<td>DES</td>
</tr>
<tr>
<td></td>
<td>des3</td>
<td>Triple-DES</td>
</tr>
<tr>
<td></td>
<td>aes128</td>
<td>AES with 128 key bits.</td>
</tr>
<tr>
<td></td>
<td>aes192</td>
<td>AES with 192 key bits.</td>
</tr>
<tr>
<td></td>
<td>aes256</td>
<td>AES with 256 key bits.</td>
</tr>
<tr>
<td>P-26</td>
<td>any</td>
<td>Use the primary IP address of external interface.</td>
</tr>
<tr>
<td></td>
<td>a.b.c.d</td>
<td>a.b.c.d IP address.</td>
</tr>
<tr>
<td></td>
<td>nu,nu-nu</td>
<td>host.name.domain FQDN</td>
</tr>
<tr>
<td>P-27</td>
<td>any</td>
<td>Use the primary IP address of external interface.</td>
</tr>
<tr>
<td></td>
<td>a.b.c.d</td>
<td>a.b.c.d IP address.</td>
</tr>
<tr>
<td></td>
<td>nu,nu-nu</td>
<td>host.name.domain FQDN</td>
</tr>
<tr>
<td>P-28</td>
<td>300..28800</td>
<td>Lifetime of IPsec SA in seconds (Max. 8h).</td>
</tr>
<tr>
<td>P-29</td>
<td>any</td>
<td>Accept all algorithms as responder, use default as initiator.</td>
</tr>
<tr>
<td></td>
<td>modp1024</td>
<td>RSA with 1024 bits modulus (DH Group 2).</td>
</tr>
<tr>
<td></td>
<td>modp1536</td>
<td>RSA with 1536 bits modulus (DH Group 5).</td>
</tr>
<tr>
<td></td>
<td>modp2048</td>
<td>RSA with 2048 bits modulus (DH Group 14).</td>
</tr>
<tr>
<td></td>
<td>modp3072</td>
<td>RSA with 3072 bits modulus (DH Group 15).</td>
</tr>
<tr>
<td></td>
<td>modp4096</td>
<td>RSA with 4096 bits modulus (DH Group 16).</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td>No perfect forward secrecy.</td>
</tr>
<tr>
<td></td>
<td>ecp256</td>
<td>NIST Elliptic Curve with 256 bits (DH Group 19).</td>
</tr>
<tr>
<td></td>
<td>ecp384</td>
<td>NIST Elliptic Curve with 384 bits (DH Group 20).</td>
</tr>
<tr>
<td></td>
<td>ecp521</td>
<td>NIST Elliptic Curve with 521 bits (DH Group 21).</td>
</tr>
<tr>
<td>P-30</td>
<td>any</td>
<td>Accept all algorithms as responder, use default as initiator.</td>
</tr>
<tr>
<td></td>
<td>hmacmd5</td>
<td>HMAC-MD5</td>
</tr>
<tr>
<td></td>
<td>hmacsha1</td>
<td>HMAC-SHA1</td>
</tr>
<tr>
<td></td>
<td>hmacsha256</td>
<td>HMAC-SHA256</td>
</tr>
<tr>
<td></td>
<td>hmacsha384</td>
<td>HMAC-SHA384</td>
</tr>
<tr>
<td></td>
<td>hmacsha512</td>
<td>HMAC-SHA512</td>
</tr>
</tbody>
</table>
### 52.1 ipsec

**Virtual Private Network (VPN)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-31</td>
<td>any</td>
<td>Accept all algorithms as responder, use default as initiator.</td>
</tr>
<tr>
<td></td>
<td>des</td>
<td>DES</td>
</tr>
<tr>
<td></td>
<td>des3</td>
<td>Triple-DES</td>
</tr>
<tr>
<td></td>
<td>aes128</td>
<td>AES with 128 key bits.</td>
</tr>
<tr>
<td></td>
<td>aes192</td>
<td>AES with 192 key bits.</td>
</tr>
<tr>
<td></td>
<td>aes256</td>
<td>AES with 256 key bits.</td>
</tr>
<tr>
<td></td>
<td>aes128ctr</td>
<td>AES-COUNTER with 128 key bits.</td>
</tr>
<tr>
<td></td>
<td>aes192ctr</td>
<td>AES-COUNTER with 192 key bits.</td>
</tr>
<tr>
<td></td>
<td>aes256ctr</td>
<td>AES-COUNTER with 256 key bits.</td>
</tr>
<tr>
<td></td>
<td>aes128gcm64</td>
<td>AES-GCM with 64 bit ICV with 128 key bits.</td>
</tr>
<tr>
<td></td>
<td>aes128gcm96</td>
<td>AES-GCM with 96 bit ICV with 128 key bits.</td>
</tr>
<tr>
<td></td>
<td>aes128gcm128</td>
<td>AES-GCM with 128 bit ICV with 128 key bits.</td>
</tr>
<tr>
<td></td>
<td>aes192gcm64</td>
<td>AES-GCM with 64 bit ICV with 192 key bits.</td>
</tr>
<tr>
<td></td>
<td>aes192gcm96</td>
<td>AES-GCM with 96 bit ICV with 192 key bits.</td>
</tr>
<tr>
<td></td>
<td>aes192gcm128</td>
<td>AES-GCM with 128 bit ICV with 192 key bits.</td>
</tr>
<tr>
<td></td>
<td>aes256gcm64</td>
<td>AES-GCM with 64 bit ICV with 256 key bits.</td>
</tr>
<tr>
<td></td>
<td>aes256gcm96</td>
<td>AES-GCM with 96 bit ICV with 256 key bits.</td>
</tr>
<tr>
<td></td>
<td>aes256gcm128</td>
<td>AES-GCM with 128 bit ICV with 256 key bits.</td>
</tr>
</tbody>
</table>

#### no ipsec connection modify

Disable the option

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** no ipsec connection modify name certificate ca add clear local [remote] [privkey] [passphrase] debug informational <P-8> not-handled <P-9> access [method] [pre-shared-key] [local-type] [local-id] [remote-type] [remote-id] key-exchange mode [protocol] [startup] [dpd-timeout] [lifetime] [exchange-mode] [margin-time] [re-authenticate] algorithms [key-agreement] [integrity] [encryption] endpoints [local-address] [remote-address] data-exchange mode [lifetime] algorithms [key-agreement] [integrity] [encryption]

#### 52.1.5 ipsec connection status

Enable or disable a IPsec VPN connection (index in connection is mandatory).

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ipsec connection status <P-1> <P-2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>VPN connection index.</td>
</tr>
<tr>
<td>P-2</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>

#### 52.1.6 ipsec connection delete

Delete a IPsec VPN connection (index in connection is mandatory).

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ipsec connection delete <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>VPN connection index.</td>
</tr>
</tbody>
</table>

#### 52.1.7 ipsec traffic-selector

IPsec VPN traffic selectors.

- **Mode:** Global Config Mode
- **Privilege Level:** Administrator
- **Format:** ipsec traffic-selector <P-1> add <P-2> [name <P-3>] delete <P-4> modify <P-5> [name <P-6>] [source-net <P-7>] [source-restriction <P-8>] [dest-net <P-9>] [dest-restriction <P-10>] status <P-11> <P-12>

add: Add new traffic selector.

[name]: Traffic selector ID.
delete: Delete an existing traffic selector.

modify: Modify an existing traffic selector.
Virtual Private Network (VPN)

52.2 show

Display device options and settings.

52.2.1 show ipsec general
General IPsec VPN settings.
► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show ipsec general

52.2.2 show ipsec connections summary
Overview of all configured connections.
► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show ipsec connections summary

52.2.3 show ipsec connections access
IPsec connection access settings.
► Mode: Command is in all modes available.
► Privilege Level: Guest
► Format: show ipsec connections access <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td></td>
<td>Traffic selector ID.</td>
</tr>
<tr>
<td>source-net</td>
<td></td>
<td>Source address for the traffic selector.</td>
</tr>
<tr>
<td>source-restriction</td>
<td></td>
<td>Source restriction for the traffic selector</td>
</tr>
<tr>
<td>dest-net</td>
<td></td>
<td>Destination address for the traffic selector.</td>
</tr>
<tr>
<td>dest-restriction</td>
<td></td>
<td>Destination restriction for the traffic selector.</td>
</tr>
<tr>
<td>status</td>
<td></td>
<td>Enable or disable an existing traffic selector.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>VPN connection index.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..16</td>
<td>Index of the traffic selector (unique inside of a IPsec VPN connection).</td>
</tr>
<tr>
<td>P-3</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
<tr>
<td>P-4</td>
<td>1..16</td>
<td>Index of the traffic selector (unique inside of a IPsec VPN connection).</td>
</tr>
<tr>
<td>P-5</td>
<td>1..16</td>
<td>Index of the traffic selector (unique inside of a IPsec VPN connection).</td>
</tr>
<tr>
<td>P-6</td>
<td>string</td>
<td>Enter a user-defined text, max. 128 characters.</td>
</tr>
<tr>
<td>P-7</td>
<td>a.b.c.d</td>
<td>Single IP address.</td>
</tr>
<tr>
<td></td>
<td>a.b.c.d</td>
<td>Address range in CIDR notation.</td>
</tr>
<tr>
<td>P-8</td>
<td>string</td>
<td>'protocol/port' Traffic selector restriction can be given as string, e.g. tcp/http or can be given as numbers, e.g. 6/80 (=tcp/http) or can be given as numbers, e.g. /53 (=any/53) 'protocol/port' Traffic selector restriction can be given as string, e.g. udp (=udp/any) or can be given as numbers, e.g. 17 (=17(udp)/any) an empty restriction '' means to have no restriction (any/any)</td>
</tr>
<tr>
<td>P-9</td>
<td>a.b.c.d</td>
<td>Single IP address.</td>
</tr>
<tr>
<td></td>
<td>a.b.c.d</td>
<td>Address range in CIDR notation.</td>
</tr>
<tr>
<td>P-10</td>
<td>string</td>
<td>'protocol/port' Traffic selector restriction can be given as string, e.g. tcp/http or can be given as numbers, e.g. 6/80 (=tcp/http) or can be given as numbers, e.g. /53 (=any/53) 'protocol/port' Traffic selector restriction can be given as string, e.g. udp (=udp/any) or can be given as numbers, e.g. 17 (=17(udp)/any) an empty restriction '' means to have no restriction (any/any)</td>
</tr>
<tr>
<td>P-11</td>
<td>1..256</td>
<td>Index of the traffic selector (unique inside of a IPsec VPN connection).</td>
</tr>
<tr>
<td>P-12</td>
<td>enable</td>
<td>Enable the option.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disable the option.</td>
</tr>
</tbody>
</table>
52.2.4 show ipsec connections certificates

IPsec connection certificates.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ipsec connections certificates <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>VPN connection index.</td>
</tr>
</tbody>
</table>

52.2.5 show ipsec connections key-exchange

IPsec connection key exchange settings (IKE).
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ipsec connections key-exchange <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>VPN connection index.</td>
</tr>
</tbody>
</table>

52.2.6 show ipsec connections data-exchange

IPsec connection data exchange settings.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ipsec connections data-exchange <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>VPN connection index.</td>
</tr>
</tbody>
</table>

52.2.7 show ipsec connections status

IPsec connection status.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ipsec connections status <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>VPN connection index.</td>
</tr>
</tbody>
</table>

52.2.8 show ipsec connections tunnels

IPsec connection tunnels.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ipsec connections tunnels <P-1>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>VPN connection index.</td>
</tr>
</tbody>
</table>

52.2.9 show ipsec traffic-selectors

Traffic selectors for a IPsec VPN connection.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Guest
- **Format:** show ipsec traffic-selectors <P-1> [P-2]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..256</td>
<td>VPN connection index.</td>
</tr>
<tr>
<td>P-2</td>
<td>1..16</td>
<td>Index of the traffic selector (unique inside of a IPsec VPN connection).</td>
</tr>
</tbody>
</table>

52.2.10 show ipsec certificate summary

Display a summary of the uploaded certificates and private keys.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Administrator
- **Format:** show ipsec certificate summary

52.2.11 show ipsec certificate details

Display the details about a specific certificate or private key.
- **Mode:** Command is in all modes available.
- **Privilege Level:** Administrator
- **Format:** show ipsec certificate details <P-1>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>1..100</td>
<td>Certificate Table Index.</td>
</tr>
</tbody>
</table>
A  Further support

Technical questions
For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.
You find the addresses of our partners on the Internet at www.hirschmann.com.
A list of local telephone numbers and email addresses for technical support directly from Hirschmann is available at hirschmann-support.belden.com.
This site also includes a free of charge knowledge base and a software download section.

Technical Documents
The current manuals and operating instructions for Hirschmann products are available at doc.hirschmann.com.

Hirschmann Competence Center
The Hirschmann Competence Center is ahead of its competitors on three counts with its complete range of innovative services:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification. You find the training courses on technology and products currently available at www.hicomcenter.com.
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.
B Readers’ Comments

What is your opinion of this manual? We are constantly striving to provide as comprehensive a description of our product as possible, as well as important information to assist you in the operation of this product. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

<table>
<thead>
<tr>
<th></th>
<th>Very Good</th>
<th>Good</th>
<th>Satisfactory</th>
<th>Mediocre</th>
<th>Poor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precise description</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Readability</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Understandability</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Examples</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Structure</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Comprehensive</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Graphics</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Drawings</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Tables</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
</tbody>
</table>

Did you discover any errors in this manual? If so, on what page?

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

Suggestions for improvement and additional information:

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

General comments:

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

Sender:

Company / Department:

Name / Telephone number:
Readers’ Comments
52.2 show

Dear User,
Please fill out and return this page
► as a fax to the number +49 (0)7127/14-1600 or
► per mail to
   Hirschmann Automation and Control GmbH
   Department 01RD-NT
   Stuttgarter Str. 45-51
   72654 Neckartenzlingen