SIEMENS

SIMATIC NET

Industrial Ethernet Security SCALANCE S615 Command Line Interface

Projektierungshandbuch

Vorwort

Security-Empfehlung 1

Allgemeines 2

Allgemeine CLI Befehle 3

Konfiguration 4

SCALANCE spezifische Funktionen 5

Systemzeit 6

Netzstrukturen 7

Netzwerk-Protokolle 8

Lastkontrolle 9

Layer 3-Funktionen 10

Sicherheit und Authentifizierung 11

Diagnose 12

01/2019

C79000-G8900-C406-07

Rechtliche Hinweise

Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

⚠GEFAHR
bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠WARNUNG
bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠VORSICHT
bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

ACHTUNG
bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das zu dieser Dokumentation zugehörige Produkt/System darf nur von für die jeweilige Aufgabenstellung **qualifiziertem Personal** gehandhabt werden unter Beachtung der für die jeweilige Aufgabenstellung zugehörigen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziertes Personal ist auf Grund seiner Ausbildung und Erfahrung befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:

⚠WARNUNG
Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle verwendet werden. Falls Fremdprodukte und -komponenten zum Einsatz kommen, müssen diese von Siemens empfohlen bzw. zugelassen sein. Der einwandfreie und sichere Betrieb der Produkte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Die zulässigen Umgebungsbedingungen müssen eingehalten werden. Hinweise in den zugehörigen Dokumentationen müssen beachtet werden.

Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Siemens AG
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

Dokument-Bestellnummer: C79000-G8900-C406
Ⓟ 01/2019 Änderungen vorbehalten

Copyright © Siemens AG 2015 - 2019.
Alle Rechte vorbehalten

Vorwort

Gültigkeitsbereich des Projektierungshandbuchs

Dieses Projektierungshandbuch behandelt das folgende Produkt:

- SCALANCE S615

Das Projektierungshandbuch gilt für folgende Softwareversion:

- SCALANCE S-615 Firmware ab Version V6.1

Zweck dieses Projektierungshandbuchs

Dieses Projektierungshandbuch enthält die CLI-Befehle, die vom SCALANCE S615 unterstützt werden. Das Dokument finden Sie auf dem mitgelieferten Datenträger.

Einordnung in die Dokumentationslandschaft

Zum Thema Remote Network gibt es außer dem Projektierungshandbuch, das Sie gerade lesen, noch folgende Dokumentationen:

- Projektierungshandbuch SCALANCE S615 Web Based Management

  Dieses Dokument soll Sie in die Lage versetzen, SCALANCE S615-Geräte über das Web Based Management in Betrieb zu nehmen und zu projektieren.

- Getting Started

  Dieses Dokument zeigt anhand von Beispielen die Projektierung des SCALANCE M800/S 615-Geräts.

- Betriebsanleitung SINEMA RC-Server

  Dieses Dokument finden Sie auf den Internetseiten des Siemens Industry Online Support. Es enthält Informationen zur Installation, Konfiguration und Bedienung der Anwendung SINEMA Remote Connect Server.

- IP-basierte Remote Networks

  In diesem Dokument erhalten Sie eine Übersicht über die möglichen Konstellationen eines IP-basierten Remote Networks mit den Voraussetzungen und den Link zur ausführlichen Projektierungsanleitung erläutert.

  Sie finden dieses Dokument im Internet unter folgender Beitrags-ID: 26662448

SIMATIC NET-Handbücher

Die SIMATIC NET-Handbücher finden Sie auf den Internetseiten des Siemens Industry Online Support:

- über die Suchfunktion:

  Link zum Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/de/)

  Geben Sie die Beitrags-ID des jeweiligen Handbuchs als Suchbegriff ein.

- über die Navigation auf der linken Seite im Bereich "Industrielle Kommunikation":

  Link zum Bereich "Industrielle Kommunikation" (https://support.industry.siemens.com/cs/ww/de/ps/15247/pm)

  Navigieren Sie zu der gewünschten Produktgruppe und nehmen Sie folgende Einstellungen vor:
  Register "Beitragsliste", Beitragstyp "Handbücher / Betriebsanleitungen"

Die Dokumente der hier relevanten SIMATIC NET-Produkte finden Sie auch auf dem Datenträger, der manchen Produkten beiliegt:

- Produkt-CD / Produkt-DVD
- SIMATIC NET Manual Collection

Training, Service & Support

Informationen zu Training, Service & Support finden Sie in dem mehrsprachigen Dokument "DC_support_99.pdf", welches sich auf dem mitgelieferten Datenträger mit Dokumentation befindet.

SIMATIC NET-Glossar

Erklärungen zu vielen Fachbegriffen, die in dieser Dokumentation vorkommen, sind im SIMATIC NET-Glossar enthalten.

Sie finden das SIMATIC NET-Glossar im Internet unter folgender Adresse:

50305045 (https://support.industry.siemens.com/cs/ww/de/view/50305045)

Security-Hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen.

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen einen Bestandteil eines solchen Konzepts.

Die Kunden sind dafür verantwortlich, unbefugten Zugriff auf ihre Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Diese Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und nur wenn entsprechende Schutzmaßnahmen (z. B. Firewalls und/oder Netzwerksegmentierung) ergriffen wurden.

Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich Industrial Security finden Sie unter https://www.siemens.com/industrialsecurity.

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Aktualisierungen durchzuführen, sobald die entsprechenden Updates zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter https://www.siemens.com/industrialsecurity.

Firmware

Die Firmware ist signiert und verschlüsselt. Es ist sichergestellt, dass nur von Siemens erstellte Firmware in das Gerät geladen werden kann.

Lizenzbedingungen

Hinweis

Open Source Software

Lesen Sie die Lizenzbedingungen zur Open Source Software genau durch, bevor Sie das Produkt nutzen.

Sie finden die Lizenzbedingungen in folgenden Dokumenten, die sich auf dem mitgelieferten Datenträger befinden:

- M87x, M81x, M826, M804PB, S615: OSS_Scalance-M-800-S615_86.pdf

Marken

Folgende und eventuell weitere nicht mit dem Schutzrechtsvermerk ® gekennzeichnete Bezeichnungen sind eingetragene Marken der Siemens AG:

SCALANCE, SINEMA, KEY-PLUG, C-PLUG

Inhaltsverzeichnis

Vorwort 3

1 Security-Empfehlung 25

2 Allgemeines 31

2.1 Nicht unterstützte Features 31

2.2 Mengengerüste für WBM und CLI 32

2.3 Einsatz in einer PROFINET-Umgebung 34

2.4 CLI-Modi 35

2.5 Mit Command Line Interface (CLI) arbeiten 37

2.6 Die CLI-Eingabeaufforderung (Der Prompt) 39

2.7 Symbolik der CLI Befehle 40

2.8 Schnittstellenbezeichnungen und Adressen 42
2.8.1 Bezeichnung von Schnittstellen 42
2.8.2 Adresstypen, Adressbereiche und Adressmasken 44
2.8.3 IPv4-Adresse 45

3 Allgemeine CLI Befehle 47

3.1 clear screen 47

3.2 do 48

3.3 end 49

3.4 exit 50

3.5 Hilfefunktionen und unterstützte Eingabe 50
3.5.1 help 51
3.5.2 Der Befehl "?" 52
3.5.3 Befehl "grep" 53
3.5.4 Ergänzung von Befehlseingaben 53
3.5.5 Verkürzte Schreibweise von Befehlen 54
3.5.6 Wiederverwenden der zuletzt verwendeten Befehle 54
3.5.7 Abarbeiten einer Befehlsfolge 55
3.5.8 clear history 56
3.5.9 Die "show"-Befehle 56
3.5.9.1 show history 57

4 Konfiguration 59

4.1 System 59
4.1.1 Die "show"-Befehle 59
4.1.1.1 show cli-console-timeout 59
4.1.1.2 show coordinates 60
4.1.1.3 show device information 60
4.1.1.4 show interfaces 61

4.1.1.5 show im ... 62
4.1.1.6 show interface mtu ... 63
4.1.1.7 show interfaces ... counters ... 64
4.1.1.8 show lldp neighbors ... 65
4.1.1.9 show lldp status ... 65
4.1.1.10 show ip interface ... 66
4.1.1.11 show versions ... 67
4.1.2 clear counters ... 68
4.1.3 configure terminal ... 69
4.1.4 clear line vty ... 69
4.1.5 disable ... 70
4.1.6 enable ... 71
4.1.7 logout ... 71
4.1.8 ping ... 72
4.1.9 Befehle im globalen Konfigurationsmodus ... 73
4.1.9.1 coordinates height ... 73
4.1.9.2 coordinates latitude ... 74
4.1.9.3 coordinates longitude ... 75
4.1.9.4 interface ... 76
4.1.9.5 no interface ... 77
4.1.9.6 cli-console-timeout ... 78
4.1.9.7 no cli-console-timeout ... 79
4.1.9.8 system contact ... 80
4.1.9.9 system location ... 80
4.1.9.10 system name ... 81
4.1.10 Befehle im Interface-Konfigurationsmodus ... 82
4.1.10.1 alias ... 82
4.1.10.2 no alias ... 83
4.1.10.3 duplex ... 83
4.1.10.4 no duplex ... 84
4.1.10.5 lldp ... 85
4.1.10.6 no lldp ... 86
4.1.10.7 negotiation ... 87
4.1.10.8 no negotiation ... 88
4.1.10.9 shutdown complete ... 88
4.1.10.10 no shutdown ... 89
4.1.10.11 speed ... 90

4.2 Load and Save ... 91
4.2.1 Die "show"-Befehle ... 91
4.2.1.1 show loadsave files ... 91
4.2.1.2 show loadsave tftp ... 92
4.2.1.3 show loadsave sftp ... 92
4.2.2 load tftp ... 93
4.2.3 save filetype ... 94
4.2.4 Befehle im globalen Konfigurationsmodus ... 95
4.2.4.1 loadsave ... 95
4.2.5 Befehle im LOADSAVE Konfigurationsmodus ... 96
4.2.5.1 delete ... 96
4.2.5.2 tftp filename ... 97
4.2.5.3 tftp load ... 98
4.2.5.4 tftp save ... 99
4.2.5.5 tftp server ... 100

4.2.5.6 sftp filename 100
4.2.5.7 sftp load 101
4.2.5.8 sftp save 102
4.2.5.9 sftp server 103
4.2.5.10 password 104
4.2.5.11 no password 106

4.3 Reset and Defaults 107
4.3.1 restart 107

4.4 Configuration Save & Restore 109
4.4.1 Die "show"-Befehle 109
4.4.1.1 show running-config 109
4.4.2 write startup-config 111
4.4.3 Befehle im globalen Konfigurationsmodus 112
4.4.3.1 auto-save 112
4.4.3.2 no auto-save 113

4.5 DCP Discovery 114
4.5.1 Die "show"-Befehle 114
4.5.1.1 show das info 114
4.5.2 Befehle im globalen Konfigurationsmodus 115
4.5.2.1 das discover interface 115
4.5.2.2 das mac name 116
4.5.2.3 das mac ip 117
4.5.2.4 das mac blink 118
4.5.2.5 das delete 119

4.6 SINEMA 120
4.6.1 Die "show"-Befehle 120
4.6.1.1 show sinema 120
4.6.2 Befehle im globalen Konfigurationsmodus 121
4.6.2.1 sinema 121
4.6.2.2 no sinema 122

5 SCALANCE spezifische Funktionen 123

5.1 PLUG 123
5.1.1 Die "show"-Befehle 123
5.1.1.1 show plug 123
5.1.2 Befehle im globalen Konfigurationsmodus 124
5.1.2.1 plug 124
5.1.3 Befehle im Plug Konfigurationsmodus 125
5.1.3.1 presetplug 125
5.1.3.2 firmware-on-plug 126
5.1.3.3 no firmware-on-plug 127
5.1.3.4 factoryclean 127
5.1.3.5 write 128

5.2 WBM 129
5.2.1 Die "show"-Befehle 129
5.2.1.1 show web-session-timeout 129
5.2.2 Befehle im globalen Konfigurationsmodus 130
5.2.2.1 web-session-timeout 130
5.2.2.2 no web-session-timeout 131

5.3 Digital Input/Output ... 132
5.3.1 Die "show"-Befehle ... 132
5.3.1.1 show digital input ... 132
5.3.1.2 show digital output ... 133
5.3.2 Befehle im globalen Konfigurationsmodus ... 133
5.3.2.1 digital output closed ... 134
5.3.2.2 digital output open ... 135

5.4 cRSP / SRS ... 136
5.4.1 Die "show"-Befehle ... 136
5.4.1.1 show srs ... 136
5.4.1.2 show srs logon ... 137
5.4.2 Befehle im globalen Konfigurationsmodus ... 137
5.4.2.1 srs ... 137
5.4.3 Befehle im SRS-Konfigurationsmodus ... 138
5.4.3.1 logon ... 139
5.4.3.2 no logon ... 139
5.4.3.3 logon idx authority ... 140
5.4.3.4 logon idx fragment ... 141
5.4.3.5 logon idx path ... 142
5.4.3.6 logon idx query ... 142
5.4.3.7 logon show-idx ... 143
5.4.3.8 shutdown ... 144
5.4.3.9 no shutdown ... 144
5.4.3.10 interval ... 145
5.4.3.11 validate cert ... 146

5.5 SINEMA RC ... 147
5.5.1 Einleitung zum Kapitel SRC ... 147
5.5.2 Die "show"-Befehle ... 147
5.5.2.1 show sinemarc ... 147
5.5.3 Befehle im globalen Konfigurationsmodus ... 148
5.5.3.1 sinemarc ... 148
5.5.4 Befehl im SINEMARC-Konfigurationsmodus ... 149
5.5.4.1 addr ... 149
5.5.4.2 autoenrollment interval ... 150
5.5.4.3 autofwnat ... 151
5.5.4.4 connection type ... 152
5.5.4.5 no autofwnat ... 153
5.5.4.6 device id ... 154
5.5.4.7 device pw ... 155
5.5.4.8 port ... 155
5.5.4.9 proxy ... 156
5.5.4.10 no proxy ... 157
5.5.4.11 shutdown ... 158
5.5.4.12 no shutdown ... 159
5.5.4.13 verification cacert ... 160
5.5.4.14 verification fingerprint ... 161

5.6 SELECT/SET-Taster ... 162
5.6.1 Befehle im globalen Konfigurationsmodus ... 162
5.6.1.1 panel-button control-restart ... 163
5.6.1.2 no panel-button control-restart ... 164

6 Systemzeit 165

6.1 System Time Setting 165
6.1.1 Die "show"-Befehle 165
6.1.1.1 show dst info 165
6.1.1.2 show time 166
6.1.2 Befehle im globalen Konfigurationsmodus 166
6.1.2.1 time 167
6.1.2.2 time dst date 168
6.1.2.3 time dst recurring 169
6.1.2.4 no time dst 170
6.1.2.5 time set 171

6.2 NTP Client 172
6.2.1 Die "show"-Befehle 172
6.2.1.1 show ntp info 172
6.2.2 Befehle im globalen Konfigurationsmodus 173
6.2.2.1 ntp 173
6.2.3 Befehle im NTP Konfigurationsmodus 174
6.2.3.1 ntp server id 174
6.2.3.2 no ntp server id 175
6.2.3.3 ntp server secure 176
6.2.3.4 ntp secure 177
6.2.3.5 no ntp secure 177
6.2.3.6 ntp time diff 178

6.3 NTP-Server 179
6.3.1 show ntp server info 179
6.3.2 Befehle im globalen Konfigurationsmodus 179
6.3.2.1 ntp server 180
6.3.2.2 no ntp server 180
6.3.3 Befehle im NTP Server Konfigurationsmodus 181
6.3.3.1 ntp server interface 181
6.3.3.2 no ntp server interface 183
6.3.3.3 ntp server secure interface 184
6.3.3.4 no ntp server secure interface 185

6.4 SNTP Client 186
6.4.1 Die "show"-Befehle 186
6.4.1.1 show sntp broadcast-mode status 186
6.4.1.2 show sntp status 187
6.4.1.3 show sntp unicast-mode status 187
6.4.2 Befehle im globalen Konfigurationsmodus 188
6.4.2.1 sntp 188
6.4.3 Befehle im SNTP Konfigurationsmodus 189
6.4.3.1 sntp time diff 189
6.4.3.2 sntp unicast-server 190
6.4.3.3 no sntp unicast-server 191
6.4.3.4 sntp client addressing-mode 192

7 Netzstrukturen 195

7.1 VLAN 195
7.1.1 Die "show"-Befehle 195
7.1.1.1 show vlan 195
7.1.1.2 show vlan device info 196
7.1.1.3 show vlan learning params 196
7.1.1.4 show vlan port config 197
7.1.1.5 show vlan protocols-group 198
7.1.2 Befehle im globalen Konfigurationsmodus 199
7.1.2.1 base bridge-mode 199
7.1.2.2 interface range 200
7.1.2.3 no interface range 201
7.1.2.4 map protocol 202
7.1.2.5 no map protocol 203
7.1.2.6 no protocol-vlan 204
7.1.2.7 protocol-vlan 205
7.1.2.8 subnet-vlan 205
7.1.2.9 no subnet-vlan 206
7.1.2.10 vlan 207
7.1.2.11 no vlan 208
7.1.3 Befehle im Interface Konfigurationsmodus 209
7.1.3.1 mtu 209
7.1.3.2 shutdown complete 210
7.1.3.3 no shutdown 210
7.1.3.4 switchport acceptable-frame-type 211
7.1.3.5 no switchport acceptable-frame-type 212
7.1.3.6 switchport ingress-filter 213
7.1.3.7 no switchport ingress-filter 213
7.1.3.8 switchport mode 214
7.1.3.9 no switchport mode 216
7.1.3.10 switchport priority default 216
7.1.3.11 no switchport priority default 217
7.1.3.12 switchport pvid 218
7.1.3.13 no switchport pvid 219
7.1.4 Befehle im VLAN Konfigurationsmodus 220
7.1.4.1 ip address 220
7.1.4.2 no ip address 221
7.1.4.3 name 222
7.1.4.4 no name 223
7.1.4.5 ports 224
7.1.4.6 no ports 225
7.1.4.7 tia interface 227

7.2 PPP 228
7.2.1 Die "show"-Befehle 228
7.2.1.1 show ppp information 228
7.2.2 Befehle im globalen Konfigurationsmodus 228
7.2.2.1 interface ppp 229
7.2.3 Befehle im Interface Konfigurationsmodus 230
7.2.3.1 forced disconnect 230
7.2.3.2 forced disconnect time 231
7.2.3.3 interface vlan 232

7.2.3.4 ip address 233
7.2.3.5 ip address dhcp....233
7.2.3.6 no ip address 234
7.2.3.7 password....235
7.2.3.8 shutdown....236
7.2.3.9 no shutdown....237
7.2.3.10 type ppo-ex 237
7.2.3.11 username 238

7.3 Passive Listening 239
7.3.1 Die "show"-Befehle 239
7.3.1.1 show passive-listening 239
7.3.2 Befehle im globalen Konfigurationsmodus 240
7.3.2.1 passive-listening bpdu-vlan-flood 240
7.3.2.2 no passive-listening bpdu-vlan-flood 241
7.3.2.3 passive-listening 241
7.3.2.4 no passive-listening 242

7.4 Spanning Tree 243
7.4.1 Die "show"-Befehle 243
7.4.1.1 show spanning-tree....243
7.4.1.2 show spanning-tree active 244
7.4.1.3 show spanning-tree bridge 245
7.4.1.4 show spanning-tree detail....246
7.4.1.5 show spanning-tree interface....246
7.4.1.6 show spanning-tree interface layer2-gateway-port....247
7.4.1.7 show spanning-tree root 248
7.4.2 clear spanning-tree detected protocols....249
7.4.3 clear spanning-tree counters 250
7.4.4 Befehle im globalen Konfigurationsmodus 250
7.4.4.1 spanning-tree 251
7.4.4.2 no spanning-tree 251
7.4.4.3 spanning-tree (Zeiteinstellungen) 252
7.4.4.4 no spanning-tree (Zeiteinstellungen) 254
7.4.5 Befehle im Interface Konfigurationsmodus....255
7.4.5.1 spanning-tree 255
7.4.5.2 no spanning-tree 257
7.4.5.3 spanning-tree auto-edge....258
7.4.5.4 no spanning-tree auto-edge....259

8 Netzwerk-Protokolle 261

8.1 Protocol IPv4....261
8.1.1 Die "show"-Befehle 261
8.1.1.1 show ip dns 261
8.1.1.2 show dcp forwarding 262
8.1.1.3 show dcp server....263
8.1.1.4 show ip route....263
8.1.1.5 show ip routing....264
8.1.1.6 show ip static route 264
8.1.1.7 show ip telnet 265
8.1.2 Befehle im globalen Konfigurationsmodus 265
8.1.2.1 dcp server 266
8.1.2.2 no dcp server 267

8.1.2.3 ip echo-reply ... 267
8.1.2.4 no ip echo-reply ... 268
8.1.2.5 ip route ... 269
8.1.2.6 no ip route ... 270
8.1.2.7 ip routing ... 271
8.1.2.8 no ip routing ... 271
8.1.2.9 telnet-server ... 272
8.1.2.10 no telnet-server ... 273
8.1.3 Befehle im Interface Konfigurationsmodus ... 273
8.1.3.1 dcp forwarding ... 274
8.1.3.2 ip address ... 275
8.1.3.3 ip address dhcp ... 276
8.1.3.4 no ip address ... 277

8.2 ARP ... 278
8.2.1 Die "show"-Befehle ... 278
8.2.1.1 show ip arp ... 278

8.3 DHCP-Client ... 280
8.3.1 Die "show"-Befehle ... 280
8.3.1.1 show ip dhcp client ... 280
8.3.2 Befehle im globalen Konfigurationsmodus ... 281
8.3.2.1 ip dhcp config-file-request ... 281
8.3.2.2 no ip dhcp config-file-request ... 282
8.3.2.3 ip dhcp client mode ... 282
8.3.2.4 dhcp duid type ... 283

8.4 DHCP-Server ... 285
8.4.1 Die "show"-Befehle ... 285
8.4.1.1 show ip dhcp-server bindings ... 285
8.4.1.2 show ip dhcp-server pools ... 286
8.4.2 Befehle im globalen Konfigurationsmodus ... 287
8.4.2.1 ip dhcp-server ... 287
8.4.2.2 no ip dhcp-server ... 288
8.4.2.3 no ip dhcp-server icmp-probe ... 288
8.4.2.4 ip dhcp-server icmp-probe ... 289
8.4.2.5 ip dhcp-server pool ... 290
8.4.2.6 no ip dhcp-server pool ... 291
8.4.3 Befehle im DHCPPOOL Konfigurationsmodus ... 292
8.4.3.1 lease-time ... 292
8.4.3.2 network ... 293
8.4.3.3 option (IP-Adresse) ... 294
8.4.3.4 option value-hex ... 295
8.4.3.5 option value-string ... 296
8.4.3.6 no option ... 297
8.4.3.7 pool-enable ... 298
8.4.3.8 no pool-enable ... 299
8.4.3.9 set-interface ... 300
8.4.3.10 static-lease ... 301
8.4.3.11 no static-lease ... 302

8.5 DNS ... 304
8.5.1 Die "show"-Befehle ... 304
8.5.1.1 show dnsclient information ... 304

8.5.1.2 show ddnsclient information 304
8.5.2 Befehle im globalen Konfigurationsmodus 305
8.5.2.1 dnsclient 305
8.5.2.2 dnsproxy 306
8.5.2.3 ddnsclient 306
8.5.3 Befehle im DNS CLIENT-Konfigurationsmodus 307
8.5.3.1 manual srv 307
8.5.3.2 no manual srv 308
8.5.3.3 server type 309
8.5.3.4 shutdown 310
8.5.3.5 no shutdown 310
8.5.4 Befehle im DNS PROXY-Konfigurationsmodus 311
8.5.4.1 cachenxdomain 311
8.5.4.2 no cachenxdomain 312
8.5.4.3 shutdown 313
8.5.4.4 no shutdown 313
8.5.5 Befehle im DDNS Client-Konfigurationsmodus 314
8.5.5.1 service 314
8.5.5.2 no service 315
8.5.5.3 userhost 316
8.5.5.4 username 317
8.5.5.5 password 317

8.6 SNMP 319
8.6.1 Die "show"-Befehle 320
8.6.1.1 show snmp 320
8.6.1.2 show snmp community 320
8.6.1.3 show snmp engineID 321
8.6.1.4 show snmp filter 321
8.6.1.5 show snmp group 322
8.6.1.6 show snmp group access 322
8.6.1.7 show snmp inform statistics 323
8.6.1.8 show snmp notif 323
8.6.1.9 show snmp targetaddr 324
8.6.1.10 show snmp targetparam 324
8.6.1.11 show snmp tcp 325
8.6.1.12 show snmp user 326
8.6.1.13 show snmp viewtree 326
8.6.2 Befehle im globalen Konfigurationsmodus 327
8.6.2.1 snmpagent 327
8.6.2.2 no snmpagent 328
8.6.2.3 snmp agent version 328
8.6.2.4 snmp access 329
8.6.2.5 no snmp access 331
8.6.2.6 snmp community index 332
8.6.2.7 no snmp community index 333
8.6.2.8 snmp filterprofile 334
8.6.2.9 no snmp filterprofile 335
8.6.2.10 snmp group 336
8.6.2.11 no snmp group 337
8.6.2.12 snmp notify 338
8.6.2.13 no snmp notify 339
8.6.2.14 snmp targetaddr 339

8.6.2.15 no snmp targetaddr ... 341
8.6.2.16 snmp targetparams ... 342
8.6.2.17 no snmp targetparams ... 344
8.6.2.18 snmp v1-v2 readonly ... 344
8.6.2.19 no snmp v1-v2 readonly ... 345
8.6.2.20 snmp user ... 346
8.6.2.21 no snmp user ... 347
8.6.2.22 snmp view ... 347
8.6.2.23 no snmp view ... 349

8.7 HTTP-Server ... 350
8.7.1 Die "show"-Befehle ... 350
8.7.1.1 show ip http server status ... 350
8.7.2 Befehle im globalen Konfigurationsmodus ... 350
8.7.2.1 ip http ... 351
8.7.2.2 no ip http ... 351

8.8 HTTPS-Server ... 353
8.8.1 Die "show"-Befehle ... 353
8.8.1.1 show ip http secure server status ... 353
8.8.1.2 show ssl server-cert ... 353
8.8.2 Befehle im globalen Konfigurationsmodus ... 354
8.8.2.1 ip http secure minimum tls-version ... 354
8.8.2.2 ip http https redirection ... 355

8.9 Proxy-Server ... 356
8.9.1 Die "show"-Befehle ... 356
8.9.1.1 show proxyserver table ... 356
8.9.2 Befehle im globalen Konfigurationsmodus ... 356
8.9.2.1 proxyserver ... 357
8.9.3 Befehle im PROXYSERVER-Konfigurationsmodus ... 357
8.9.3.1 srv name ... 358
8.9.3.2 no srv ... 359
8.9.3.3 srv name addr ... 360
8.9.3.4 srv name auth ... 361
8.9.3.5 srv name port ... 362
8.9.3.6 srv name pw ... 363
8.9.3.7 srv name type ... 364
8.9.3.8 srv name user ... 364
8.9.3.9 srv show-names ... 366

8.10 SMTP-Client ... 367
8.10.1 Die "show"-Befehle ... 367
8.10.1.1 show events smtp-server ... 367
8.10.1.2 show events sender email ... 368
8.10.1.3 show events smtp-port ... 368
8.10.2 Befehle im Events Konfigurationsmodus ... 369
8.10.2.1 send test mail ... 369
8.10.2.2 smtp-server ... 370
8.10.2.3 no smtp-server ... 371
8.10.3 Befehle im STMP-Server Konfigurationsmodus ... 372
8.10.3.1 auth username ... 372
8.10.3.2 no auth username ... 373
8.10.3.3 port ... 373

8.10.3.4 no port 374
8.10.3.5 receiver-address 375
8.10.3.6 no receiver-address 375
8.10.3.7 security 376
8.10.3.8 no security 377
8.10.3.9 sender address 378
8.10.3.10 no sender address 378
8.10.3.11 test 379

8.11 SSH-Server 380
8.11.1 Die "show"-Befehle 380
8.11.1.1 show ip ssh 380
8.11.2 Befehle im globalen Konfigurationsmodus 381
8.11.2.1 ssh-server 381
8.11.2.2 no ssh-server 382

9 Lastkontrolle 383

9.1 Flow Control 383
9.1.1 Die "show"-Befehle 383
9.1.1.1 show flow-control 383
9.1.2 Befehle im Interface Konfigurationsmodus 384
9.1.2.1 flowcontrol 385

9.2 Dynamic MAC Aging 386
9.2.1 Die "show"-Befehle 386
9.2.1.1 show mac-address-table aging-time 386
9.2.1.2 show mac-address-table aging-status 387
9.2.2 Befehle im globalen Konfigurationsmodus 387
9.2.2.1 mac-address-table aging 388
9.2.2.2 no mac-address-table aging 389
9.2.2.3 mac-address-table aging-time 390

10 Layer 3-Funktionen 391

10.1 VRRPv3 (IPv4) 391
10.1.1 clear vrrp3 statistics 391
10.1.2 Die "show"-Befehle 392
10.1.2.1 show vrrp3 392
10.1.2.2 show vrrp3 interface 393
10.1.2.3 show vrrp3 track 393
10.1.3 Befehle im globalen Konfigurationsmodus 394
10.1.3.1 router vrrp3 394
10.1.3.2 no router vrrp3 395
10.1.4 Befehle im VRRP3 Router Konfigurationsmodus 396
10.1.4.1 interface 396
10.1.4.2 no interface 397
10.1.4.3 track interface 398
10.1.4.4 no track interface 399
10.1.4.5 track links 400
10.1.4.6 no track links 401
10.1.4.7 vrrp vrid-track 402
10.1.4.8 no vrrp vrid-track 402
10.1.5 Befehle im Interface Konfigurationsmodus 403
10.1.5.1 vrrp associated-ip 403

10.1.5.2 no vrrp associated-ip ... 404
10.1.5.3 vrrp primary-ip ... 405
10.1.5.4 no vrrp primary-ip ... 406
10.1.5.5 vrrp priority ... 407
10.1.5.6 no vrrp priority ... 408
10.1.5.7 vrrp timer ... 408
10.1.5.8 no vrrp timer ... 410
10.1.5.9 vrrp track decrement ... 411
10.1.5.10 no vrrp track ... 412

10.2 NAT ... 413
10.2.1 Die "show"-Befehle ... 413
10.2.1.1 show firewallnat masquerading ... 413
10.2.1.2 show firewallnat napt ... 414
10.2.1.3 show firewallnat netmap ... 414
10.2.1.4 show firewallnat src-nat ... 415
10.2.2 Befehle im globalen Konfigurationsmodus ... 415
10.2.2.1 firewallnat ... 416
10.2.3 Befehle im FIREWALL NAT-Konfigurationsmodus ... 416
10.2.3.1 Einleitungssatz FirewallNAT Konfigurationsmodus ... 416
10.2.3.2 ipsec connection show-idx ... 417
10.2.3.3 masquerading show-idx ... 418
10.2.3.4 masquerading ... 418
10.2.3.5 no masquerading ... 419
10.2.3.6 napt show-idx ... 420
10.2.3.7 napt type ipv4 ... 421
10.2.3.8 no napt ... 422
10.2.3.9 no napt all ... 423
10.2.3.10 netmap destination srcint ... 424
10.2.3.11 netmap show-idx ... 426
10.2.3.12 netmap source type ipv4 ... 427
10.2.3.13 no netmap srcint ... 429
10.2.3.14 no netmap all ... 430
10.2.3.15 src-nat show-idx ... 431
10.2.3.16 src-nat type ipv4 ... 432
10.2.3.17 no src-nat all ... 434
10.2.3.18 no src-nat ... 434

11 Sicherheit und Authentifizierung ... 437

11.1 RADIUS-Client ... 437
11.1.1 Die "show"-Befehle ... 437
11.1.1.1 show radius statistics ... 438
11.1.1.2 show radius server ... 438
11.1.2 Befehle im globalen Konfigurationsmodus ... 439
11.1.2.1 login authentication ... 439
11.1.2.2 no login authentication ... 440
11.1.2.3 radius authorization-mode ... 441
11.1.2.4 radius-server ... 442
11.1.2.5 no radius-server ... 444

11.2 Benutzerverwaltung ... 445
11.2.1 Die "show"-Befehle ... 445
11.2.1.1 show password-policy ... 445

11.2.1.2 show roles 445
11.2.1.3 show user-accounts 446
11.2.1.4 show user-groups 447
11.2.1.5 show users 448
11.2.2 change password 448
11.2.3 whoami 449
11.2.4 Befehle im globalen Konfigurationsmodus 450
11.2.4.1 loginpage 450
11.2.4.2 password-policy 451
11.2.4.3 role 451
11.2.4.4 no role 453
11.2.4.5 user-account 454
11.2.4.6 no user-account 457
11.2.4.7 user-account-ext 458
11.2.4.8 no user-account-ext 459
11.2.4.9 user-group 460
11.2.4.10 no user-group 461
11.2.4.11 username 462

11.3 Firewall 464
11.3.1 Einleitung zum Kapitel Firewall 464
11.3.2 Die "show"-Befehle 464
11.3.2.1 show firewall icmp-services ipv4 464
11.3.2.2 show firewall information 465
11.3.2.3 show firewall ip-protocols 465
11.3.2.4 show firewall ip-rules ipv4 466
11.3.2.5 show firewall ip-services 466
11.3.2.6 show firewall pre-rules ipv4 467
11.3.2.7 show firewall ruleset 467
11.3.2.8 show firewall ruleset assignment 468
11.3.3 Befehle im globalen Konfigurationsmodus 468
11.3.3.1 firewall 468
11.3.4 Befehle im FIREWALL-Konfigurationsmodus 469
11.3.4.1 Einleitungssatz Firewall Konfigurationsmodus 469
11.3.4.2 di-input set address 471
11.3.4.3 di-input set ruleset 472
11.3.4.4 di-input show-idx 473
11.3.4.5 icmp name 473
11.3.4.6 no icmp 475
11.3.4.7 icmp name set type 476
11.3.4.8 icmp show-names 477
11.3.4.9 icmp show-types-codes 477
11.3.4.10 idle timeout icmp 478
11.3.4.11 idle timeout tcp 479
11.3.4.12 idle timeout udp 479
11.3.4.13 ipv4rule 480
11.3.4.14 ipv4rule del ruleset 483
11.3.4.15 no ipv4 rule 484
11.3.4.16 ipv4rule set action 484
11.3.4.17 ipv4rule set dstip 485
11.3.4.18 ipv4rule set from 486
11.3.4.19 ipv4rule set log 487
11.3.4.20 ipv4rule set prior 488

11.3.4.21 ipv4rule set ruleset ... 489
11.3.4.22 ipv4rule set service ... 490
11.3.4.23 ipv4rule set srcip ... 492
11.3.4.24 ipv4rule set to ... 493
11.3.4.25 ipv4rule ipsec connection ... 494
11.3.4.26 ipv4rule show interfaces ... 494
11.3.4.27 ipv4rule show-rules ... 495
11.3.4.28 prerule all ipv4 ... 496
11.3.4.29 prerule cloudconnector ipv4 ... 497
11.3.4.30 prerule dhcp ipv4 ... 498
11.3.4.31 prerule dns ipv4 ... 499
11.3.4.32 prerule http ipv4 ... 500
11.3.4.33 prerule https ipv4 ... 501
11.3.4.34 prerule ipsec ipv4 ... 502
11.3.4.35 prerule ipv4 show-int ... 503
11.3.4.36 prerule ping ipv4 ... 503
11.3.4.37 prerule snmp ipv4 ... 504
11.3.4.38 prerule ssh ipv4 ... 505
11.3.4.39 prerule systime ipv4 ... 506
11.3.4.40 prerule telnet ipv4 ... 507
11.3.4.41 proto name ... 508
11.3.4.42 no proto ... 509
11.3.4.43 proto show-names ... 510
11.3.4.44 ruleset idx ... 511
11.3.4.45 ruleset name ... 512
11.3.4.46 ruleset show-idx ... 513
11.3.4.47 no ruleset ... 513
11.3.4.48 service name ... 514
11.3.4.49 no service ... 516
11.3.4.50 service name set dst ... 517
11.3.4.51 service name set prot ... 518
11.3.4.52 service name set src ... 519
11.3.4.53 service show-names ... 520
11.3.4.54 shutdown ... 520
11.3.4.55 no shutdown ... 521
11.3.4.56 useraccount show-idx ... 522
11.3.4.57 useraccount ruleset ... 522
11.3.4.58 no useraccount ruleset ... 523

11.4 IPsec VPN ... 525
11.4.1 Die "show"-Befehle ... 525
11.4.1.1 show ipsec conn-authentication ... 525
11.4.1.2 show ipsec connections ... 526
11.4.1.3 show ipsec conn-phase1 ... 526
11.4.1.4 show ipsec conn-phase2 ... 527
11.4.1.5 show ipsec information ... 527
11.4.1.6 show ipsec remoteend ... 528
11.4.2 Befehle im globalen Konfigurationsmodus ... 528
11.4.2.1 ipsec ... 529
11.4.3 Befehle im IPSEC-Konfigurationsmodus ... 529
11.4.3.1 crl-policy ... 530
11.4.3.2 connection name ... 530
11.4.3.3 no connection name ... 531

11.4.3.4 no connection all 532
11.4.3.5 nat-keep-alive 533
11.4.3.6 remote-end name 534
11.4.3.7 no remote-end name 535
11.4.3.8 no remote-end all 536
11.4.3.9 shutdown 536
11.4.3.10 no shutdown 537
11.4.4 Befehle im IPSEC REMOTE END-Konfigurationsmodus 537
11.4.4.1 addr 538
11.4.4.2 addr-mode 539
11.4.4.3 conn-mode 540
11.4.4.4 subnet 541
11.4.4.5 vir-ip 542
11.4.4.6 no vir-ip 543
11.4.5 Befehle im IPSEC CONNECTION-Konfigurationsmodus 543
11.4.5.1 authentication 544
11.4.5.2 k-proto 544
11.4.5.3 loc-subnet 545
11.4.5.4 operation 546
11.4.5.5 phase 547
11.4.5.6 rmend name 548
11.4.5.7 timeout 548
11.4.5.8 vir-ip 549
11.4.5.9 no vir-ip 550
11.4.6 Befehle im IPSEC AUTHENTICATION-Konfigurationsmodus 551
11.4.6.1 auth cacert 551
11.4.6.2 auth psk 552
11.4.6.3 auth remcert 553
11.4.6.4 no auth 554
11.4.6.5 local-id 554
11.4.6.6 no local-id 555
11.4.6.7 rem-id 556
11.4.6.8 no rem-id 557
11.4.7 Befehle im IPSEC PHASE1-Konfigurationsmodus 557
11.4.7.1 aggressive 558
11.4.7.2 no aggressive 558
11.4.7.3 default-ciphers 559
11.4.7.4 no default-ciphers 560
11.4.7.5 dpd 561
11.4.7.6 no dpd 562
11.4.7.7 dpd-period 562
11.4.7.8 dpd-timeout 563
11.4.7.9 ike-auth 564
11.4.7.10 ike-encryption 565
11.4.7.11 ike-keyderivation 566
11.4.7.12 ike-keytries 567
11.4.7.13 ike-lifetime 568
11.4.8 Befehle im IPSEC PHASE2-Konfigurationsmodus 569
11.4.8.1 auto-fwrules 569
11.4.8.2 no auto-fwrules 570
11.4.8.3 default-ciphers 571
11.4.8.4 no default-ciphers 572

11.4.8.5 esp-auth ... 573
11.4.8.6 esp-encryption ... 574
11.4.8.7 esp-keyderivation ... 575
11.4.8.8 lifebyte ... 576
11.4.8.9 lifetime ... 577
11.4.8.10 port ... 578
11.4.8.11 proto ... 579

11.5 Zertifikate ... 580
11.5.1 Befehle im globalen Konfigurationsmodus ... 580
11.5.1.1 certificate ... 580
11.5.2 Befehle im CERT-Konfigurationsmodus ... 581
11.5.2.1 Die "show"-Befehle ... 581
11.5.2.2 cacert ... 583
11.5.2.3 del ... 584
11.5.2.4 passphrase ... 585
11.5.2.5 passphrase show-idx ... 586

11.6 OpenVPN ... 587
11.6.1 Die "show"-Befehle ... 587
11.6.1.1 show openvpn authentication ... 587
11.6.1.2 show openvpn connections ... 588
11.6.1.3 show openvpn remoteend ... 588
11.6.2 Befehle im globalen Konfigurationsmodus ... 589
11.6.2.1 openvpn ... 589
11.6.3 OPENVPN-Konfigurationsmodus ... 590
11.6.3.1 connection name ... 590
11.6.3.2 no conn ... 591
11.6.3.3 remote name ... 592
11.6.3.4 no remote ... 593
11.6.3.5 shutdown ... 593
11.6.3.6 no shutdown ... 594
11.6.4 Befehle im OPENVPN REMOTE END-Konfigurationsmodus ... 595
11.6.4.1 connection ... 595
11.6.4.2 port ... 596
11.6.4.3 proto ... 596
11.6.4.4 proxy ... 597
11.6.4.5 remote-addr ... 598
11.6.4.6 show-context ... 599
11.6.5 Befehle im OPENVPN CONNECTION-Konfigurationsmodus ... 599
11.6.5.1 auth-algo ... 600
11.6.5.2 authentication ... 601
11.6.5.3 autoFW ... 601
11.6.5.4 encryp-algo ... 602
11.6.5.5 NAT ... 603
11.6.5.6 operation ... 604
11.6.5.7 LZO ... 605
11.6.5.8 no LZO ... 606
11.6.5.9 show auth-names ... 606
11.6.5.10 show context ... 607
11.6.6 Befehle im OPENVPN AUTHENTICATION-Konfigurationsmodus ... 607
11.6.6.1 auth ... 608
11.6.6.2 no auth ... 609

11.6.6.3 auth user 609

12 Diagnose 611

12.1 Events- und Faults-Handling 611
12.1.1 Die "show"-Befehle 611
12.1.1.1 show events config 612
12.1.1.2 show events severity....612
12.1.1.3 show events faults config....613
12.1.1.4 show events faults status....614
12.1.1.5 show fault counter....614
12.1.1.6 show fwlog 615
12.1.1.7 show logbook 616
12.1.1.8 show power-line-state 616
12.1.1.9 show seclog 617
12.1.2 clear fault counter 618
12.1.3 clear fwlog....618
12.1.4 clear logbook....619
12.1.5 clear seclog....619
12.1.6 fault report ack 620
12.1.7 no logging console 621
12.1.8 logging console 621
12.1.9 Befehle im globalen Konfigurationsmodus 622
12.1.9.1 events 622
12.1.10 Befehle im Events Konfigurationsmodus 623
12.1.10.1 add log 623
12.1.10.2 client config 624
12.1.10.3 no client config 625
12.1.10.4 event config....626
12.1.10.5 no event config....628
12.1.10.6 link....629
12.1.10.7 no link....630
12.1.10.8 severity....631
12.1.10.9 no severity....632

12.2 Syslog Client 634
12.2.1 Die "show"-Befehle 634
12.2.1.1 show events syslogserver....634
12.2.2 Befehle im Events Konfigurationsmodus 635
12.2.2.1 syslogserver....636
12.2.2.2 no syslogserver....637

Index.... 639

Security-Empfehlung

1

Um nicht autorisierten Zugriff zu unterbinden, beachten Sie folgende Security-Empfehlungen.

Eine Checkliste unterstützt Sie beim Einrichten Ihres Geräts. Sie finden die Checkliste unter folgender Adresse: (https://support.industry.siemens.com/cs/ww/de/view/109745536)

Allgemein

- Stellen Sie regelmäßig sicher, dass das Gerät diese Empfehlungen und/oder andere interne Security-Richtlinien erfüllt.
- Bewerten Sie Ihre Anlage ganzheitlich im Hinblick auf Sicherheit. Nutzen Sie ein Zellenschutzkonzept mit entsprechenden Produkten:

  Link: (https://www.industry.siemens.com/topics/global/de/industrial-security/Seiten/default.aspx)
- Wenn das interne und externe Netzwerk entkoppelt sind, kann ein Angreifer nicht auf interne Daten zugreifen. Betreiben Sie das Gerät daher nur innerhalb eines geschützten Netzwerkbereichs.
- Nutzen Sie VPN, um die Kommunikation von und zu den Geräten zu verschlüsseln und zu authentifizieren.
- Nutzen Sie für die Datenübertragung über ein unsicheres Netzwerk einen verschlüsselten VPN-Tunnel (IPsec, Open VPN).
- Trennen Sie Verbindungen ordnungsgemäß (WBM, Telnet, SSH usw.).

Physischer Zugang

- Beschränken Sie den physischen Zugang zu dem Gerät auf qualifiziertes Personal.
  Die Speicherkarte bzw. der PLUG (C-PLUG, KEY-PLUG) enthalten sensible Daten, wie Zertifikate, Schlüssel usw., die ausgelesen und verändert werden können.
- Sperren Sie ungenutzte physische Ports auf dem Gerät. Ungenutzte Ports können verwendet werden, um unerlaubt auf die Anlage zuzugreifen.

Software (Security-Funktionen)

- Halten Sie die Software aktuell. Informieren Sie sich regelmäßig über Sicherheitsupdates des Produkts.
  Informationen hierzu finden Sie auf den Internetseiten "Industrial Security (https://www.siemens.com/industrialsecurity)".
- Informieren Sie sich regelmäßig über Security Advisories und Bulletins, die vom Siemens ProductCERT (https://www.siemens.com/cert/de/cert-security-advisories.htm) veröffentlicht werden.
- Aktivieren Sie nur Protokolle, die Sie wirklich für den Einsatz des Gerätes benötigen.

- Beschränken Sie den Zugriff auf das Management des Geräts durch Firewall-Regeln.
- Die Möglichkeit der VLAN-Strukturierung bietet guten Schutz gegen DoS-Attacken und nicht autorisierte Zugriffe. Prüfen Sie, ob dies in ihrem Umfeld sinnvoll ist.
- Nutzen Sie einen zentralen Logging-Server, um Änderungen und Zugriffe zu protokollieren. Betreiben Sie Ihren Logging-Server innerhalb des geschützten Netzwerkbereichs und prüfen Sie regelmäßig die Logging-Informationen.
- Es wird empfohlen einen nicht verwendeten PLUG zu formatieren.

Passwörter

- Definieren Sie Regeln für die Nutzung der Geräte und die Vergabe von Passwörtern.
- Aktualisieren Sie regelmäßig Passwörter und Schlüssel, um die Sicherheit zu erhöhen.
- Ändern Sie alle Standard-Passwörter für Benutzer, bevor Sie das Gerät betreiben.
- Verwenden Sie ausschließlich Passwörter mit hoher Passwortstärke. Vermeiden Sie schwache Passwörter, wie z. B. passwort1, 123456789, abcdefgh.
- Stellen Sie sicher, dass alle Passwörter geschützt und unzugänglich für unbefugtes Personal sind.
- Verwenden Sie dasselbe Passwort nicht für verschiedene Benutzer und Systeme oder nachdem es abgelaufen ist.

Schlüssel und Zertifikate

In diesem Abschnitt werden die Security-Schlüssel und -Zertifikate thematisiert, die Sie benötigen, um TLS, VPN (IPsec, OpenVPN) und SINEMA RC einzurichten.

- Im Gerät ist ein vorinstalliertes X.509-Zertifikat mit Schlüssel vorhanden. Ersetzen Sie dieses Zertifikat durch ein selbst erstelltes Zertifikat mit Schlüssel. Es wird empfohlen, ein Zertifikat zu verwenden, das entweder durch eine zuverlässige externe oder interne Zertifizierungsstelle signiert ist.
- Nutzen Sie eine Zertifizierungsstelle inklusive Schlüsselwiderruf und -verwaltung, um die Zertifikate zu signieren.
- Stellen Sie sicher, dass benutzerdefinierte private Schlüssel geschützt und unzugänglich für unbefugte Personen sind.
- Verifizieren Sie Zertifikate und Fingerprints auf Server- und Clientseite, um "Man-in-the-middle"-Angriffe zu verhindern.
- Es wird empfohlen, passwortgeschützte Zertifikate im PKCS#12-Format zu verwenden
- Es wird empfohlen, Zertifikate mit einer Schlüssellänge von mindestens 2048 Bit zu verwenden.
- Ändern Sie Schlüssel und Zertifikate umgehend, wenn der Verdacht auf Kompromittierung besteht.

Sichere/Unsichere Protokolle

- Vermeiden oder deaktivieren Sie unsichere Protokolle, wie z. B. Telnet und TFTP. Diese Protokolle sind aus historischen Gründen noch verfügbar, jedoch nicht für einen sicheren Einsatz gedacht. Setzen Sie unsichere Protokolle auf dem Gerät über eine gesicherte Verbindung (z. B. SINEMA RC) ein.
- Vermeiden oder deaktivieren Sie unsichere Protokolle. Prüfen Sie die Notwendigkeit der Nutzung folgender Protokolle:
  - Telnet
  - HTTP
  - Broadcast-Pings
  - Nicht authentifizierte und unverschlüsselte Schnittstellen
  - ICMP (redirect)
  - LLDP
  - Syslog
  - DHCP-Optionen 66/67
  - SNTP
  - NTP
  - TFTP
  - TIA Portal Cloud Connector
- Die folgenden Protokolle bieten sichere Alternativen:
  - SNMPv1/v2 → SNMPv3

    Prüfen Sie die Notwendigkeit der Nutzung von SNMPv1. SNMPv1 ist als unsicher eingestuft. Nutzen Sie die Möglichkeit den Schreibzugriff zu unterbinden. Das Produkt bietet entsprechende Einstellmöglichkeiten.

    Wenn SNMP aktiviert ist, ändern Sie die Community-Namen. Wenn kein uneingeschränkter Zugriff erforderlich ist, beschränken Sie den Zugriff über SNMP.
  - HTTP → HTTPS
  - Telnet → SSH
  - NTP → Secure NTP
  - SNTP → Secure NTP
  - TFTP → SFTP
  - TIA Portal Cloud Connector über eine sichere Verbindung.

    Verwenden Sie den im Produkt integrierten "TIA Portal Cloud Connector" über eine VPN-Lösung (z.B. SINEMA RC).

    Konfigurieren Sie die Firewall Einstellungen des SCALANCE M800/S615 (z.B. Vordefinierte IPv4 Regeln "Cloud Connector", um den unbefugten Zugriff von Netzteilnehmer auf den "TIA Portal Cloud Connector Server" zu verhindern).
- Nutzen Sie sichere Protokolle, wenn der Zugriff auf das Gerät nicht durch physische Schutzvorkehrungen gesichert ist.

- Um einem unbefugten Zugriff auf das Gerät bzw. Netzwerk vorzubeugen, treffen Sie angemessene Schutzvorkehrungen gegen unsichere Protokolle.
- Wenn Sie unsichere Protokolle und Dienste benötigen, aktivieren Sie diese an Schnittstellen, die sich in einem geschützten Netzwerkbereich befinden.
- Beschränken Sie mit einer Firewall die nach außen angebotenen Dienste und Protokolle auf das erforderliche Mindestmaß.
- Aktivieren Sie für die DCP-Funktion nach der Inbetriebnahme den "DCP Read Only"-Modus.

Liste verfügbarer Protokolle

Nachfolgend werden alle verfügbaren Dienste und deren Ports aufgelistet, über die auf das Gerät zugegriffen werden kann.

Dienst	Protokoll/ Portnummer	Voreingestellter Portstatus		Konfigurierbar		Authentifizierung	Verschlüsselung
		Lokaler Zugriff	Externer Zugriff 1)	Dienst	Port		
DHCP-Client	UDP/68	Geschlossen	Geschlossen	✓	--	--	--
DHCP-Server	UDP/67	Geschlossen 2)	Geschlossen 3)	✓	--	--	--
DNS-Client	TCP/53 UDP/53	Nur ausgehend	Nur ausgehend	✓	--	--	--
DNS-Server	TCP/53 UDP/53	Offen 4)	Geschlossen	✓	--	--	--
DynDNS	TCP/80	Nur ausgehend	Nur ausgehend	✓	--	✓	--
HTTP	TCP/80	Offen	Geschlossen	--	--	✓	--
HTTP Proxy	TCP/80 TCP/443	Nur ausgehend	Nur ausgehend	✓	✓	Optional	--
HTTPS	TCP/443	Offen	Geschlossen	✓	--	✓	✓
IPsec/IKE	UDP/500 UDP/4500	Geschlossen	Geschlossen	✓	--	✓	✓
NTP-Client	UDP/123	Nur ausgehend	Nur ausgehend	✓	✓	--	--
NTP-Client (secure)	UDP/123	Nur ausgehend	Nur ausgehend	✓	✓	✓	--
NTP-Server	UDP/123	Geschlossen	Geschlossen	✓	✓	--	--
NTP-Server (secure)	UDP/123	Geschlossen	Geschlossen	✓	✓	✓	--
OpenVPN	UDP/1194 TCP/1194	Nur ausgehend	Nur ausgehend	✓	✓	✓	✓
Ping	ICMP	Offen	Geschlossen	✓	--	✓	--
PROFINET	UDP/34964	Geschlossen	Geschlossen	--	--	--	--
RADIUS Client	TCP/1812 UDP/1812	Nur ausgehend	Nur ausgehend	✓	✓	✓	--
SFTP	TCP/22	Nur ausgehend	Nur ausgehend	✓	✓	✓	✓

Dienst	Protokoll/ Portnummer	Voreingestellter Portstatus		Konfigurierbar		Authentifizierung	Verschlüsselung
		Lokaler Zugriff	Externer Zugriff [1]	Dienst	Port		
Siemens Remote Service (cRSP/SRS)	TCP/443	Nur ausgehend	Nur ausgehend	✓	--	Optional	✓
SINEMA RC	HTTPS/443 und TCP/UDP abhängig von Serverkonfiguration	Nur ausgehend	Nur ausgehend	✓	✓	✓	✓
SMTP	TCP/25	Nur ausgehend	Nur ausgehend	✓	✓	--	--
SMTP (Secure)	TCP/465 TCP/587	Nur ausgehend	Nur ausgehend	✓	✓	Optional	✓
SNMPv1	UDP/161	Offen	Geschlossen	✓	--	--	--
SNMPv3	UDP/161	Offen	Geschlossen	✓	--	Optional	Optional
SNTP	UDP/123	Geschlossen	Geschlossen	✓	--	--	--
SSH	TCP/22	Offen	Geschlossen	✓	--	✓	✓
Syslog	UDP/514	Nur ausgehend	Nur ausgehend	✓	✓	--	--
Telnet	TCP/23	Geschlossen	Geschlossen	✓	--	✓	--
TFTP	UDP/69	Nur ausgehend	Nur ausgehend	✓	✓	--	--
TIA Portal Cloud Connector [5]	TCP/9023	Geschlossen	Geschlossen	✓	✓	--	--

1) SCALANCE M826 und M804PB ist im Auslieferungszustand (Werkseinstellung) nur der Zugriff über vlan1 möglich.

2) Nur beim SCALANCE M826 offen

3) Nur beim SCALANCE S615 offen

4) Nur beim SCALANCE S615 geschlossen

5) Nur beim SCALANCE M804PB

Erläuterung zu der Tabelle:

- Voreingestellter Portstatus

  Bei dem Status des Ports im Auslieferungszustand (Werkseinstellung) wird zwischen lokalem und externem Zugriff unterschieden.

  – Lokaler Zugriff: Auf den Port wird über eine lokale Verbindung (vlan1) zugegriffen.

  – Externer Zugriff: Auf den Port wird über eine externe Verbindung (vlan2) zugegriffen.

- Dienst / Port konfigurierbar

  Gibt an, ob die Port-Nummer oder der Dienst über das WBM / CLI konfigurierbar sind.

- Authentifizierung

  Gibt an, ob eine Authentifizierung des Kommunikationspartners stattfindet.

  Bei Optional ist die Authentifizierung bei Bedarf konfigurierbar.

- Verschlüsselung

  Gibt an, ob die Übertragung verschlüsselt wird.

  Bei Optional ist die Verschlüsselung bei Bedarf konfigurierbar.

Allgemeines 2

2.1 Nicht unterstützte Features

Folgendes Feature wird von den SCALANCE M-800-Geräten nicht unterstützt:

- IPv6

Auch wenn dieses Feature in der Dokumentation als Parameter aufgeführt ist und mit den Hilfefunktionen `help` und `?` angezeigt werden, können Sie sie mit einem SCALANCE M-800-Gerät nicht ausführen.

2.2 Mengengerüste für WBM und CLI

Mengengerüst des Geräts

In der folgenden Tabelle ist das Mengengerüst für das Web Based Management und das Command Line Interface des Geräts aufgeführt.

Abhängig von Ihrem Gerät stehen Ihnen manche Funktionen nicht zur Verfügung.

	konfigurierbare Funktion	maximale Anzahl
System	Syslog-Server	3
	SMTP-Server	3
	E-Mail-Empfänger	60 20 pro SMTP-Server
	SNMPv1-Trap-Empfänger	10
	SNTP-Server	2
	NTP-Server	3 pro Layer 3-Schnittstelle 1
	DHCP-Pools	8
	IPv4-Adressen, die der DHCP-Server verwaltet (dynamisch + statisch)	100
	Statische Zuordnungen pro DHCP-Pool	20
	DHCP-Optionen (1, 2, 3, 4, 5, 6, 42, 66, 67)	9
	SINEMA RC	1
	Proxy Server	5
Layer 2	Virtuelle LANs (portbased; inklusive VLAN 1)	16
	Maximale Framegröße	2048 Bytes
Layer 3	IP-Schnittstellen	12
	Statische Routen	100
	NETMAP	256
	SourceNAT	32
	NAPT	32
	VRRPv3	VRRPv3-Instanzen (VRID): 2 Zugeordnete IP-Adressen: 1 pro VRID

	konfigurierbare Funktion	maximale Anzahl
Security	Benutzer	30 (inkl. werkseitig voreingestelltem Benutzer "admin")
	Gruppen	32
	Rollen	32 (inkl. der vordefinierten Rollen)
	RADIUS-Server	4
	Firewall	IP-Protokolle:16 IP-Dienste:32 ICMP-Dienste:16 IP-Regeln: 128 Benutzerspezifische Firewall: • Maximale Anzahl: 8 Regelsätze • Parallele Benutzerzugriffe: 4 • Maximal 128 IP-Regeln pro Firewall-Regelsatz
	IPsec VPN	20 Maximal 20 Phase 2-Verbindungen können pro Phase 1 angelegt werden.
	OpenVPN	Verbindungen: 5 Remote-Endpunkte: 25

2.3 Einsatz in einer PROFINET-Umgebung

Hinweis

Gültigkeit CCA-Erklärung

Die CCA Erklärung gilt für PROFINET RT ohne den Einsatz in Medienredundanz Strukturen.

Konfigurationshinweise

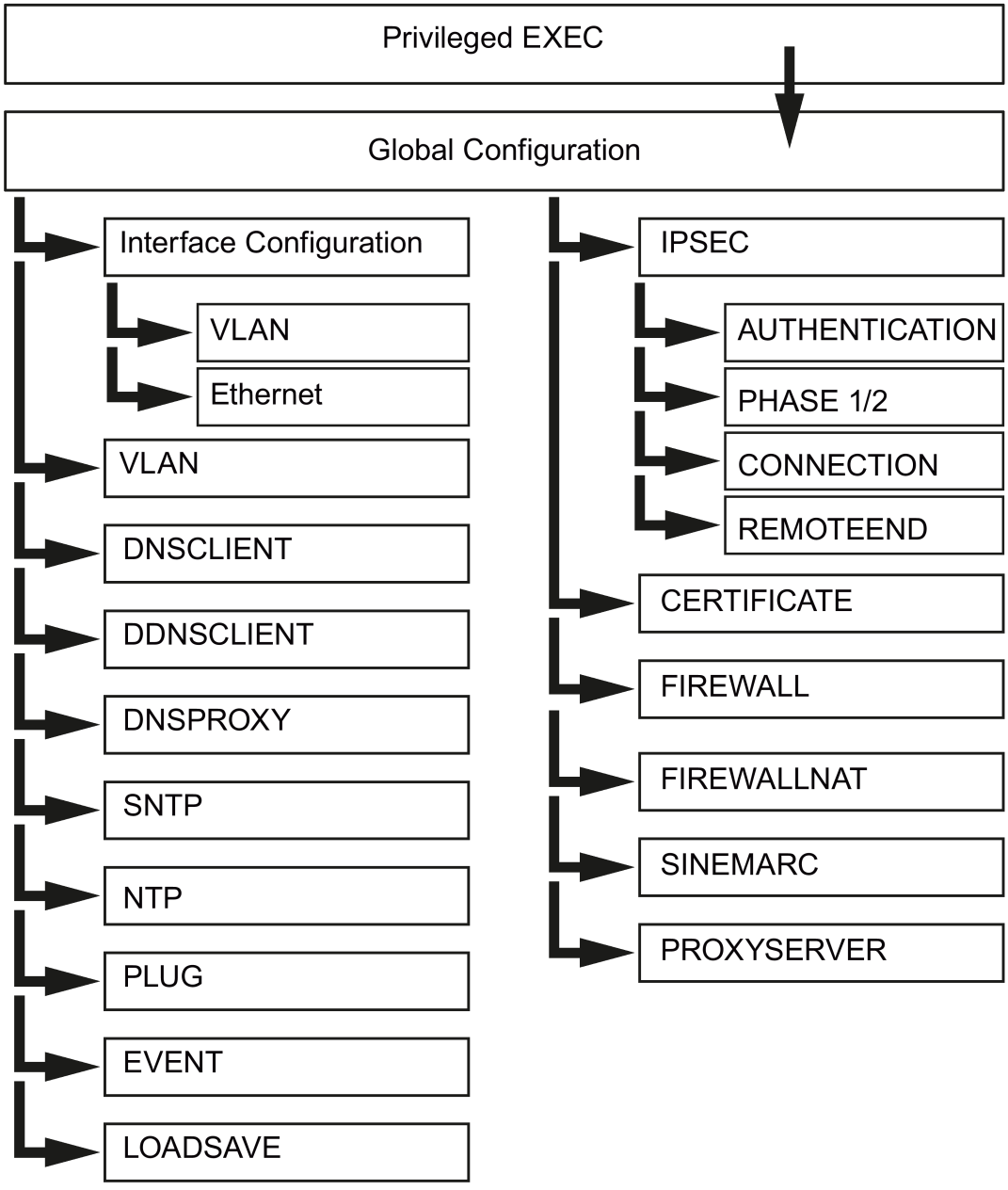
Beachten Sie beim Einsatz des Geräts in einer PROFINET-Umgebung folgende Konfigurationshinweise:

- Stellen Sie die "Aging Time" auf 45 Sekunden.
- Deaktivieren Sie Spanning Tree und aktivieren Sie Passive Listening.

2.4 CLI-Modi

Gliederung der Befehle in verschiedenen Modi

Die Befehle des Command Line Interface sind in verschiedene Modi gegliedert. Von wenigen Ausnahmen abgesehen (help, exit) können Befehle nur in dem Modus aufgerufen werden, dem sie zugeordnet sind. Diese Unterteilung ermöglicht abgestufte Zugriffsrechte für die einzelnen Gruppen von Befehlen. Die folgende Grafik zeigt die verfügbaren Modi in einer Übersicht.



Privileged EXEC Mode

In diesem Modus können Sie sich die Konfigurationsdaten anzeigen lassen und verändern.

Wenn Sie sich mit dem Benutzer "admin" anmelden, gelangen Sie direkt den Privileged EXEC Modus.

Um vom User EXEC Modus in den Privileged Exec Modus zu wechseln, geben Sie den Befehl `enable` ein. Bei Ausführung des Befehls werden Sie aufgefordert das Passwort für den Benutzer "admin" einzugeben. Mit dem Befehl `exit` werden Sie ausgeloggt.

Global Configuration Mode

In diesem Modus können Sie grundlegende Konfigurationseinstellungen vornehmen. Außerdem können Sie die Modi für die Konfiguration spezieller Schnittstellen oder Funktionen aufrufen, z. B. für die Konfiguration eines VLAN oder eines PLUGs. Sie gelangen in diesem Modus, wenn Sie im Privileged EXEC Modus `configure terminal` eingeben. Sie verlassen diesen Modus, wenn Sie `end` oder `exit` eingeben.

Weitere Konfigurations-Modi

Von dem globalen Konfigurationsmodus können Sie in weitere Konfigurations-Modi für spezielle Aufgabe gelangen. Dies sind entweder allgemeine Konfigurationsmodi (zum Beispiel Line Configuration, Interface Configuration) oder protokollspezifische Konfigurations-Modi (FTP, NTP).

2.5 Mit Command Line Interface (CLI) arbeiten

Einleitung

Mit dem Command Line Interface (CLI) können alle Konfigurationseinstellungen für das Gerät festgelegt werden. Das CLI bietet die gleichen Möglichkeiten wie das Web Based Management (WBM). Beachten Sie deshalb auch die ausführlichen Erklärungen zu den Parametern im Projektierungshandbuch "SCALANCE M-800 Web Based Management". Mit dem CLI ist eine Remote-Konfiguration über Telnet und SSH möglich.

Standardmäßig ist der Zugriff über SSH aktiviert. Wenn Sie über eine Telnet-Verbindung auf das CLI zugreifen möchten, müssen Sie unter "System > Konfiguration" die Option "Telnet-Server" aktivieren.

SSH-Verbindung

Für den Zugriff über SSH benötigen Sie einen SSH-Client für Windows.

Telnet-Verbindung: Starten des CLI in einer Windows-Konsole

Hinweis

Telnet - Verwendung unter Windows 7

Wenn Sie unter Windows 7 auf das Command Line Interface zugreifen wollen, achten Sie darauf, dass die hierfür benötigten Funktionen in Windows 7 freigeschaltet sind.

Führen Sie folgende Schritte aus, um das Command Line Interface in einer Windows-Konsole aufzurufen:

1. Öffnen Sie eine Windows-Konsole und geben Sie den Befehl "telnet" gefolgt von der IP-Adresse des zu konfigurierenden Geräts ein:
   ```
   C:\>telnet <IP-Adresse>
   ```
2. Geben Sie Ihr Login und Ihr Passwort ein.

Alternativ dazu können Sie auch im Menü Start > Ausführen den Befehl "telnet" gefolgt von der IP-Adresse des zu konfigurierenden Geräts eingeben.

Hinweis

Voraussetzung für den Einsatz des CLI

Benutzen Sie das Command Line Interface nur, wenn Sie ein erfahrener Benutzer sind.

Auch Befehle, die eine grundlegende Änderung der Konfiguration bewirken, werden ohne Rückfrage ausgeführt.

Fehler in der Konfiguration können dazu führen, dass im gesamten Netzwerk kein Betrieb mehr möglich ist!

Parameter ändern

Wenn Sie die Betriebsart "Automatic Save" aktiviert haben und einen Parameter ändern, startet der Speichervorgang erst, nachdem der Timer abgelaufen ist. Die Dauer des Speichervorgangs ist vom Gerät und von den Änderungen abhängig.

Schalten Sie das Gerät erst aus, wenn der Speichervorgang abgeschlossen ist. Denn erst wenn der Speichervorgang beendet ist, wurde der Parameter in die aktuelle Konfiguration übernommen.

Vorgehen

1. Geben Sie den Befehl `show device information` ein.
   - Im Privileged EXEC Modus: `show device information`
   - In jedem anderen Modus: `do show device information`
2. Prüfen Sie den Status bei Config Change.
   - Saved: Die Änderung ist in der aktuellen Konfiguration gespeichert.
   - Not Saved: Der Speichervorgang dauert noch an.

2.6 Die CLI-Eingabeaufforderung (Der Prompt)

Übersicht

Die Eingabeaufforderung des Command Line Interface zeigt folgende Informationen an:

- den Modus, in dem sich das CLI aktuell befindet.
  Die meisten Befehle können Sie nur in einem bestimmten Modus aufrufen. Überprüfen Sie deshalb den Modus, in dem sich das CLI befindet, an der Eingabeaufforderung.
  - User Exec Modus: `CLI>`
  - Privileged Exec Modus und Konfigurationsmodi: `CLI(...)#`

  Hinweis

  Systemname ändern

  Wenn Sie den Systemnamen ändern, ändert sich auch die Eingabeaufforderung. Statt "`CLI`" wird dann der entsprechende Systemname angezeigt.

- die ausgewählte Schnittstelle, wenn sich das CLI in einem Interface Konfigurationsmodus befindet.
  Im Interface Konfigurationsmodus werden die Parameter für jeweils eine Schnittstelle konfiguriert. Die Eingabeaufforderung wird in der Form `CLI(config-if-$$$)#` dargestellt, wobei der Platzhalter `$$$` durch die Bezeichnung der Schnittstelle ersetzt ist. Sie wählen die Schnittstelle aus, indem Sie den Befehl `interface` entsprechend parametrieren.
- ein Kennzeichen, wenn der Trial-Modus aktiviert ist.
  Wenn Sie Änderungen an der Konfiguration zunächst testen und gegebenenfalls wieder verwerfen wollen, deaktivieren Sie die Auto-Save-Funktion mit dem Befehl `no auto-save`. Sie befinden sich dann im Trial-Modus.
  Nicht gespeicherte Änderungen an der Konfiguration werden durch einen Stern vor der Eingabeaufforderung angezeigt: `*CLI(...)#`.
  Sie speichern die Änderungen der Konfiguration mit dem Befehl `write startup-config`.
  Mit dem Befehl `auto-save` aktivieren Sie die Auto-Save-Funktion wieder.

  Hinweis

  Groß- und Kleinschreibung

  Das Command Line Interface unterscheidet bei den Befehlseingaben nicht zwischen Groß- und Kleinschreibung.

  Beachten Sie aber, dass für Bezeichnungen, die vom Betriebssystem oder anderen Programmen genutzt werden, die korrekte Schreibweise verwendet wird.

  Leerzeichen

  Um Leerzeichen in einem Text zu verwenden, geben Sie den Text mit Anführungszeichen ein, z. B. "H a l l o"

2.7 Symbolik der CLI Befehle

Symbolik für die Darstellung der CLI-Befehle

Bei der Parametrierung von CLI-Befehlen werden folgende Zeichen verwendet:

Zeichen	Bedeutung	
< ... >	notwendiger Parameter	Sie müssen an der Stelle des Klammerausdrucks einen Wert eingeben.
[...]	optionaler Parameter	Sie können an der Stelle des Klammerausdrucks einen Wert eingeben.
(...)	Wert oder Wertebereich	Geben Sie an der Stelle des Klammerausdrucks einen Wert ein.
(... - ...)	Wertebereich	Geben Sie einen Wert aus diesem Wertebereich ein.
{ ... }	Auswahlliste	Wählen Sie ein oder mehrere Elemente der Liste aus.
{ ... | ... }	exklusive Auswahl	Wählen Sie genau ein Element aus dieser Liste aus.

Diese Zeichen werden in Kombinationen eingesetzt, um notwendige und optionale Eingaben zu beschreiben.

Im Folgenden sind einige dieser Kombinationen in allgemeiner Form beschrieben:

Zeichenkombination	Bedeutung
< Parameter >	Geben Sie an Stelle des Klammerausdrucks <> einen zulässigen Wert an.
< Einheit (a - b) >	Geben Sie an Stelle des Klammerausdrucks <> einen Wert aus dem Bereich "a" bis "b" an. Die benutzte Einheit wird vor der Klammer () angegeben und wird ebenfalls durch die Eingabe ersetzt.
[<Parameter 1 >< Parameter 2 >]	Das Parameterpaar ist optional. Wenn Sie die Parametrierung verwenden, müssen Sie an Stelle beider Klammerausdrücke <> jeweils einen zulässigen Wert angeben.
[Schlüsselwort < Einheit (a - b)>]	Die Parametrierung ist optional. Wenn Sie das Schlüsselwort verwenden, müssen Sie an Stelle des Klammerausdrucks <> einen Wert aus dem Bereich "a" bis "b" angeben.
[Schlüsselwort { A | B | C }]	Die Parametrierung ist optional. Wenn Sie das Schlüsselwort verwenden, müssen Sie genau einen der Werte "A", "B" oder "C" angeben.
Schlüsselwort [A] [B] [C]	Geben Sie nach dem Schlüsselwort keinen oder mehrere der Werte "A", "B" oder "C" an.

Zeichenkombination	Bedeutung

Hinweis

Fragezeichen "?" im Benutzername/Passwort

Im CLI ist das Fragezeichen "?" ein Befehl. Wenn im Benutzernamen oder im Passwort ein "?" enthalten ist z. B. für die Anmeldung am RADIUS-Server, wird dies als Befehl interpretiert. Konfigurieren Sie diesen Benutzername und dieses Passwort über das WBM.

2.8 Schnittstellenbezeichnungen und Adressen

2.8.1 Bezeichnung von Schnittstellen

Schnittstellen ansprechen

Das Gerät verfügt über mehrere Arten von Schnittstellen, die in unterschiedlicher Weise angesprochen werden:

Physikalische Schnittstellen ansprechen

Diese Schreibweise gilt entsprechend für andere Befehle, die eine Schnittstelle adressieren.

- Geben Sie den Befehl `interface` an.
- Geben Sie den Schnittstellentyp an, `<interface-type>`.
- Geben Sie nach einem Leerzeichen die Schnittstellenbezeichnung an, `<interface-id>`.

  Die Schnittstellenbezeichnung setzt sich aus der Modulnummer und der Portnummer zusammen, getrennt durch einen Schrägstrich. Die fest im Gerät eingebauten Schnittstellen werden mit Modul 0 bezeichnet.

Beispiel:

Fast-Ethernet: `interface fa 0/1`

Logische Schnittstellen ansprechen

Diese Schreibweise gilt entsprechend für andere Befehle, die eine logische Schnittstelle adressieren.

- Geben Sie den Befehl `interface` an.
- Geben Sie das Schlüsselwort für die VLAN-Schnittstelle an.
- Geben Sie nach einem Leerzeichen die Nummer der VLAN-Schnittstelle an, die Sie beim Anlegen vergeben haben.

Beispiel:

VLAN 2: `interface vlan 2`

Verfügbare physikalische Schnittstellen

Gerät	Schnittstellen	interface-type	interface-id	
S615	5 x Fast-Ethernet	`fa: fast-ethernet`	X = 1 .. 5	`fa 0/X`

Verfügbare logische Schnittstellen

- VLAN
  Das Gerät unterstützt bis zu 16 virtuelle Netze.
  Um ein VLAN nutzen zu können, legen Sie es mit dem Befehl `vlan` an.

Schnittstelle konfigurieren im Interface Konfigurationsmodus

Zum Konfigurieren der Schnittstelle verwenden Sie im globalen Konfigurationsmodus den Befehl `interface`.

Syntax

```
interface{vlan<vlan-id(1-4094)>|<interface-type><interface-id>}
```

- Geben Sie die Schnittstelle an, die Sie konfigurieren wollen. Mit diesem Befehl wechseln Sie in den Interface Konfigurationsmodus.

Da Sie im Interface Konfigurationsmodus jeweils genau eine der vorhandenen Schnittstellen konfigurieren, zeigt die Eingabeaufforderung nicht nur den Modus, sondern auch die Bezeichnung dieser Schnittstelle an.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Dabei ist der Platzhalter `$$$` durch folgende Bezeichnung der Schnittstelle ersetzt:

Schnittstelle	Eingabeaufforderung
`fastethernet: fa 0/x`	`cli(config-if-F0-X) #`
`vlan $`	`cli(config-if-vlan-$)#`

Die Platzhalter `$`, `X` bezeichnen die Nummerierung der Schnittstelle.

2.8.2 Adresstypen, Adressbereiche und Adressmasken

Übersicht

Da die verschiedenen Arten von Adressen jeweils in unterschiedlichen Schreibweisen dargestellt werden können, sind im Folgenden die Notierungen angegeben, die im Command Line Interface verwendet werden:

- IPv4-Adressen
  Adressen für das Internet Protokoll Version 4 werden in der dezimalen Schreibweise von vier Zahlen aus dem Bereich von 0 bis 255, getrennt durch jeweils einen Punkt, angegeben.

  Hinweis

  Bei führenden Nullen werden die Zahlen als Oktalzahlen interpretiert, z. B.: 192.168.070.071 → 192.168.56.57.

- Netzwerkmasken
  Eine Netzwerkmaske ist eine Bitfolge, die den Netzwerkanteil eine IP-Adresse beschreibt.
  Üblich ist die dezimale Schreibweise entsprechend der IP-Adresse.
- Alternative Schreibweise für Netzwerkmasken
  Abweichend von der oben beschriebenen Notierung können Netzwerkmasken auch als Anzahl der 1-Bits dargestellt werden. Die Maske der Dezimaldarstellung 255.255.0.0 wird dann als /16 beschrieben.
  Die Syntax lautet dann z. B.: <ipaddress> / 16
  Beachten Sie, dass sich vor und hinter dem "/" ein Leerzeichen befinden muss.
- MAC-Adressen
  In der Syntax des Command Line Interface wird eine MAC-Adresse als Folge von 6 Bytes in hexadezimaler Form dargestellt, jeweils getrennt durch einen Doppelpunkt.
  Die Syntax lautet dann z. B.: aa:aa:aa:aa:aa:aa
- Multicast-Adressen
  Layer 2 Multicast-Adressen, wie sie in diesem Gerät verwendet werden, werden als MAC-Adressen notiert.
  Für zulässige Adressbereiche beachten Sie die Regelwerke oder fragen Sie Ihren Netzwerkverwalter.

2.8.3 IPv4-Adresse

Wertebereich für IPv4-Adresse

Die IPv4-Adresse besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; z. B. 141.80.0.16

Adressformat IPv4 - Notation

Eine IPv4-Adresse besteht aus 4 Byte. Jedes Byte wird dezimal dargestellt und ist durch einen Punkt vom vorherigen getrennt.

XXX.XXX.XXX.XXX

XXX steht für eine Zahl zwischen 0 und 255

Die IPv4-Adresse besteht aus zwei Teilen:

- Der Adresse des (Sub-)Netzes
- Der Adresse des Teilnehmers (im allgemeinen auch Endteilnehmer, Host oder Netzknoten genannt)

Wertebereich für Subnetzmaske

Die Subnetzmaske besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; z. B. 255.255.0.0

Die 4 Dezimalzahlen der Subnetzmaske müssen in ihrer binären Darstellung von links eine Folge von lückenlosen Werten "1" und von rechts eine Folge von lückenlosen Werten "0" enthalten.

Die Werte "1" bestimmen die Netznummer innerhalb der IPv4-Adresse. Die Werte "0" die Host-Adresse innerhalb der IPv4-Adresse.

Beispiel:

richtige Werte:

255.255.0.0 D = 1111 1111.1111 1111.0000 0000.0000 0000 B

255.255.128.0 D = 1111 1111.1111 1111.1000 0000.0000 0000 B

255.254.0.0 D = 1111 1111.1111 1110.0000 0000.0000.0000 B

falscher Wert:

255.255.1.0 D = 1111 1111.1111 1111.0000 0001.0000 0000 B

Zusammenhang IPv4-Adresse und Subnetzmaske

Die erste Dezimalzahl der IPv4-Adresse (von links) bestimmt den Aufbau der Subnetzmaske hinsichtlich der Anzahl der Werte "1" (binär) wie folgt (für "x" steht die Host-Adresse):

Erste Dezimalzahl der IPv4-Adresse	Subnetzmaske
0 bis 127	255.x.x.x
128 bis 191	255.255.x.x
192 bis 223	255.255.255.x

Classless Inter-Domain Routing (CIDR)

CIDR ist ein Verfahren das mehrerer IPv4-Adressen zu einem Adressbereich zusammenfasst, indem eine IPv4-Adresse mit ihrer Subnetzmaske kombiniert dargestellt wird. Dazu wird an die IPv4-Adresse ein Suffix angehängt, das die Anzahl der auf 1 gesetzten Bits der Netzmaske angibt. Durch die CIDR-Notation lassen sich Routing-Tabellen reduzieren und die verfügbaren Adressbereiche besser ausnutzen.

Beispiel:

IPv4-Adresse 192.168.0.0 mit Subnetzmaske 255.255.255.0

Der Netzanteil der Adresse umfasst in der binären Darstellung 3 x 8 Bits, also 24 Bits.

Daraus ergibt sich die CIDR-Notation 192.168.0.0/24.
Der Host-Anteil umfasst in der binären Darstellung 1 x 8 Bits. Daraus ergibt sich der Adressbereich von 28, also 256 mögliche Adressen.

Wertebereich für Adresse des Netzübergangs

Die Adresse besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; z. B. 141.80.0.1

Zusammenhang IPv4-Adresse und Adresse des Netzübergangs

Die IPv4-Adresse und die Adresse des Netzübergangs dürfen nur an den Stellen unterschiedlich sein, an denen in der Subnetzmaske "0" steht.

Beispiel:

Sie haben eingegeben: für Subnetzmaske 255.255.255.0; für IPv4-Adresse 141.30.0.5 und für die Adresse des Netzübergangs 141.30.128.0. Die IPv4-Adresse und die Adresse des Netzübergangs dürfen nur in der 4. Dezimalzahl einen unterschiedlichen Wert haben. Im Beispiel ist aber die 3. Stelle schon unterschiedlich.

Im Beispiel müssen Sie also alternativ ändern:

die Subnetzmaske auf: 255.255.0.0 oder

die IPv4-Adresse auf: 141.30.128.1 oder

die Adresse des Netzübergangs auf: 141.30.0.1

Allgemeine CLI Befehle 3

In diesem Kapitel werden Befehle beschrieben, die Sie in jedem Modus aufrufen können.

3.1 clear screen

Beschreibung

Mit diesem Befehl leeren Sie den Bildschirm.

Die Eingabeaufforderung wird angezeigt.

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
clear screen
```

Ergebnis

Der Bildschirm ist geleert.

Die Eingabeaufforderung wird angezeigt.

3.2 do

Beschreibung

Mit diesem Befehl können Sie in jedem Konfigurationsmodus die Befehle aus dem Privileged EXEC Modus ausführen.

Syntax

Rufen Sie den Befehl mit folgenden Parametern auf:

```
do [Befehl]
```

Dabei ersetzen Sie `[Befehl]` durch den Befehl aus dem Privileged EXEC Modus, den Sie ausführen wollen.

Beispiel

Sie befinden sich im Interface Konfigurationsmodus und Sie wollen den Befehl `write startup-config` aus dem Privileged EXEC Modus ausführen.

```
cli(config-if-$$)# do write startup-config
```

Ergebnis

Der Befehl aus dem Privileged EXEC Modus wird ausgeführt.

3.3 end

Beschreibung

Mit diesem Befehl verlassen Sie den Konfigurationsmodus und befinden sich dann im Privileged EXEC Modus.

Voraussetzung

Sie befinden sich in einem Konfigurationsmodus.

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
end
```

Ergebnis

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

3.4 exit

Beschreibung

Mit diesem Befehl schließen Sie den aktuellen Modus.

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
exit
```

Ergebnis

Der aktuelle Modus wurde verlassen. Sie befinden sich dann auf der nächsthöheren Ebene.

Wenn Sie sich im Privileged EXEC Modus oder im User EXEC Modus befinden, werden Sie ausgeloggt.

3.5 Hilfefunktionen und unterstützte Eingabe

Das Command Line Interface stellt verschiedene Funktionen zur Verfügung, die bei der Eingabe über die Kommandozeile hilfreich sind:

- `help`
- ?
- Befehlsergänzung mit der Tabulatortaste
- automatische Ergänzung unvollständiger Befehle
- Blättern in der Liste der zuletzt verwendeten Befehle
- Anzeige der Liste der zuletzt verwendeten Befehle (`show history`)

3.5.1 help

Beschreibung

Mit diesem Befehl rufen Sie den Hilfeeintrag zu einem Befehl oder die Befehlsliste auf.

Syntax

Rufen Sie die Hilfe mit folgenden Parametern auf:

```
help [Befehl]
```

Dabei ersetzen Sie `[Befehl]` durch den Befehl, für den Sie Hilfe benötigen.

Wenn der Befehl, für den Sie Hilfe benötigen, aus mehreren Worten besteht, geben Sie diese Worte ohne Leerzeichen ein.

Ergebnis

Die Syntax des Befehls wird angezeigt.

Syntax

Rufen Sie die Hilfe ohne Parameter auf, um eine Liste aller zulässigen Befehle des aktuellen Modus zu erhalten:

```
help
```

Ergebnis

Es werden die Modus-spezifischen und die globalen Befehle angezeigt.

Hinweis

Unvollständiger Befehlsnamen

Wenn Sie beim Aufruf der Hilfe einen unvollständigen Befehl angeben, wird eine Liste aller Befehle erstellt, die mit dem eingegebenen Begriff beginnen.

3.5.2 Der Befehl "?"

Beschreibung

Mit diesem Befehl rufen Sie die Befehlsliste auf.

Syntax

Geben Sie ein Fragezeichen ein, um eine Liste aller zulässigen Befehle des aktuellen Modus zu erhalten:

```
?
```

Für diesen Befehl muss die Eingabetaste nicht gedrückt werden. Der Befehl wird unmittelbar nach Eingabe des Zeichens ausgeführt.

Ergebnis

Es werden die Modus-spezifischen und die globalen Befehle angezeigt.

Hinweis

Unvollständiger Befehlsname

Wenn Sie beim Aufruf der Hilfefunktion einen unvollständigen Befehl angegeben haben, wird eine Liste aller Befehle erstellt, die mit dem eingegebenen Begriff beginnen.

Hinweis

Seitenweise Ausgabe

Bei langen Listen werden die Ergebnisse seitenweise angezeigt. Wenn am unteren Rand der Ausgabe `-- more --` erscheint, gelangen Sie mit der Leerzeichen-Taste auf die nächste Seite. In einer seitenweisen Anzeige können Sie nicht zurückblättern. Mit der Taste `q` beenden Sie die seitenweise Ausgabe.

3.5.3 Befehl "grep"

Beschreibung

Mit diesem Befehl können Sie nach regulären Begriffen in der Ausgabe eines CLI-Befehls suchen. "grep" steht für "get regular expression print".

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
<CLI-Command> | grep [-v] <search string>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`CLI-Command`	Beliebiger CLI-Befehl	-
`-v`	Invertiert die Suche. Listet die Zeilen auf, die nicht dem Suchbegriff entsprechen.	-
`search string`	Sucht in der Ausgabe des CLI-Befehls nach dem diesem Suchbegriff.	Geben Sie den regulären Suchbegriff mit Anführungszeichen an. Beispiel: `show running-config interface vlan 1 | grep "ip address"`

Ergebnis

Die Zeilen werden aufgelistet, die dem Suchbegriff ensprechen bzw. die dem Suchbegriff nicht entsprechen.

3.5.4 Ergänzung von Befehlseingaben

Beschreibung

Der Befehls-Interpreter des Command Line Interface unterstützt Sie bei der Befehlseingabe.

Sobald die ersten Zeichen eines Befehls in der Eingabezeile stehen, kann das System die Eingabe ergänzen, soweit die Zeichenfolge eindeutig ist.

Der Vorgang kann nach der Eingabe weiterer Zeichen wiederholt werden.

Vorgehensweise

Geben Sie die ersten Zeichen des Befehls ein.

Drücken Sie die Tabulatortaste.

Ergebnis

Der Befehls-Interpreter ergänzt die Eingabe soweit, wie der Befehl eindeutig ist.

Wenn Sie eine Zeichenfolge eingegeben haben, die nicht zu einem Befehl ergänzt werden kann, wird eine Fehlermeldung ausgegeben.

- Befehl nicht eindeutig: `% Ambiguous Command`
- Befehl unbekannt: `% Invalid Command`
- Befehl unvollständig: `% Incomplete command`

Wenn die Eingabe noch nicht vollständig ist, geben Sie weitere Zeichen ein.

Mit `?` erhalten Sie eine Liste der möglichen Befehle.

Wiederholen Sie den Vorgang gegebenenfalls, bis der Befehl vollständig ist und ausgeführt werden kann.

3.5.5 Verkürzte Schreibweise von Befehlen

Beschreibung

Der Befehls-Interpreter des Command Line Interface erkennt Befehle auch dann, wenn nur die jeweils ersten Zeichen des Befehls bzw. seiner Teile eingegeben werden.

Voraussetzung dafür ist, dass alle Bestandteile der verkürzten Eingabe genau einem Befehl bzw. den Teilen eines Befehls zugeordnet werden können.

Beispiel

Der Befehl `show event config` kann durch den Ausdruck `sh e c` ersetzt werden.

3.5.6 Wiederverwenden der zuletzt verwendeten Befehle

Beschreibung

Das Command Line Interface speichert die 14 zuletzt verwendeten Befehle in einer Liste, die dem jeweiligen Modus zugeordnet ist. Diese ist dann auch nur in dem betreffenden Modus abrufbar.

Beispiel:
Im globalen Konfigurationsmodus werden alle eingegebenen Befehle gespeichert. Wenn Sie zuvor im Interface Konfigurationsmodus Befehle eingegeben haben, werden diese Befehle nicht in die Liste des globalen Konfigurationsmodus aufgenommen. Diese Befehle können Sie nur im Interface Konfigurationsmodus zur Wiederverwendung aufrufen.

Vorgehensweise

Sie blättern in der Liste der zuletzt eingegebenen Befehle mit der Pfeil-auf- und der Pfeil-ab-Taste.

Wenn der gesuchte Befehl angezeigt wird, können Sie die Befehlszeile nach Bedarf editieren und den Befehl mit der Eingabetaste ausführen.

Weitere Hinweise

Sie zeigen die Liste der zuletzt verwendeten Befehle mit dem Befehl `show history` an. Diese Funktion ist in jedem Modus verfügbar.

Siehe auch

show history (Seite 57)

3.5.7 Abarbeiten einer Befehlsfolge

Trennzeichen für mehrere Befehle in einer Zeile

Sie können im CLI in einer Zeile mehrere Befehle hintereinander aufrufen.

Trennen Sie die Befehle durch ein Semikolon (;) voneinander ab.

Starten Sie nach Beendigung der Eingabe die Bearbeitung dieser Befehlsfolge mithilfe der Eingabetaste.

Beispiel

Die Befehlsfolge

```
CLI#conf t; int vlan 1; no ip address dhcp; ip address 192.168.1.1 255.255.255.0;
end; write startup
```

bewirkt das Gleiche wie:

```
CLI#conf t
CLI(config)#int vlan 1
CLI(config-if-vlan-1)#no ip address dhcp
CLI(config-if-vlan-1)#ip address 192.168.1.1 255.255.255.0
CLI(config-if-vlan-1)#end
CLI#write startup
```

3.5.8 clear history

Beschreibung

Mit diesem Befehl werden die zuletzt eingegebenen Befehle gelöscht.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
clear history
```

Ergebnis

Die zuletzt eingegebenen Befehle werden gelöscht.

Weitere Hinweise

Sie zeigen eine Liste der 14 zuletzt eingegebenen Befehle mit dem Befehl `show history` an.

3.5.9 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

3.5.9.1 show history

Beschreibung

Dieser Befehl zeigt die 14 zuletzt eingegebenen Befehle an.

Die Befehle werden in der Reihenfolge ihres Aufrufs aufgelistet. Der Befehl `show history` wird als zuletzt eingegebener Befehl aufgelistet.

Die Liste ist abhängig vom Modus. Im globalen Konfigurationsmodus werden die 14 Befehle angezeigt, die zuletzt in diesem Modus eingegeben wurden. Diese Befehle werden nicht in der Liste des Interface Konfigurationsmodus aufgeführt.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show history
```

Ergebnis

Die Liste der aufgerufenen Befehle wird angezeigt.

Konfiguration 4

In diesem Kapitel wird Folgendes beschrieben:

- Systemeinstellungen
- Speichern und Laden von Konfigurationen und Firmware
- Neustart des Geräts und Wiederherstellen der Werkseinstellung
- Speichern und Wiederherstellen von Konfigurationsbackups

4.1 System

In diesem Kapitel werden Befehle beschrieben, mit denen allgemeine Systemeigenschaften angezeigt und konfiguriert werden können.

4.1.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

4.1.1.1 show cli-console-timeout

Beschreibung

Dieser Befehl zeigt die Timeout-Einstellung der CLI-Sitzung an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show cli-console-timeout
```

Ergebnis

Die Timeout-Einstellung der CLI-Sitzung wird angezeigt.

4.1.1.2 show coordinates

Beschreibung

Dieser Befehl zeigt die geografischen Koordinaten an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show coordinates
```

Ergebnis

Die geografischen Koordinaten werden angezeigt.

4.1.1.3 show device information

Beschreibung

Dieser Befehl zeigt Informationen über das Gerät an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show device information
```

Ergebnis

Folgende Informationen über das Gerät werden angezeigt:

- MAC-Adresse des Geräts
- Serial Number
- System Up Time
- System Name
- System Contact
- System Location
- Device Type
- Restart Counter
- Config Save Mode
- Config Change: Es wird angezeigt, ob die aktuelle Konfiguration gespeichert ist.
- Login Authentication Mode: Es wird gezeigt, ob die Authentifizierung lokal oder am RADIUS-Server stattfindet.

4.1.1.4 show interfaces

Beschreibung

Dieser Befehl zeigt den Status und die Konfiguration einer, mehrerer oder aller Schnittstellen an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show interfaces [{ [<interface-type> <interface-id>] [{ description | status }] |
{vlan <vlan-id(1-4094)> } }]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstelle	
`description`	zeigt die Beschreibung der Schnittstelle an	-
`status`	zeigt den Status der Schnittstelle an	-
`vlan`	Schlüsselwort für eine VLAN Verbindung	-
`vlan-id`	Nummer des angesprochenen VLAN	1 ... 4094

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Wenn Sie keinen Parameter aus der Parameterliste auswählen, werden der Status und die Konfiguration für alle verfügbaren Schnittstellen angezeigt.

Ergebnis

Der Status und die Konfiguration der ausgewählten Schnittstellen werden angezeigt.

4.1.1.5 show im

Beschreibung

Dieser Befehl zeigt Informationen zu gerätespezifischen Hersteller- und Wartungsdaten wie Artikelnummer, Seriennummer, Versionsnummern etc. an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show im
```

Ergebnis

Die Informationen werden angezeigt.

4.1.1.6 show interface mtu

Beschreibung

Mit diesem Befehl zeigen Sie die Einstellung für die Maximum Transmission Unit (MTU) der Schnittstellen im Gerät an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show interface mtu [{ Vlan <vlan-id (1-4094)> | <interface-type> <interface-id> }]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vlan`	Schlüsselwort für eine VLAN Verbindung	-
`vlan-id`	Nummer des angesprochenen VLAN	1 ... 4094
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstelle	

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Wenn Sie keinen Parameter angeben, werden die Einstellungen für alle Schnittstellen angezeigt.

Ergebnis

Die Einstellungen werden angezeigt.

4.1.1.7 show interfaces ... counters

Beschreibung

Dieser Befehl zeigt die Zähler einer, mehrerer oder aller Schnittstellen an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show interfaces [{ <interface-type> <interface-id> | vlan <vlan-id(1-4094)> }]
counters
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstelle	
`vlan`	Schlüsselwort für eine VLAN-Verbindung	-
`vlan-id`	Nummer des angesprochenen VLAN	1 ... 4094

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Wenn Sie keinen Parameter aus der Parameterliste auswählen, werden die Zähler für alle verfügbaren Schnittstellen angezeigt.

Ergebnis

Die Zähler der ausgewählten Schnittstellen werden angezeigt.

Weitere Hinweise

Die Zähler werden beim Neustart oder mit dem Befehl `clear counters` zurückgesetzt.

4.1.1.8 show lldp neighbors

Beschreibung

Dieser Befehl zeigt den aktuellen Inhalt der Nachbarschaftstabelle an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show lldp neighbors
```

Ergebnis

Die Nachbarschaftstabelle wird angezeigt.

4.1.1.9 show lldp status

Beschreibung

Dieser Befehl zeigt pro Port an, ob LLDP-Telegramme gesendet oder empfangen werden.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show lldp status [port {<interface-type> <interface-id>}]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
port	Schlüsselwort für eine Portbeschreibung.	-
interface-type	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
interface-id	Modul-Nr. und Port-Nr. der Schnittstelle	

Zur Bezeichnung von Schnittstellen und Adressen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Informationen werden angezeigt.

4.1.1.10 show ip interface

Beschreibung

Dieser Befehl zeigt die Konfiguration einer, mehrerer oder aller IP Schnittstellen an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show ip interface [{vlan <vlan-id(1-4094)> | <interface-type> <interface-id> }]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vlan`	Schlüsselwort für eine VLAN-Verbindung	-
`vlan-id`	Nummer des angesprochenen VLAN	1 ... 4094
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstelle	

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Wenn Sie keinen Parameter aus der Parameterliste auswählen, wird die Konfiguration für alle verfügbaren IP Schnittstellen angezeigt.

Ergebnis

Die Konfiguration der ausgewählten IP-Schnittstelle wird angezeigt.

4.1.1.11 show versions

Beschreibung

Dieser Befehl zeigt die Ausgabestände der Hardware und der Software des Geräts an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show versions
```

Ergebnis

Die folgenden Einstellungen werden angezeigt:

- Basic Device
- Name
- Revision
- Order ID
- Firmware
- Bootloader
- Description
- Version
- Date

4.1.2 clear counters

Beschreibung

Mit diesem Befehl setzen Sie die Zähler einer Schnittstelle zurück.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
clear counters [ <interface-type> <interface-id> ]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstelle	

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Wenn Sie keinen Parameter angeben, werden die Zähler für alle Schnittstellen zurückgesetzt.

Ergebnis

Die Zähler der Schnittstelle sind zurückgesetzt.

Weitere Hinweise

Sie zeigen die statistischen Informationen der Schnittstellen mit dem Befehl `show interfaces ... counters` an.

4.1.3 configure terminal

Beschreibung

Mit diesem Befehl wechseln Sie in den globalen Konfigurationsmodus.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
configure terminal
```

Ergebnis

Sie befinden sich jetzt im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Weitere Hinweise

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end`.

4.1.4 clear line vty

Beschreibung

Mit diesem Befehl beenden Sie eine Konsolensitzung auf dem Gerät.

Mit der Option `forceful-clear` beenden Sie eine Session, die nicht reagiert.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
clear line vty {<line-number(2-9)> | all} [forceful-clear]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`line-number`	Nummer der Verbindung, die beendet wird	2 ... 9
`all`	beendet alle Verbindungen	-
`forceful-clear`	beendet eine Session, die nicht reagiert	-

Ergebnis

Die Konsolensitzung ist beendet.

Weitere Hinweise

Sie zeigen die angemeldeten Benutzer mit dem Befehl `show users` an.

4.1.5 disable

Beschreibung

Mit diesem Befehl schließen Sie den Privileged EXEC Modus.

Sie befinden sich dann im User EXEC Modus.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
disable
```

Ergebnis

Sie befinden sich jetzt im User EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli>
```

4.1.6 enable

Beschreibung

Mit diesem Befehl wechseln Sie in den Privileged EXEC Modus.

Voraussetzung

Sie befinden sich im User EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli>
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
enable
```

Ergebnis

Sie werden aufgefordert ein Passwort einzugeben. Geben Sie das Passwort des werkseitig voreingestellten Benutzers "admin" ein. Das Passwort wird bei der ersten Anmeldung geändert und auch der Name kann geändert werden.

Nach erfolgter Anmeldung befinden Sie sich im Privileged EXEC Modus. Die Eingabeaufforderung lautet:

```
cli#
```

4.1.7 logout

Beschreibung

Mit diesem Befehl verlassen Sie das Command Line Interface.

Wenn Sie mit dem Gerät über Telnet verbunden sind, wird die Sitzung geschlossen.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
logout
```

Ergebnis

Die CLI-Sitzung wird beendet und der Windows Login Prompt wird angezeigt.

4.1.8 ping

Beschreibung

Mit diesem Befehl fordern Sie bei einem Gerät im Netzwerk eine Antwort an.

Auf diese Weise können Sie die Erreichbarkeit eines anderen Teilnehmers prüfen.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ping { <destination-address> | fqdn-name <FQDN> }
[size <byte(0-2080)>] [count <packet_count (1-10)>] [timeout <seconds(1-100)>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`destination-address`	Adresse des gerufenen Teilnehmers	Geben Sie eine gültige IPv4-Adresse.
`fqdn-name`	Schlüsselwort für einen Domainnamen	-
`FQDN`	Domainname (Fully Qualified Domain Name) des gerufenen Teilnehmers	Maximal 100 Zeichen
`size`	Schlüsselwort für die Größe der Pakete, die übertragen werden	-
`byte`	Schlüsselwort für die Größe der Pakete in Byte	0 … 2080 Default: 32
`count`	Schlüsselwort für die Anzahl der Pakete, die angefordert werden	-
`packet_count`	Zahl der Pakete	1 … 10 Default: 3

Parameter	Beschreibung	Wertebereich/Anmerkung
`timeout`	Antwort-Wartezeit Nach Ablauf dieser Zeit wird die Anfrage als "timed out" gemeldet.	-
`seconds`	Zeit bis zum Timeout in Sekunden	1 … 100 Default: 1

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Wenn Sie keine Parameter aus der Parameterliste auswählen, werden die voreingestellten Werte verwendet.

Ergebnis

Die Meldungen über die Antwort des gerufenen Teilnehmers werden angezeigt.

4.1.9 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

4.1.9.1 coordinates height

Beschreibung

Mit diesem Befehl geben Sie die geographische Höhe an.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
coordinates height <meter>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`meter`	Geographische Höhe	max. 32 Zeichen Geben Sie den Wert für die geografische Höhe über oder unter normal Null (Meereshöhe) in Metern ein. Um Leerzeichen in der Eingabe zu verwenden, geben Sie die Höhe mit Anführungszeichen ein: `coordinates height "123 456"`

Ergebnis

Die geographische Höhe ist angelegt.

Weitere Hinweise

Sie zeigen die Koordinaten mit dem Befehl `show coordinatea` an.

4.1.9.2 coordinates latitude

Beschreibung

Mit diesem Befehl geben Sie die geographische Breite an.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
coordinates latitude <latitude>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`latitude`	Geographische Breite	max. 32 Zeichen Geben Sie den Wert für nördliche oder südliche Breite ein. Um Leerzeichen in der Eingabe zu verwenden, geben Sie die Breite mit Anführungszeichen ein: `coordinates latitude "123 456"`

Ergebnis

Die geographische Breite ist angelegt.

Weitere Hinweise

Sie zeigen die Koordinaten mit dem Befehl `show coordinatea` an.

4.1.9.3 coordinates longitude

Beschreibung

Mit diesem Befehl geben Sie die geographische Länge an.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
coordinates longitude <longitude>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`longitude`	Geographische Länge	max. 32 Zeichen Geben Sie den Wert für östliche oder westliche Länge ein. Um Leerzeichen in der Eingabe zu verwenden, geben Sie die Länge mit Anführungszeichen ein: `coordinates longitude "123 456"`

Ergebnis

Die geographische Länge ist angelegt.

Weitere Hinweise

Sie zeigen die Koordinaten mit dem Befehl `show coordinatea` an.

4.1.9.4 interface

Beschreibung

Mit diesem Befehl wechseln Sie in den Interface Konfigurationsmodus.

Dort bearbeiten Sie die Einstellungen für jeweils eine Schnittstelle. Sie wählen die Schnittstelle durch die Parametrierung dieses Befehls aus. Wenn Sie eine logische Schnittstelle angeben, die nicht existiert, wird diese angelegt. Die Bezeichnung der ausgewählten Schnittstelle wird in der Eingabeaufforderung angezeigt.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
interface{vlan<vlan-id(1-4094>|<interface-type><interface-id>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Werte
`vlan`	Schlüsselwort für eine VLAN Verbindung	-
`vlan-id`	Nummer des angesprochenen VLAN	1 … 4094
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstelle	

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Dabei ist der Platzhalter `$$$` durch folgende Bezeichnung der Schnittstelle ersetzt:

Typ der Schnittstelle	Eingabeaufforderung
`vlan`	`cli(config-if-vlan-$)#`
`fastethernet`	`cli(config-if-F-X)#`

Die Platzhalter `$` und `X` bezeichnen die Nummerierung der Schnittstelle.

Die Wertebereiche für die physikalischen Schnittstellen sind von der Hardwareausstattung abhängig.

Weitere Hinweise

Sie verlassen den Interface Konfigurationsmodus mit dem Befehl `end` oder `exit`.

Sie löschen eine logische Schnittstelle mit dem Befehl `no interface`.

Sie zeigen den Status und die Konfiguration der Schnittstellen mit dem Befehl `show interfaces` an.

4.1.9.5 no interface

Beschreibung

Mit diesem Befehl löschen Sie eine logische Schnittstelle.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no interface { vlan <vlan-id (1-4094)> }
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vlan`	Schlüsselwort für eine VLAN Verbindung	-
`vlan-id`	Nummer des angesprochenen VLAN	1 … 4094

Ergebnis

Die logische Schnittstelle ist gelöscht.

Weitere Hinweise

Sie konfigurieren eine Schnittstelle mit dem Befehl `interface`.

Sie zeigen den Status und die Konfiguration der Schnittstellen mit dem Befehl `show interfaces` an.

4.1.9.6 cli-console-timeout

Beschreibung

Mit diesem Befehl aktivieren Sie das automatische Ausloggen und Sie konfigurieren die Timeout-Einstellung für die CLI-Sitzung.

Hinweis

Keine automatische Abmeldung vom CLI

Wenn die Verbindung nach der eingestellten Zeit nicht beendet wird, prüfen Sie am Telnet Client die Einstellung von "Keep alive".

Ist die Intervallzeit kleiner als die projektierte Zeit, wird die die Verbindung aufrecht erhalten, obwohl keine Nutzdaten übertragen werden. Z. B. Sie haben bei der automatischen Abmeldung 300 Sekunden und bei "Keep alive" 120 Sekunden eingestellt. In diesem Fall wird alle 120 Sekunden ein Paket gesendet, dass die Verbindung aufrecht erhält.

- Schalten Sie die "Keep alive" aus. (Intervallzeit=0)

  oder
- Stellen Sie die Intervallzeit so hoch ein, dass die unterlagerte Verbindung bei Inaktivität beendet wird.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
cli-console-timeout [<seconds(60-600)>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`seconds`	Zeit bis zum automatischen Ausloggen nach der letzten Eingabe in Sekunden	60 ... 600 Default: 300

Ergebnis

Die Zeitdauer ist konfiguriert und das automatische Ausloggen ist aktiviert.

Weitere Hinweise

Sie deaktivieren das automatische Ausloggen mit dem Befehl `no cli-console-timeout`.

Sie zeigen die aktuelle Timeout-Einstellung mit dem Befehl `show cli-console-timeout` an.

4.1.9.7 no cli-console-timeout

Beschreibung

Mit diesem Befehl deaktivieren Sie das automatische Ausloggen.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no cli-console-timeout
```

Ergebnis

Das automatische Ausloggen ist deaktiviert.

Weitere Hinweise

Sie aktivieren das automatische Ausloggen mit dem Befehl `cli-console-timeout`.

Sie zeigen die aktuelle Timeout-Einstellung mit dem Befehl `show cli-console-timeout` an.

4.1.9.8 system contact

Beschreibung

Mit diesem Befehl geben Sie Kontaktinformationen für das System ein.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
system contact <contact info>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`contact info`	Eingabefeld für die Kontaktinformationen	max. 255 Zeichen

Ergebnis

Die Kontaktinformationen sind im System angelegt.

Weitere Hinweise

Sie zeigen die allgemeinen Geräteinformationen mit dem Befehl `show device information` an.

4.1.9.9 system location

Beschreibung

Mit diesem Befehl geben Sie Standortinformationen für das System ein.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
system location <location name>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`location name`	Eingabefeld für die Standortinformationen	max. 255 Zeichen

Ergebnis

Die Standortinformationen sind im System angelegt.

Weitere Hinweise

Sie zeigen die allgemeinen Geräteinformationen mit dem Befehl `show device information` an.

4.1.9.10 system name

Beschreibung

Mit diesem Befehl geben Sie einen Namen für das System ein.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
system name <system name>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`system name`	Eingabefeld für den Namen	max. 255 Zeichen

Ergebnis

Der Name ist im System angelegt.

In der Eingabeaufforderung wird statt "`cli`" der entsprechende Systemname angezeigt:
`system name``(config)#`

Weitere Hinweise

Sie zeigen die allgemeinen Geräteinformationen mit dem Befehl `show device information` an.

4.1.10 Befehle im Interface-Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im Interface Konfigurationsmodus aufrufen können. Abhängig von der eingestellten Schnittstelle sind verschiedene Befehlssätze verfügbar.

Geben Sie im globalen Konfigurationsmodus den Befehl `interface` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im Interface Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

- Wenn Sie den Interface Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den Interface Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im Interface Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

4.1.10.1 alias

Beschreibung

Mit diesem Befehl weisen Sie einer Schnittstelle einen Namen zu. Der Name hat nur informativen Charakter und keine Auswirkungen auf die Konfiguration.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
alias <interface-name>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`interface-name`	Name der Schnittstelle	max. 63 Zeichen

Ergebnis

Der Schnittstelle wurde ein Name zugewiesen.

Weitere Hinweise

Sie löschen den Namen der Schnittstelle mit Befehl `no alias`.

4.1.10.2 no alias

Beschreibung

Mit diesem Befehl löschen Sie den Namen der Schnittstelle.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no alias
```

Ergebnis

Der Name der Schnittstelle ist entfernt.

Weitere Hinweise

Sie konfigurieren den Namen der Schnittstelle mit Befehl `alias`.

4.1.10.3 duplex

Beschreibung

Elektrische Schnittstellen können im Voll-Duplex-Modus oder im Halb-Duplex-Modus betrieben werden. Die Möglichkeit dazu hängt vom jeweils angeschlossenen Gerät ab.

Optische Verbindungen werden immer im Voll-Duplex-Modus betrieben, da sie jeweils eine Faser für jede Übertragungsrichtung haben.

Mit diesem Befehl konfigurieren Sie den Duplex-Modus einer Schnittstelle. Bei verbundenen Schnittstellen muss der gleiche Modus eingestellt sein.

Voraussetzung

- Autonegotiation ist deaktiviert.
- Sie befinden sich im Interface Konfigurationsmodus einer elektrischen Schnittstelle.

  Die Eingabeaufforderung lautet:

  `cli(config-if-$$$)#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

`duplex {full|half}`

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`full`	die Schnittstelle wird im Voll-Duplex-Modus betrieben.	Default: `full`
`half`	die Schnittstelle wird im Halb-Duplex-Modus betrieben	-

Ergebnis

Der Duplex-Modus der Schnittstelle ist konfiguriert.

Weitere Hinweise

Sie setzen den Duplex-Modus der Schnittstelle mit dem Befehl `no duplex` auf den voreingestellten Wert zurück.

Sie deaktivieren Autonegotiation mit dem Befehl `no negotiation`.

4.1.10.4 no duplex

Beschreibung

Mit diesem Befehl setzen Sie den Duplex-Modus einer Schnittstelle auf den voreingestellten Wert zurück.

Der voreingestellte Wert ist `full`.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

`cli(config-if-$$$)#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no duplex
```

Ergebnis

Der Duplex-Modus der Schnittstelle ist auf den voreingestellten Wert zurückgestellt.

Weitere Hinweise

Sie konfigurieren den Duplex-Modus der Schnittstelle mit dem Befehl `duplex`.

4.1.10.5 lldp

Beschreibung

Mit diesem Befehl aktivieren Sie das Senden oder Empfangen von LLDP Paketen auf der Schnittstelle.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
lldp{transmit|receive}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung
`transmit`	das Senden von LLDP Pakete wird aktiviert
`receive`	das Empfangen von LLDP Pakete wird aktiviert

Bei Systemstart bzw. bei Verwendung des Befehls `restart` mit der Option `memory` oder `factory` gelten folgende Voreinstellungen:

- Senden und Empfangen von LLDP Paketen sind aktiviert.

Hinweis
Beide Optionen aktivieren

Sie können bei einem Aufruf des Befehls nur eine Option auswählen.

Wenn Sie beide Optionen aktivieren wollen, rufen Sie den Befehl erneut auf.

Ergebnis

Die Einstellung ist konfiguriert.

Weitere Hinweise

Sie deaktivieren das Senden oder Empfangen von LLDP Paketen mit dem Befehl `no lldp`.

Sie zeigen den Status von LLDP mit dem Befehl `show lldp status` an.

4.1.10.6 no lldp

Beschreibung

Mit diesem Befehl deaktivieren Sie das Senden oder Empfangen von LLDP Paketen auf der Schnittstelle.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no lldp{transmit|receive}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung
`transmit`	das Senden von LLDP Pakete wird deaktiviert
`receive`	das Empfangen von LLDP Pakete wird deaktiviert

Hinweis

Beide Optionen deaktivieren

Sie können bei einem Aufruf des Befehls nur eine Option auswählen.

Wenn Sie beide Optionen deaktivieren wollen, rufen Sie den Befehl erneut auf.

Ergebnis

Die Einstellung ist konfiguriert.

Weitere Hinweise

Sie aktivieren das Senden oder Empfangen von LLDP Paketen mit dem Befehl `lldp`.

Sie zeigen den Status von LLDP mit dem Befehl `show lldp status` an.

4.1.10.7 negotiation

Beschreibung

Mit diesem Befehl aktivieren Sie das automatische Aushandeln von Verbindungsparametern auf einer Schnittstelle.

Bei verbundenen Schnittstellen muss bei jeder Schnittstelle Autonegotiation eingestellt sein.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
negotiation
```

Ergebnis

Das automatische Aushandeln von Verbindungsparametern auf einer Schnittstelle ist aktiviert.

Weitere Hinweise

Sie deaktivieren das automatische Aushandeln von Verbindungsparametern mit dem Befehl `no negotiation`.

4.1.10.8 no negotiation

Beschreibung

Mit diesem Befehl deaktivieren Sie das automatische Aushandeln von Verbindungsparametern auf einer Schnittstelle.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no negotiation
```

Ergebnis

Das automatische Aushandeln von Verbindungsparametern auf einer Schnittstelle ist deaktiviert.

Weitere Hinweise

Sie aktivieren das automatische Aushandeln von Verbindungsparametern mit dem Befehl `negotiation`.

4.1.10.9 shutdown complete

Beschreibung

Mit diesem Befehl schalten Sie die Schnittstelle ab.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
shutdown complete
```

Ergebnis

Die Schnittstelle ist abgeschaltet.

Hinweis

Wenn Sie diesen Befehl im Interface Konfigurationsmodus für ein VLAN (Eingabeaufforderung `CLI(config-if-vlan-$)#`) anwenden, ist ein Managementzugriff auf das Gerät nicht mehr möglich. Dies betrifft die Konfiguration über CLI, WBM und SNMP. Ein Zugriff ist erst wieder nach dem Zurücksetzen des Geräts auf Werkseinstellungen mit dem Reset-Taster möglich.

Weitere Hinweise

Sie schalten die Schnittstelle mit dem Befehl `no shutdown` ein.

Sie zeigen den Status dieser Funktion und weitere Informationen mit dem Befehl `show interfaces` an.

4.1.10.10 no shutdown

Beschreibung

Mit diesem Befehl schalten Sie eine Schnittstelle ein.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no shutdown
```

Ergebnis

Die Schnittstelle ist angeschaltet.

Weitere Hinweise

Sie schalten die Schnittstelle mit dem Befehl `shutdown complete` ab.

Sie zeigen den Status dieser Funktion und weitere Informationen mit dem Befehl `show interfaces` an.

4.1.10.11 speed

Beschreibung

Mit diesem Befehl konfigurieren Sie die Übertragungsgeschwindigkeit einer Schnittstelle.

Hinweis

Verfügbarkeit dieser Funktion

Die Übertragungsgeschwindigkeit kann nur bei elektrischer Datenübertragung konfiguriert werden.

Bei optischen Verbindungen ist die Übertragungsgeschwindigkeit fest eingestellt.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
speed {10|100}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung
10	Übertragungsgeschwindigkeit 10Mbps
100	Übertragungsgeschwindigkeit 100Mbps

Ergebnis

Die Übertragungsgeschwindigkeit der Schnittstelle ist konfiguriert.

4.2 Load and Save

In diesem Kapitel werden Befehle zum Anzeigen, Kopieren, Speichern und Laden von Dateien für das Gerät beschrieben.

Hinweis

Beachten Sie bei der Installation einer Vorgängerversion kann es zu Verlust der Konfigurationsdaten kommen. In diesem Fall startet das Gerät nach der Installation der Firmware mit den werkseitigen Konfigurationseinstellungen.

4.2.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

4.2.1.1 show loadsave files

Beschreibung

Dieser Befehl zeigt die aktuellen Load&Save-Dateiinformationen an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show loadsave files
```

Ergebnis

Die aktuellen Load&Save-Dateiinformationen werden angezeigt.

4.2.1.2 show loadsave tftp

Beschreibung

Dieser Befehl zeigt die aktuelle Konfiguration des TFTP-Servers für Load&Save an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show loadsave tftp
```

Ergebnis

Die aktuelle Konfiguration des TFTP-Servers für Load&Save wird angezeigt.

4.2.1.3 show loadsave sftp

Beschreibung

Dieser Befehl zeigt die aktuelle Konfiguration des SFTP-Servers für Load&Save an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show loadsave sftp
```

Ergebnis

Die aktuelle Konfiguration des SFTP-Servers für Load&Save wird angezeigt.

4.2.2 load tftp

Beschreibung

Mit diesem Befehl laden Sie Dateien von einem TFTP-Server oder einem SFTP-Server.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
load {tftp | sftp} {ipv4 <ucast_addr> | fqdn-name <FQDN>} [port <tcp port (1-65535)>]
file <filename> filetype <filetype> [user <username>] [password <password>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`tftp`	TFTP-Server	-
`sftp`	SFTP-Server	-
`ipv4`	Schlüsselwort für eine IPv4-Adresse	-
`ucast_addr`	IPv4-Unicast-Adresse des TFTP-Servers	Geben Sie eine gültige Unicast-IPv4-Adresse an.
`fqdn-name`	Schlüsselwort für einen Domainnamen	-
`FQDN`	Domainname (Fully Qualified Domain Name) des TFTP-Servers	Maximal 100 Zeichen
`port`	Schlüsselwort für den Port des Servers, über den die TFTP-Verbindung läuft	-
`tcp port`	Nummer des Ports	1 … 65535
`file`	Schlüsselwort für einen Dateinamen, der zugewiesen wird	-
`filename`	Name der Datei	Maximal 100 Zeichen
`filetype`	Schlüsselwort für den Dateityp, der geladen wird	-
`filetype`	Name des Dateityps	Maximal 100 Zeichen
`user`	Schlüsselwort für Benutzer	-
`username`	Benutzername für den Zugriff auf den SFTP-Server	Geben Sie einen gültigen Benutzernamen ein. Vorausgesetzt, auf dem SFTP-Server ist ein Benutzer mit den entsprechenden Rechten angelegt.

Parameter	Beschreibung	Wertebereich/Anmerkung
`password`	Schlüsselwort für Passwort	-
`password`	Passwort des Benutzers	Geben Sie das Passwort für den Benutzer ein.

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Datei wird vom TFTP-Server oder vom SFTP-Server in das Gerät geladen.

4.2.3 save filetype

Beschreibung

Mit diesem Befehl speichern Sie Dateien auf einem TFTP-Server oder einem SFTP-Server.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
save filetype <filetype> {tftp | sftp} {ipv4 <ucast_addr> | fqdn-name <FQDN>} [port
<tcp port (1-65535)>] file <filename> [user <username>] [password <password>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`filetype`	Schlüsselwort für einen Dateityp, der geladen wird	-
`filetype`	Name des Dateityps	Maximal 100 Zeichen
`tftp`	TFTP-Server	-
`sftp`	SFTP-Server	-
`ipv4`	Schlüsselwort für eine IPv4-Adresse	
`ucast_addr`	IPv4-Unicast-Adresse des TFTP-Servers	Geben Sie eine gültige Unicast-IPv4-Adresse an.
`fqdn-name`	Schlüsselwort für einen Domainnamen	-
`FQDN`	Domainname (Fully Qualified Domain Name) des TFTP-Servers	Maximal 100 Zeichen

Parameter	Beschreibung	Wertebereich/Anmerkung
`port`	Schlüsselwort für den Port des Servers, über den die TFTP-Verbindung läuft	-
`tcp port`	Nummer des Ports	1 … 65535
`file`	Schlüsselwort für einen Dateinamen, der zugewiesen wird	-
`filename`	Name der Datei	Maximal 100 Zeichen

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Datei wird auf dem TFTP-Server oder dem SFTP-Server gespeichert.

4.2.4 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

4.2.4.1 loadsave

Beschreibung

Mit diesem Befehl wechseln Sie in den LOADSAVE Konfigurationsmodus.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
loadsave
```

Ergebnis

Sie befinden sich jetzt im LOADSAVE Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-loadsave)#
```

Weitere Hinweise

Sie verlassen den LOADSAVE Konfigurationsmodus mit dem Befehl `exit`.

4.2.5 Befehle im LOADSAVE Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im LOADSAVE Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl `loadsave` ein, um in diesen Modus zu wechseln.

Die gültigen Dateitypen für die Befehle im LOADSAVE Konfigurationsmodus zeigen Sie mit dem globalen Befehl `show loadsave tftp` an.

- Wenn Sie den LOADSAVE Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den LOADSAVE Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im LOADSAVE Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

4.2.5.1 delete

Beschreibung

Mit diesem Befehl rufen Sie die möglichen Dateien auf oder löschen eine bestimmte Datei.

Voraussetzung

Sie befinden sich im LOADSAVE Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-loadsave)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
delete { showfiles | filetype <filetype> }
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`showfiles`	zeigt die verfügbaren Dateien an	-
`filetype`	Schlüsselwort für den Dateityp, der gelöscht wird	-
`filetype`	Name des Dateityps	max. 100 Zeichen

Ergebnis

Die Dateien werden angezeigt bzw. die Datei wird gelöscht.

Weitere Hinweise

Mit dem Befehl `show loadsave files` können Sie sich die Dateitypen anzeigen lassen.

4.2.5.2 tftp filename

Beschreibung

Mit diesem Befehl weisen Sie einem Dateityp einen Namen zu.

Der Dateityp bestimmt den Typ, der durch eine `tftp load` oder `tftp save` Aktion betroffen ist. Der Name bestimmt die Datei, die zum oder vom TFTP-Server kopiert wird.

Voraussetzung

Sie befinden sich im LOADSAVE Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-loadsave)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
tftp filename {showfiles | filetype <filetype> name <filename>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`showfiles`	zeigt die verfügbaren Dateien an	-
`filetype`	Schlüsselwort für einen Dateityp, dem ein Name zugewiesen wird	-

Parameter	Beschreibung	Wertebereich/Anmerkung
`filetype`	Name des Dateityps	max. 100 Zeichen
`name`	Schlüsselwort für einen Dateinamen, der dem Dateityp zugewiesen wird	-
`filename`	Name der Datei	max. 100 Zeichen

Ergebnis

Die Dateitypen werden angezeigt bzw. dem Dateityp ist ein Name zugewiesen.

Weitere Hinweise

Mit dem Befehl `show loadsave files` können Sie sich die Dateitypen anzeigen lassen.

4.2.5.3 tftp load

Beschreibung

Mit diesem Befehl laden Sie eine Datei von einem TFTP-Server in das Dateisystem des Geräts. Zum Übertragen wird das TFTP-Protokoll verwendet. Zusätzlich können Sie sich eine Liste der verfügbaren Dateien anzeigen lassen.

Voraussetzung

- Der Name der Datei ist festgelegt
- Sie befinden sich im LOADSAVE Konfigurationsmodus.
  Die Eingabeaufforderung lautet:
  `cli(config-loadsave)#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
tftp load { showfiles | filetype <filetype> }
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`showfiles`	zeigt die verfügbaren Dateien an	-
`filetype`	Schlüsselwort für einen Dateityp, der geladen wird	-
`filetype`	Name des Dateityps	max. 100 Zeichen

Ergebnis

Die Dateitypen werden angezeigt bzw. die Datei wird auf das Gerät geladen.

Weitere Hinweise

Sie konfigurieren den Namen der Datei mit dem Befehl `tftp filename` .

Mit dem Befehl `show loadsave files` können Sie sich die Dateitypen anzeigen lassen.

4.2.5.4 tftp save

Beschreibung

Mit diesem Befehl kopieren Sie eine Datei aus dem Dateisystem des Geräts auf einen TFTP-Server. Zum Übertragen wird das TFTP-Protokoll verwendet. Zusätzlich können Sie sich eine Liste der verfügbaren Dateien anzeigen lassen.

Voraussetzung

- Der Name der Datei ist festgelegt
- Sie befinden sich im LOADSAVE Konfigurationsmodus.
  Die Eingabeaufforderung lautet:
  `cli(config-loadsave)#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
tftp save { showfiles | filetype <filetype> }
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`showfiles`	zeigt die verfügbaren Dateien an	-
`filetype`	Schlüsselwort für einen Dateityp, der geladen wird	-
`filetype`	Name des Dateityps	max. 100 Zeichen

Ergebnis

Die Dateitypen werden angezeigt bzw. die Datei wird kopiert.

Weitere Hinweise

Sie konfigurieren den Namen der Datei mit dem Befehl `tftp filename` .

Mit dem Befehl `show loadsave files` können Sie sich die Dateitypen anzeigen lassen.

4.2.5.5 tftp server

Beschreibung

Mit diesem Befehl konfigurieren Sie den Zugang auf einen TFTP-Server.

Voraussetzung

Sie befinden sich im LOADSAVE Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-loadsave)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
tftp server {ipv4 <ucast-addr> | fqdn-name <FQDN>} [port <tcp port(1-65535)>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ipv4`	Schlüsselwort für eine IPv4-Adresse	-
`ipv4-address`	Wert für eine IPv4-Unicast-Adresse	Geben Sie eine gültige IPv4-Unicast-Adresse an.
`fqdn-name`	Schlüsselwort für einen Domainnamen	-
`FQDN`	Domainname (Fully Qualified Domain Name)	Maximal 100 Zeichen
`port`	Schlüsselwort für den Port des Servers, über den die TFTP-Verbindung läuft	-
`tcp port`	Nummer des Ports	1 … 65535

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Einstellungen für den Zugang auf den gewählten TFTP-Server sind konfiguriert.

4.2.5.6 sftp filename

Beschreibung

Mit diesem Befehl weisen Sie einem Dateityp einen Namen zu.

Der Dateityp bestimmt den Typ, der durch eine `sftp load` oder `sftp save` Aktion betroffen ist. Der Name bestimmt die Datei, die zum oder vom SFTP-Server kopiert wird.

Voraussetzung

Sie befinden sich im LOADSAVE Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-loadsave)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
sftp filename {showfiles | filetype <filetype> name <filename>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`showfiles`	zeigt die verfügbaren Dateien an	-
`filetype`	Schlüsselwort für einen Dateityp, dem ein Name zugewiesen wird	-
`filetype`	Name des Dateityps	max. 100 Zeichen
`name`	Schlüsselwort für einen Dateinamen, der dem Dateityp zugewiesen wird	-
`filename`	Name der Datei	max. 100 Zeichen

Ergebnis

Die Dateitypen werden angezeigt bzw. dem Dateityp ist ein Name zugewiesen.

Weitere Hinweise

Mit dem Befehl `show loadsave files` können Sie sich die Dateitypen anzeigen lassen.

4.2.5.7 sftp load

Beschreibung

Mit diesem Befehl laden Sie eine Datei von einem SFTP-Server in das Dateisystem des Geräts. Zusätzlich können Sie sich eine Liste der verfügbaren Dateien anzeigen lassen.

Voraussetzung

- Der Name der Datei ist festgelegt
- Sie befinden sich im LOADSAVE Konfigurationsmodus.
  Die Eingabeaufforderung lautet:
  `cli(config-loadsave)#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
sftp load { showfiles | filetype <filetype> }
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`showfiles`	zeigt die verfügbaren Dateien an	-
`filetype`	Schlüsselwort für einen Dateityp, der geladen wird	-
`filetype`	Name des Dateityps	max. 100 Zeichen

Ergebnis

Die Dateitypen werden angezeigt bzw. die Datei wird auf das Gerät geladen.

Weitere Hinweise

Sie konfigurieren den Namen der Datei mit dem Befehl `sftp filename` .

Mit dem Befehl `show loadsave files` können Sie sich die Dateitypen anzeigen lassen.

4.2.5.8 sftp save

Beschreibung

Mit diesem Befehl kopieren Sie eine Datei aus dem Dateisystem des Geräts auf einen SFTP-Server. Zum Übertragen wird das SFTP-Protokoll verwendet. Zusätzlich können Sie sich eine Liste der verfügbaren Dateien anzeigen lassen.

Voraussetzung

- Der Name der Datei ist festgelegt
- Sie befinden sich im LOADSAVE Konfigurationsmodus.
  Die Eingabeaufforderung lautet:
  `cli(config-loadsave)#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
sftp save { showfiles | filetype <filetype> }
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`showfiles`	zeigt die verfügbaren Dateien an	-
`filetype`	Schlüsselwort für einen Dateityp, der geladen wird	-
`filetype`	Name des Dateityps	max. 100 Zeichen

Ergebnis

Die Dateitypen werden angezeigt bzw. die Datei wird kopiert.

Weitere Hinweise

Sie konfigurieren den Namen der Datei mit dem Befehl `sftp filename`.

Mit dem Befehl `show loadsave files` können Sie sich die Dateitypen anzeigen lassen.

4.2.5.9 sftp server

Beschreibung

Mit diesem Befehl konfigurieren Sie den Zugang auf einen SFTP-Server.

Voraussetzung

Sie befinden sich im LOADSAVE Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-loadsave)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
 sftp server {ipv4 <ucast_addr> | fqdn-name <FQDN>} [port <tcp port (1-65535)>] [user
<username>] [password <password>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ipv4`	Schlüsselwort für eine IPv4-Adresse	-
`ucast_addr`	Wert für eine IPv4-Unicast-Adresse	Geben Sie eine gültige IPv4-Unicast-Adresse an.
`fqdn-name`	Schlüsselwort für einen Domainnamen	-
`FQDN`	Domainname (Fully Qualified Domain Name)	Maximal 100 Zeichen

Parameter	Beschreibung	Wertebereich/Anmerkung
`port`	Schlüsselwort für den Port des Servers, über den die SFTP-Verbindung läuft	-
`tcp port`	Nummer des Ports	1 … 65535
`user`	Schlüsselwort für Benutzer	-
`username`	Benutzername für den Zugriff auf den SFTP-Server	Geben Sie einen gültigen Benutzernamen ein. Vorausgesetzt, auf dem SFTP-Server ist ein Benutzer mit den entsprechenden Rechten angelegt.
`password`	Schlüsselwort für Passwort	-
`password`	Passwort des Benutzers	Geben Sie das Passwort für den Benutzer ein.

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Einstellungen für den Zugang auf den gewählten SFTP-Server sind konfiguriert.

4.2.5.10 password

Beschreibung

Mit diesem Befehl aktivieren und konfigurieren Sie das für eine Datei festgelegte Passwort.

Voraussetzung

Sie befinden sich im LOADSAVE Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-loadsave)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
password { showfiles | filetype <filetype> [pw <password>] }
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Werte
`showfiles`	Zeigt die verfügbaren Dateien an. Für den Dateityp HTTPSCert wird zusätzlich der Status angezeigt. Es gibt folgende Möglichkeiten: • Invalid Das Passwort passt nicht zum Zertifikat. Nach einem Neustart wird das Default-Zertifikat verwendet. • Valid Das Passwort passt zum Zertifikat. Nach einem Neustart wird das geladene Zertifikat verwendet. • - Es wurde kein Passwort vergeben. Nach einem Neustart wird das Default-Zertifikat verwendet.	-
`filetype`	Schlüsselwort für den Dateityp.	-
`filetype`	Name des Dateityps	max. 100 Zeichen
`pw`	Schlüsselwort für das Passwort	-
`password`	Passwort	Geben Sie für die Datei das Passwort ein.

Ergebnis

Das Passwort für die Datei ist konfiguriert und aktiviert.

Weitere Hinweise

Sie deaktivieren das Passwort mit dem Befehl `no password`.

4.2.5.11 no password

Beschreibung

Mit diesem Befehl deaktivieren Sie das Passwort für eine Datei.

Voraussetzung

Sie befinden sich im LOADSAVE Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-loadsave)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no password { showfiles | filetype <filetype>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Werte
`showfiles`	zeigt die verfügbaren Dateien an	-
`filetype`	zeigt an, dass der Dateityp folgt, der geladen wird	-
`filetype`	Name des Dateityps	max. 100 Zeichen

Ergebnis

Das Passwort für die Datei ist deaktiviert.

Weitere Hinweise

Sie aktivieren das Passwort für das Benutzerzertifikat mit dem Befehl `password`.

4.3 Reset and Defaults

In diesem Kapitel werden Befehle zum Neustart des Geräts und zum Wiederherstellen der Ursprungskonfiguration beschrieben.

4.3.1 restart

Beschreibung

Mit diesem Befehl starten Sie das Gerät neu.

Wählen Sie eine der folgenden Konfigurationseinstellungen:

- Neustart des Geräts mit der aktuellen Konfiguration
- Neustart des Geräts mit den werkseitigen Konfigurationseinstellungen mit Ausnahme folgender Parameter:
  - IP-Adressen
  - Subnetzmaske
  - IP-Adresse des Standard-Gateways
  - DHCP Client ID
  - DHCP
  - Systemname
  - System-Aufstellungsort
  - System-Ansprechpartner
  - Benutzernamen und Passwörter
  - Betriebsart des Geräts
- Neustart des Geräts mit den werkseitigen Konfigurationseinstellungen.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
restart[{memory|factory}]
```

Dabei haben die Parameter folgende Bedeutung:

- ohne Angabe von Parametern: startet das System mit der aktuellen Konfiguration neu

Parameter	Beschreibung
`memory`	Setzt das System auf die werkseitigen Konfigurationseinstellungen zurück und startet das System neu. Vom Zurücksetzen sind die oben aufgeführten Parameter ausgenommen.
`factory`	Setzt das System auf die werkseitigen Konfigurationseinstellungen zurück und startet das System neu.

Hinweis

Durch das Zurücksetzen auf die werkseitigen Konfigurationseinstellungen verliert das Gerät seine projektierte IP-Adresse und ist wieder über die werkseitig eingestellte IP-Adresse 192.168.1.1 zu erreichen.

Ergebnis

Das Gerät wird mit den ausgewählten Einstellungen neu gestartet.

4.4 Configuration Save & Restore

In diesem Kapitel werden Befehle zum Anzeigen, Speichern und Wiederherstellen von Konfigurationseinstellungen beschrieben.

4.4.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

4.4.1.1 show running-config

Beschreibung

Dieser Befehl zeigt Konfigurationseinstellungen des Geräts an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show running-config [{syslog | dhcp | vlan [ <vlan-id (1-4094)>] | interface {
<interface-type> <interface-id> | vlan <vlan-id(1-4094)> | ppp <id(0-6)>} | ssh | ssl
| ip | snmp | sntp | http | auto-logout | time | ntp | auto-save | events | firewall
| firewallnat | openvpn | sinemarc | proxyserver | srs | ipsec | ddnsclient |
dnsclient | dnsproxy | modem}] [all]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich
`syslog`	Zeigt die Konfigurationseinstellungen der Syslog Funktion an.	-
`dhcp`	Zeigt die Konfigurationseinstellungen des Dynamic Host Configuration Protocol an.	-
`vlan`	Schlüsselwort für eine VLAN Verbindung	-
`vlan-id`	Nummer des angesprochenen VLAN	1 ... 4094
`interface`	Zeigt an, dass eine Schnittstellenbeschreibung folgt.	-

Parameter	Beschreibung	Wertebereich
interface-type	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
interface-id	Modul-Nr. und Port-Nr. der Schnittstelle	
ppp	Schlüsselwort für die PPP-Schnittstelle	
id	Nummer der Schnittstelle	0 ... 6
ssh	Zeigt die Konfigurationseinstellungen des Secure Shell Protokolls an.	-
ssl	Zeigt die Konfigurationseinstellungen des Secure Sockets Layer Protokolls an.	-
ip	Zeigt die Konfigurationseinstellungen des Internet Protocol an.	-
snmp	Zeigt die Konfigurationseinstellungen des Simple Network Management Protocol an.	-
http	Zeigt die Konfigurationseinstellungen des Hypertext Transfer Protocol an.	-
sntp	Zeigt die Konfigurationseinstellungen des Simple Network Time Protocol an.	-
http	Zeigt die Konfigurationseinstellungen des Hypertext Transfer Protocol an.	-
auto-logout	Zeigt die Konfigurationseinstellungen der Funktion Auto Logout an.	-
time	Zeigt die Konfigurationseinstellungen der Systemzeit an.	-
ntp	Zeigt die Konfigurationseinstellungen des Network Time Protocol an.	-
auto-save	Zeigt die Konfigurationseinstellungen der Funktion Auto-Save an.	-
events	Zeigt die Konfigurationseinstellungen der Systemer-eignisse an.	-
firewall	Zeigt die Konfigurationseinstellungen der Firewall an.	-
firewallnat	Zeigt die Konfigurationseinstellungen von NAT an.	-
openvpn	Zeigt die Konfigurationseinstellungen von OpenVPN an.	
sinemarc	Zeigt die Konfigurationseinstellungen der SINEMA RC-Verbindung an.	-
proxyserver	Zeigt die Konfigurationseinstellungen der Proxy-Server an.	-
srs	Zeigt die Konfigurationseinstellungen von SRS an.	-
ipsec	Zeigt die Konfigurationseinstellungen von IPsec an.	-
ddnsclient	Zeigt die Konfigurationseinstellungen des dynami-schen DNS-Clients an.	-
dnsclient	Zeigt die Konfigurationseinstellungen des DNS-Clients an.	-
dnsproxy	Zeigt die Konfigurationseinstellungen des DNS-Proxys an.	-
modem	Zeigt die Konfiguration des Geräts an.	-
all	Zeigt alle Konfigurationseinstellungen an.	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Wenn Sie den Befehl ohne Parameter aufrufen, werden nur die aktiven Betriebseinstellungen aller Module in allen Schnittstellen angezeigt, die nicht den voreingestellten Werten entsprechen.

Ergebnis

Die ausgewählten Konfigurationseinstellungen des Geräts werden angezeigt.

4.4.2 write startup-config

Beschreibung

Mit diesem Befehl speichern Sie die Änderungen an der Konfiguration in der Konfigurationsdatei.

Die Verwendung dieses Befehls ist im Trial-Modus erforderlich. Er kann auch im Auto-Save-Modus verwendet werden.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`*cli#` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
write startup-config
```

Ergebnis

Die Änderungen sind in der Konfigurationsdatei gespeichert.

Wenn Sie das Gerät mit dem Befehl `restart` ohne Parametrierung neu starten, wird diese Konfiguration verwendet.

Weitere Hinweise

Sie aktivieren die Auto-Save-Funktion bzw. deaktivieren den Trial-Modus mit dem Befehl `auto-save`.

Sie deaktivieren die Auto-Save-Funktion bzw. aktivieren den Trial-Modus mit dem Befehl `no auto-save`.

4.4.3 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

4.4.3.1 auto-save

Beschreibung

Das CLI kann Änderungen an der Konfiguration automatisch abspeichern.

Wenn Sie Änderungen an der Konfiguration zunächst testen und gegebenenfalls wieder verwerfen wollen, können Sie die Auto-Save-Funktion deaktivieren.

Sie befinden sich dann im Trial-Modus.

Nicht gespeicherte Änderungen an der Konfiguration werden durch einen Stern vor der Eingabeaufforderung angezeigt: `*cli(...)#`.

Sie speichern die Änderungen der Konfiguration mit dem Befehl `write startup-config`.

Mit dem Befehl `auto-save` aktivieren Sie die Auto-Save-Funktion.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
auto-save
```

Der Defaultwert der Funktion ist "aktiviert".

Ergebnis

Die Auto-Save-Funktion ist aktiviert.

Weitere Hinweise

Sie speichern Änderungen der Konfiguration im Trial-Modus mit dem Befehl `write startup-config`.

Sie deaktivieren die Funktion mit dem Befehl `no auto-save`.

Sie zeigen den Status dieser Funktion und weitere Informationen mit dem Befehl `show device information` an.

4.4.3.2 no auto-save

Beschreibung

Mit diesem Befehl deaktivieren Sie die Auto-Save-Funktion.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no auto-save
```

Ergebnis

Die Auto-Save-Funktion ist deaktiviert. Der Trial-Modus ist eingeschaltet.

Weitere Hinweise

Sie aktivieren die Funktion mit dem Befehl `auto-save`.

Sie zeigen den Status dieser Funktion und weitere Informationen mit dem Befehl `show device information` an.

Sie speichern Änderungen der Konfiguration im Trial-Modus mit dem Befehl `write startup-config`.

4.5 DCP Discovery

In diesem Kapitel werden Befehle zum Anzeigen und Setzen von Netzwerkparametern beschrieben.

4.5.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

4.5.1.1 show das info

Beschreibung

Dieser Befehl zeigt die Geräte an, die über die Schnittstelle erreichbar sind und DCP unterstützen. DCP Discovery sucht nur nach Geräten, die im gleichen Subnetz liegen wie die Schnittstelle.

Das Ergebnis der Suche wird nicht dauerhaft gespeichert. Führen Sie die Suche nach einem Neustart erneut durch.

Voraussetzung

- Der Befehl `das discover interface` ist ausgeführt.
- Sie befinden sich im Privileged EXEC Modus.

  Die Eingabeaufforderung lautet:

  ```
  cli#
  ```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show das info
```

Ergebnis

In der Tabelle werden die erreichbaren Geräte und ihre Netzwerkparameter angezeigt.

Weitere Hinweise

Sie starten die Suche nach verfügbaren Geräten mit dem Befehl `das discover interface`.

Sie konfigurieren die Netzwerkparameter des erreichbaren Geräts mit dem Befehl `das mac ip`.

Sie löschen den Inhalt der Tabelle mit dem Befehl `das delete`.

Sie konfigurieren den PROFINET-Gerätenamen des erreichbaren Geräts mit dem Befehl `das mac name`.

4.5.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

4.5.2.1 das discover interface

Beschreibung

Mit diesem Befehl starten Sie die Suche nach Geräten, die über die gewählte Schnittstelle erreichbar sind. Die Funktion ist nur in dem mit der TIA-Schnittstelle assoziierten VLAN verfügbar.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
das discover interface { <interface-type> <interface-id> | vlan <vlan-id(1-4094)> |
port-channel <port-channel-id (1-8)}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstelle	
`vlan`	Schlüsselwort für eine VLAN-Verbindung	-
`vlan-id`	Nummer des angesprochenen VLAN	1 … 4094
`port-channel`	Schlüsselwort für eine Link Aggregation	-
`port-channel-id`	Nummer der angesprochenen Link Aggregation	1 ... 8

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Nach den erreichbaren Geräten wird gesucht. Nach dem Abschluss der Suche werden die erreichbaren Geräte in einer Tabelle gespeichert. Sie zeigen die Tabelle mit dem Befehl `show das info` an.

4.5.2.2 das mac name

Beschreibung

Mit diesem Befehl konfigurieren Sie den PROFINET-Gerätenamen des ausgewählten Geräts.

Voraussetzung

- Der Befehl `das discover interface` ist ausgeführt.
- Sie befinden sich im globalen Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
das mac <aa:aa:aa:aa:aa:aa> name <name(127)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
-	MAC-Adresse des erreichbaren Geräts	`aa:aa:aa:aa:aa:aa`
`name`	PROFINET-Gerätename	Maximal 127 Zeichen Der Gerätename muss DNS-konform sein.

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Der PROFINET-Gerätename des ausgewählten Geräts ist konfiguriert.

Um sicherzustellen, dass die Eigenschaft korrekt übernommen wurden, führen Sie erneut den Befehl `das discover interface` aus.

Weitere Hinweise

Sie zeigen den konfigurierten PROFINET-Gerätenamen mit dem Befehl `show das info` an.

4.5.2.3 das mac ip

Beschreibung

Mit diesem Befehl konfigurieren Sie die Netzwerkparameter des ausgewählten Geräts.

Voraussetzung

- Der Befehl `das discover interface` ist ausgeführt.
- Sie befinden sich im globalen Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
das mac <aa:aa:aa:aa:aa:aa> ip <ip address> {<subnet-mask> | / <prefix-length(1-32)>}
[gateway <ip address>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
-	MAC-Adresse des erreichbaren Geräts	`aa:aa:aa:aa:aa:aa`
`ip`	Schlüsselwort für IPv4-Adresse	
`ip address`	IPv4-Adresse des Geräts	Geben Sie eine gültige IPv4-Adresse an.
`subnet-mask`	Subnetzmaske	
`prefix-length`	Dezimale Darstellung der Maske als Anzahl der "1" Bits	1 ... 32
`gateway`	Schlüsselwort für Gateway	-
`ip address`	IPv4-Adresse des Gateways	Geben Sie eine gültige IPv4-Adresse an.

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Netzparameter des ausgewählten Geräts sind konfiguriert.

Um sicherzustellen, dass die Eigenschaft korrekt übernommen wurden, führen Sie erneut den Befehl `das discover interface` aus.

Weitere Hinweise

Sie zeigen die Netzwerkparameter mit dem Befehl `show das info` an.

4.5.2.4 das mac blink

Beschreibung

Mit diesem Befehl lassen Sie die Port-LEDs des ausgewählten Geräts blinken.

Voraussetzung

- Der Befehl `das discover interface` ist ausgeführt.
- Sie befinden sich im globalen Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
das mac <aa:aa:aa:aa:aa:aa> blink [timeout <seconds(5-60)>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
-	MAC-Adresse des erreichbaren Geräts	`aa:aa:aa:aa:aa:aa`
`timeout`	Schlüsselwort für die Blink-Dauer	-
`seconds`	Blink-Dauer in Sekunden	5 ... 60 Default: 5 Sekunden

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Port-LEDs des ausgewählten Geräts blinken. Wenn die Zeit (`timeout`) abgelaufen ist, wird das Blinken beendet.

4.5.2.5 das delete

Beschreibung

Mit diesem Befehl löschen Sie den Inhalt der Tabelle, in der die erreichbaren Geräte gespeichert sind.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
das delete {mac <aa:aa:aa:aa:aa:aa> | all }
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`mac`	Löscht das ausgewählte Gerät aus der Tabelle.	`aa:aa:aa:aa:aa:aa`
`all`	Löscht den Inhalt der ganzen Tabelle.	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Das ausgewählte Gerät oder der ganze Inhalt wurde aus der Tabelle entfernt.

4.6 SINEMA

4.6.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen allgemeine Systemeigenschaften angezeigt und konfiguriert werden können.

4.6.1.1 show sinema

Beschreibung

Dieser Befehl zeigt an, ob die SINEMA-Konfigurationsschnittstelle aktiviert oder deaktiviert ist.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show sinema
```

Ergebnis

Der Einstellung der SINEMA-Konfigurationsschnittstelle wird angezeigt.

4.6.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

4.6.2.1 sinema

Beschreibung

Mit diesem Befehl aktivieren Sie die SINEMA-Konfigurationsschnittstelle.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
sinema
```

Ergebnis

Die SINEMA-Konfigurationsschnittstelle ist aktiviert.

Weitere Hinweise

Sie deaktivieren die SINEMA-Konfigurationsschnittstelle mit dem Befehl `no sinema`.

Sie zeigen die Einstellung, ob die SINEMA-Konfigurationsschnittstelle aktiviert oder deaktiviert ist, mit dem Befehl `show sinema` an.

4.6.2.2 no sinema

Beschreibung

Mit diesem Befehl deaktivieren Sie die SINEMA-Konfigurationsschnittstelle.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no sinema
```

Ergebnis

Die SINEMA-Konfigurationsschnittstelle ist deaktiviert.

Weitere Hinweise

Sie aktivieren die SINEMA-Konfigurationsschnittstelle mit dem Befehl `sinema`.

Sie zeigen die Einstellung, ob die SINEMA-Konfigurationsschnittstelle aktiviert oder deaktiviert ist, mit dem Befehl `show sinema` an.

SCALANCE spezifische Funktionen 5

In diesem Abschnitt finden Sie die Kapitel, die SCALANCE-spezifische Funktionen beschreiben.

5.1 PLUG

Der C-PLUG bzw. KEY-PLUG speichert die Konfiguration eines Geräts und kann somit im Fall eines Geräteaustausches die Konfiguration des alten Geräts auf das neue Gerät übertragen.

Der KEY-PLUG enthält zusätzlich zur Konfiguration noch eine Lizenz, welche die Nutzung bestimmter Funktionen freischaltet.
In diesem Kapitel werden Befehle beschrieben, die für das Arbeiten mit dem C-PLUG bzw. KEY-PLUG relevant sind.

5.1.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

5.1.1.1 show plug

Beschreibung

Dieser Befehl zeigt die aktuellen Informationen des PLUG an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show plug
```

Ergebnis

Die aktuellen Informationen des PLUG werden angezeigt.

5.1.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

5.1.2.1 plug

Beschreibung

Mit diesem Befehl wechseln Sie in den Plug Konfigurationsmodus.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
plug
```

Ergebnis

Sie befinden sich jetzt im Plug Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-plug)#
```

Weitere Hinweise

Sie verlassen den Plug Konfigurationsmodus mit dem Befehl `end` oder `exit`.

5.1.3 Befehle im Plug Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im Plug Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl `plug` ein, um in diesen Modus zu wechseln.

- Wenn Sie den Plug Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den Plug Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im Plug Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

5.1.3.1 presetplug

Beschreibung

Mit diesem Befehl erstellen Sie einen PRESET-PLUG. Ein PRESET-PLUG enthält neben den Konfigurationsdaten auch die Firmwareversion des erstellenden Geräts. Der PRESET-PLUG ist schreibgeschützt.

Startet ein Gerät mit einem PRESET-PLUG, wird ein Up-/Downgrade der Firmware durchgeführt, wenn auf dem Gerät eine andere Firmwareversion vorhanden ist. Dies wird durch ein Blinken der roten F-LED angezeigt (Blinkintervall: 2Sek an/0.2Sek. aus). Danach wird das Gerät neu gestartet und die auf dem PRESET-PLUG gespeicherte Gerätekonfiguration, inkl. Benutzer und Zertifikate auf das Gerät überspielt.

Um den PLUG wieder beschreibbar zu machen rufen sie den Befehl `factoryclean` auf.

Voraussetzung

- Der PLUG ist formatiert.
- Auf dem PLUG ist eine Gerätekonfiguration vorhanden.
- Sie befinden sich im Plug Konfigurationsmodus.
  Die Eingabeaufforderung lautet:
  `cli(config-plug)#`

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
presetplug
```

Ergebnis

Die Firmware des ausführenden Geräts wird auf den PLUG geschrieben und der PLUG wird schreibgeschützt.

5.1.3.2 firmware-on-plug

Beschreibung

Mit diesem Befehl legen Sie fest, dass die Firmware auf dem PLUG gespeichert wird.

Voraussetzung

- Auf dem PLUG ist eine Gerätekonfiguration vorhanden.
- Sie befinden sich im Plug Konfigurationsmodus.
  Die Eingabeaufforderung lautet:
  `cli(config-plug)#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
firmware-on-plug
```

Ergebnis

Die Firmware ist auf dem PLUG gespeichert.

Beim Start des Geräts wird überprüft, ob die Version auf dem PLUG gültig ist und ob diese mit der Version auf dem Gerät übereinstimmt. Wenn das nicht der Fall ist, wird die Firmware auf dem Gerät installiert und danach neu gestartet. Damit können mit dem PLUG automatische Firmware-Updates/Downgrades durchgeführt werden.

Weitere Hinweise

Sie deaktivieren diese Einstellung mit dem Befehl `no firmware-on-plug`.

5.1.3.3 no firmware-on-plug

Beschreibung

Mit diesem Befehl deaktivieren Sie die Funktion. Die Firmware wird vom PLUG entfernt.

Voraussetzung

- Auf dem PLUG ist eine Gerätekonfiguration vorhanden.
- Sie befinden sich im Plug Konfigurationsmodus.
  Die Eingabeaufforderung lautet:
  `cli(config-plug)#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no firmware-on-plug
```

Ergebnis

Die Firmware ist vom PLUG entfernt.

5.1.3.4 factoryclean

Beschreibung

Mit diesem Befehl löschen Sie die Gerätekonfiguration, die auf dem PLUG gespeichert ist.

Voraussetzung

- Auf dem PLUG ist eine Gerätekonfiguration vorhanden.
- Sie befinden sich im Plug Konfigurationsmodus.
  Die Eingabeaufforderung lautet:
  `cli(config-plug)#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
factoryclean
```

Ergebnis

Die Gerätekonfiguration auf dem PLUG ist gelöscht.

5.1.3.5 write

Beschreibung

Mit diesem Befehl formatieren Sie den PLUG und kopieren die aktuelle Gerätekonfiguration darauf.

Voraussetzung

- Der PLUG ist formatiert.
- Sie befinden sich im Plug Konfigurationsmodus.
  Die Eingabeaufforderung lautet:
  `cli(config-plug)#`

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
write
```

Ergebnis

Die aktuelle Gerätekonfiguration ist auf den formatierten PLUG kopiert.

5.2 WBM

Sie können auf dem Gerät den Zugriff über das Web Based Management zeitlich beschränken. Wenn eine bestimmte Zeit keine Eingabe erfolgt, wird die WBM-Sitzung beendet.

In diesem Kapitel werden Befehle beschrieben, die für die Konfiguration dieser Eigenschaft relevant sind.

5.2.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

5.2.1.1 show web-session-timeout

Beschreibung

Dieser Befehl zeigt die Timeout-Einstellung für das WBM an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show web-session-timeout
```

Ergebnis

Die Timeout-Einstellung für das WBM wird angezeigt.

5.2.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

5.2.2.1 web-session-timeout

Beschreibung

Mit diesem Befehl aktivieren Sie das automatische Ausloggen und Sie konfigurieren die Timeout-Einstellung für das WBM.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
web-session-timeout [<seconds(60-3600)>]
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`seconds`	Zeit bis zum automatischen Ausloggen nach der letzten Eingabe in Sekunden	60 … 3600 Default: 900

Ergebnis

Die Zeitdauer ist konfiguriert und das automatische Ausloggen ist aktiviert.

Weitere Hinweise

Sie deaktivieren das automatische Ausloggen mit dem Befehl `no web-session-timeout`.

Sie zeigen die aktuelle Timeout-Einstellung mit dem Befehl `show web-session-timeout` an.

5.2.2.2 no web-session-timeout

Beschreibung

Mit diesem Befehl deaktivieren Sie das automatischen Ausloggen.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no web-session-timeout
```

Ergebnis

Das automatische Ausloggen ist deaktiviert.

Weitere Hinweise

Sie aktivieren das automatische Ausloggen mit dem Befehl `web-session-timeout`.

Sie zeigen die aktuelle Timeout-Einstellung mit dem Befehl `show web-session-timeout` an.

5.3 Digital Input/Output

Einleitung

Das SCALANCE S-Gerät verfügt über einen digitalen Ein- / Ausgang. Der Anschluss erfolgt über zwei 2-poligen Klemmenblöcke. Informationen zur Pin-Belegung finden Sie in der Betriebsanleitung des Geräts.

Mit CLI-Befehlen können Sie den digitalen Ausgang öffnen oder schließen.

Anwendungsbeispiele

- Digitaler Eingang, um eine einzelne Information zu melden, z. B. "Tür auf", "Tür zu"
- Digitaler Ausgang z. B. zum "Schlafenlegen" von Geräten auf einem fahrerlosen Transportsystem.

5.3.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

5.3.1.1 show digital input

Beschreibung

Dieser Befehl zeigt die aktuelle Einstellung des digitalen Eingangs an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

show digital output

Ergebnis

Die aktuelle Einstellung des digitalen Eingangs wird angezeigt.

5.3.1.2 show digital output

Beschreibung

Dieser Befehl zeigt die aktuelle Einstellung des digitalen Ausgangs an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

show digital output

Ergebnis

Die aktuelle Einstellung des digitalen Ausgangs wird angezeigt.

5.3.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

5.3.2.1 digital output closed

Beschreibung

Mit diesem Befehl wird der digitale Ausgang geschlossen.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
digital output close
```

Ergebnis

Der digitale Ausgang ist geschlossen.

Weitere Hinweise

Sie öffnen den digitalen Ausgang mit dem Befehl `digital output open`.

Sie zeigen die aktuelle Einstellung des digitalen Ausgangs mit dem Befehl `show digital output` an

5.3.2.2 digital output open

Beschreibung

Mit diesem Befehl wird der digitale Ausgang geöffnet.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
digital output open
```

Ergebnis

Der digitale Ausgang ist geöffnet.

Weitere Hinweise

Sie schließen den digitalen Ausgang mit dem Befehl `digital output close`.

Sie zeigen die aktuelle Einstellung des digitalen Ausgangs mit dem Befehl `show digital output` an

5.4 cRSP / SRS

In diesem Kapitel werden Befehle zu cRSP / SRS beschrieben.

Hinweis

Common Remote Service Platform (cRSP) / Siemens Remote Service (SRS) ist eine Fernwartungsplattform über die der Fernwartungszugriff durchgeführt wird.

Zur Nutzung der Plattform sind zusätzliche Serviceverträge notwendig und Randbedingungen zu beachten. Bei Interesse an cRSP / SRS wenden Sie sich an Ihren Siemens-Ansprechpartner vor Ort und besuchen Sie folgendeWebseite (https://support.industry.siemens.com/cs/de/de/sc/2281).

5.4.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

5.4.1.1 show srs

Beschreibung

Dieser Befehl zeigt an, ob die Nutzung von cRSP / SRS aktiviert ist und ob das Gerät das empfangene Serverzertifikat auf Gültigkeit prüft.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show srs
```

Ergebnis

Die Konfiguration wird angezeigt.

5.4.1.2 show srs logon

Beschreibung

Dieser Befehl zeigt die konfigurierten Zielserver des Common Remote Service Platform (cRSP) / Siemens Remote Service (SRS) an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show srs overview
```

Ergebnis

Die Konfiguration wird angezeigt.

5.4.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

5.4.2.1 srs

Beschreibung

Mit diesem Befehl wechseln Sie in den SRS-Konfigurationsmodus.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
srs
```

Ergebnis

Sie befinden sich jetzt im SRS-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-srs)#
```

Weitere Hinweise

Sie verlassen den SRS-Konfigurationsmodus mit dem Befehl `end` oder `exit`.

5.4.3 Befehle im SRS-Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im SRS-Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl `srs` ein, um in diesen Modus zu wechseln.

- Wenn Sie den SRS-Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den SRS-Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

5.4.3.1 logon

Beschreibung

Mit diesem Befehl legen Sie fest, welcher Zielserver verwendet wird.

Voraussetzung

Sie befinden sich im SRS-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-srs)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
logon {idx <num(1-20)> | all} {enabled|disabled}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`idx`	Schlüsselwort für die Nummer des Zielservers	-
`index`	Nummer, die einem bestimmten Zielserver entspricht.	Geben Sie die gewünschte Nummer an. 1 ... 20
`all`	Verwendet alle Zielserver	-
`enabled`	Aktiviert den Eintrag	-
`disabled`	Deaktiviert den Eintrag.	

Ergebnis

Der angegebene Zielserver ist aktiviert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show srs logon` an.

Sie deaktivieren den Zielserver dem Befehl `no logon`.

Sie zeigen die Nummern der Zielserver mit dem Befehl `logon show-idx` an.

5.4.3.2 no logon

Beschreibung

Mit diesem Befehl löschen Sie einen bestimmten Zielserver oder alle Zielserver.

Voraussetzung

Sie befinden sich im SRS-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-srs)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no logon {idx <num(1-20)> | all}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`idx`	Schlüsselwort für die Nummer des Zielservers	-
`num`	Nummer, die einem bestimmten Zielserver entspricht.	Geben Sie die gewünschte Nummer an.
`all`	Löscht alle Zielserver	-

Ergebnis

Der angegebene Zielserver-Eintrag ist gelöscht.

Weitere Hinweise

Sie zeigen die Nummern der Zielserver mit dem Befehl `logon show-idx` an.

5.4.3.3 logon idx authority

Beschreibung

Mit diesem Befehl konfigurieren Sie die Adresse eines bestimmten Zielservers.

Voraussetzung

Sie befinden sich im SRS-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-srs)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
logon idx <num(1-20)> authority <string(255)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`num`	Nummer, die einem bestimmten Zielserver entspricht.	Geben Sie die gewünschte Nummer an.
`string`	Adresse des Zielservers	Geben Sie die Adresse des Zielservers an.

Ergebnis

Die Adresse des Zielservers ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show srs logon` an.

Sie zeigen die Nummern des Eintrags mit dem Befehl `logon show-idx` an.

5.4.3.4 logon idx fragment

Beschreibung

Mit diesem Befehl können Sie lokale Teile der Ressource, z. B. das Anker-Attribut einer Webseite adressieren.

Voraussetzung

Sie befinden sich im SRS-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-srs)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
logon idx <num(1-20)> fragment <string(255)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`num`	Nummer, die einem bestimmten Zielserver entspricht.	Geben Sie die gewünschte Nummer an.
`string`	Teil der Ressource	Maximal 255 Zeichen

Ergebnis

Die Einstellung ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show srs logon` an.

Sie zeigen die Nummern der Zielserver mit dem Befehl `logon show-idx` an.

5.4.3.5 logon idx path

Beschreibung

Mit diesem Befehl legen Sie den Zielpfad zur Ressource fest.

Voraussetzung

Sie befinden sich im SRS-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-srs)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
logon idx <num(1-20)> path <string(255)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`num`	Nummer, die einem bestimmten Zielserver entspricht.	Geben Sie die gewünschte Nummer an.
`string`	Zielpfad zur Ressource	Maximal 255 Zeichen

Ergebnis

Die Einstellung ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show srs logon` an.

Sie zeigen die Nummern der Zielserver mit dem Befehl `logon show-idx` an.

5.4.3.6 logon idx query

Beschreibung

Mit diesem Befehl konfigurieren Sie Anfragen, die Parameterwerte für eine Anwendung enthalten können.

Voraussetzung

Sie befinden sich im SRS-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-srs)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
logon idx <num(1-20)> query <string(255)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`num`	Nummer, die einem bestimmten Zielserver entspricht.	Geben Sie die gewünschte Nummer an.
`string`	Anfrage	Maximal 255 Zeichen

Ergebnis

Die Einstellung ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show srs logon` an.

Sie zeigen die Nummern der Zielserver mit dem Befehl `logon show-idx` an.

5.4.3.7 logon show-idx

Beschreibung

Mit diesem Befehl zeigen Sie die verfügbaren Zielserver an.

Voraussetzung

Sie befinden sich im SRS-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-srs)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
logon show-idx
```

Ergebnis

Die Zielserver werden aufgelistet.

Weitere Hinweise

Sie erstellen einen Zielserver-Eintrag mit dem Befehl `logon addr`.

5.4.3.8 shutdown

Beschreibung

Mit diesem Befehl deaktivieren Sie die Nutzung von SRS.

Voraussetzung

Sie befinden sich im SRS-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-srs)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

shutdown

Ergebnis

Die Nutzung von SRS ist deaktiviert.

Weitere Hinweise

Sie aktivieren die Nutzung mit dem Befehl `no shutdown`.

5.4.3.9 no shutdown

Beschreibung

Mit diesem Befehl aktivieren Sie die Nutzung von SRS.

Voraussetzung

Sie befinden sich im SRS-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-srs)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no shutdown
```

Ergebnis

Die Nutzung von SRS ist aktiviert.

Weitere Hinweise

Sie deaktivieren die Nutzung mit dem Befehl `shutdown`.

5.4.3.10 interval

Beschreibung

Mit diesem Befehl konfigurieren Sie die Zeitspanne, nach der die IPv4-Adresse an den gewünschten Zielserver übertragen wird.

Voraussetzung

Sie befinden sich im SRS-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-srs)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
interval <time (60-86400)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`time`	Intervall in Sekunden	60 ... 86400

Ergebnis

Das Intervall ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show srs logon` an.

5.4.3.11 validate cert

Beschreibung

Mit diesem Befehl legen Sie fest, ob das Gerät das empfangene Serverzertifikat auf Gültigkeit überprüft.

Voraussetzung

Sie befinden sich im SRS-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-srs)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
validate cert {enabled|disabled}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung
`enabled`	Aktiviert die Überprüfung
`disabled`	Deaktiviert die Überprüfung

Ergebnis

Die Einstellung ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show srs` an.

5.5 SINEMA RC

5.5.1 Einleitung zum Kapitel SRC

In diesem Kapitel werden Befehle für den Zugriff zu SINEMA RC-Server beschrieben. Weiterführende Informationen dazu finden Sie in der Betriebsanleitung zum SINEMA RC-Server

5.5.2 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

5.5.2.1 show sinemarc

Hinweis

Dieser Befehl ist nur mit KEY PLUG verfügbar.

Beschreibung

Dieser Befehl zeigt Informationen zu SINEMA RC an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show sinemarc
```

Ergebnis

Die Informationen werden angezeigt.

5.5.3 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

5.5.3.1 sinemarc

Hinweis

Dieser Befehl ist nur mit KEY PLUG verfügbar.

Beschreibung

Mit diesem Befehl wechseln Sie in den SINEMARC-Konfigurationsmodus.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
sinemarc
```

Ergebnis

Sie befinden sich jetzt im SINEMARC-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-sinemarc)#
```

Weitere Hinweise

Sie verlassen den SINEMARC-Konfigurationsmodus mit dem Befehl `end` oder `exit`.

5.5.4 Befehl im SINEMARC-Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im SINEMARC-Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl sinemarc ein, um in diesen Modus zu wechseln.

- Wenn Sie den SINEMARC-Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den SINEMARC-Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

5.5.4.1 addr

Hinweis

Dieser Befehl ist nur mit KEY PLUG verfügbar.

Beschreibung

Mit diesem Befehl konfigurieren Sie die IPv4-Adresse oder den DNS-Hostnamen des SINEMA RC-Servers.

Voraussetzung

Sie befinden sich im SINEMARC-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-sinemarc)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
addr <ip_addr|dns(50)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`ip_addr`	IPv4-Adresse	Geben Sie die IPv4-Adresse des SINEMA RC-Servers an.
`dns`	DNS-Hostname	Geben Sie den DNS-Hostnamen des SINEMA RC-Servers an. Maximal 50 Zeichen

Ergebnis

Die IPv4-Adresse des SINEMA RC-Servers ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show sinemarc` an.

5.5.4.2 autoenrollment interval

Hinweis

Dieser Befehl ist nur mit KEY PLUG verfügbar.

Beschreibung

Mit diesem Befehl legen Sie das Intervall fest, nach dem Anfragen an den SINEMA RC Server gesendet werden. Mit dieser Anfrage prüft das Gerät, ob auf dem SINEMA RC Server eine neuere Firmware-Datei vorhanden ist oder ob sich die Verbindungseinstellungen geändert haben.

Voraussetzung

Sie befinden sich im SINEMARC-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-sinemarc)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
autoenrollment interval {0 | <minute(10-10080)>}
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`0`	Intervall	Die Anfrage wird nie gesendet.
`minute`		Geben Sie das Intervall in Minunten an. 10 ... 10080

Ergebnis

Das Intervall ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show sinemarc` an.

5.5.4.3 autofwnat

Hinweis

Dieser Befehl ist nur mit KEY PLUG verfügbar.

Beschreibung

Mit diesem Befehl aktivieren Sie das automatische Anlegen der Firewall- und NAT-Regeln für die Verbindung zum SINEMA RC-Server.

Voraussetzung

Sie befinden sich im SINEMARC-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-sinemarc)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
autofwnat
```

Ergebnis

Die automatischen Firewall- und NAT-Regeln werden erstellt. Dabei werden die Verbindungen, die zwischen den projektierten exportierten Subnetzen und den Subnetzen, die über den SINEMA RC-Server erreichbar sind, zugelassen. Die NAT-Einstellungen werden wie im SINEMA RC-Server projektiert umgesetzt.

Weitere Hinweise

Sie aktivieren die Einstellung mit dem Befehl `autofwnat`.

Sie deaktivieren die Einstellung mit dem Befehl `no autofwnat`.

5.5.4.4 connection type

Hinweis

Dieser Befehl ist nur mit KEY PLUG verfügbar.

Beschreibung

Mit diesem Befehl legen Sie fest, wie die Verbindung aufgebaut wird.

Voraussetzung

Sie befinden sich im SINEMARC-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-sinemarc)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
connection type {auto|permanent|di|sms|di-sms}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`auto`	Das Gerät übernimmt die Einstellungen des SINEMA RC Server. Die Einstellungen auf dem SINEMA RC Server konfigurieren Sie unter "Fernverbindungen > Geräte". Weiterführende Informationen hierzu finden Sie in der Betriebsanleitung "SINEMA RC Server".	-
`permanent`	Die Einstellungen des SINEMA RC-Servers werden ignoriert. Das Gerät baut eine VPN-Verbindung zum SINEMA RC-Server. Der VPN-Tunnel wird permanent aufrechterhalten	-
`di`	Die Einstellungen des SINEMA RC-Servers werden ignoriert. Beim Eintreten des Ereignisses "Digital In" versucht das Gerät zum SINEMA RC-Server eine VPN-Verbindung aufzubauen. Vorausgesetzt ist, dass das Ereignis "Digital In" an die VPN-Verbindung weitergegeben wird. Dazu aktivieren Sie unter "System > Events > Configuration" beim Ereignis "Digital In" "VPN Tunnel".	-

Parameter	Beschreibung	Wertebereich/Anmerkung
`sms`	Nur bei M87x Die Einstellungen des SINEMA RC-Servers werden ignoriert. Wenn das Gerät eine Befehl-SMS (Wake-up SMS) erhält, versucht das Gerät zum SINEMA RC-Server aufzubauen. Vorausgesetzt unter "System > SMS > SMS Command" ist festgelegt, von wem eine Befehl-SMS der Klasse "System" akzeptiert wird.	-
di-sms	Nur bei M87x Die Einstellungen des SINEMA RC-Servers werden ignoriert. Wenn das Ereignis "Digital In" eintritt oder wenn das Gerät eine Befehl-SMS erhält, versucht das Gerät eine VPN-Verbindung zum SINEMA RC-Server aufzubauen	-

Ergebnis

Die Einstellung ist konfiguriert

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show sinemarc` an.

5.5.4.5 no autofwnat

Hinweis

Dieser Befehl ist nur mit KEY PLUG verfügbar.

Beschreibung

Mit diesem Befehl deaktivieren Sie die Firewall- und NAT-Regeln.

Voraussetzung

Sie befinden sich im SINEMARC-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-sinemarc)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
autofwnat
```

Ergebnis

Die Firewall- und NAT-Regeln sind deaktiviert.

Weitere Hinweise

Sie aktivieren die Einstellung mit dem Befehl `autofwnat`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show sinemarc` an.

5.5.4.6 device id

Hinweis

Dieser Befehl ist nur mit KEY PLUG verfügbar.

Beschreibung

Mit diesem Befehl konfigurieren Sie die Geräte-ID. Die Geräte-ID wird beim Konfigurieren des Geräts am SINEMA RC-Server vergeben. Weiterführende Informationen dazu finden Sie in der Betriebsanleitung zum SINEMA RC-Server

Voraussetzung

Sie befinden sich im SINEMARC-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-sinemarc)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
device id <number>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`number`	Geräte-ID	Geben Sie die Geräte-ID an.

Ergebnis

Die Geräte-ID ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show sinemarc` an.

5.5.4.7 device pw

Hinweis

Dieser Befehl ist nur mit KEY PLUG verfügbar.

Beschreibung

Mit diesem Befehl konfigurieren Sie das Passwort, mit dem sich das Gerät am SINEMA RC-Server anmeldet. Das Passwort wird beim Konfigurieren des Geräts am SINEMA RC-Server vergeben. Weiterführende Informationen dazu finden Sie in der Betriebsanleitung zum SINEMA RC-Server.

Voraussetzung

Sie befinden sich im SINEMARC-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-sinemarc)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
device pw <password(256)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
password	Gerätepasswort	Geben Sie das Passwort an. Maximal 256 Zeichen

Ergebnis

Das Gerätepasswort ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show sinemarc` an.

5.5.4.8 port

Hinweis

Dieser Befehl ist nur mit KEY PLUG verfügbar.

Beschreibung

Mit diesem Befehl stellen Sie den Port ein, über den das WBM des SINEMA RC-Servers erreichbar ist.

Voraussetzung

Sie befinden sich im SINEMARC-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-sinemarc)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
port <number(1-65535)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
number	Portnummer	Geben Sie den Port an. 1 ... 65535

Ergebnis

Der Port ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show sinemarc` an.

5.5.4.9 proxy

Hinweis

Dieser Befehl ist nur mit KEY PLUG verfügbar.

Beschreibung

Mit diesem Befehl legen Sie fest, dass die Verbindung zu dem definierten SINEMA RC-Server über einen Proxy-Server aufgebaut wird.

Voraussetzung

- Der Proxy-Server ist konfiguriert.
- Sie befinden sich im SINEMARC-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-sinemarc)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
proxy <string(128)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`string`	Proxy-Servername	Geben Sie den Proxy-Servernamen an. Maximal 128 Zeichen

Ergebnis

Der Proxy-Server, über den die Verbindung aufgebaut wird, ist konfiguriert.

Weitere Hinweise

Sie entfernen den Proxy-Server mit dem Befehl `no proxy`.

Sie zeigen die verfügbaren Proxy-Servernamen mit dem Befehl `srv show-names` an.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show sinemarc` an.

5.5.4.10 no proxy

Hinweis

Dieser Befehl ist nur mit KEY PLUG verfügbar.

Beschreibung

Mit diesem Befehl entfernen Sie den Proxy-Server.

Voraussetzung

Sie befinden sich im SINEMARC-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-sinemarc)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no proxy
```

Ergebnis

Der Proxy-Server ist entfernt.

Weitere Hinweise

Sie konfigurieren den Proxy-Server mit dem Befehl `proxy`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show sinemarc` an.

5.5.4.11 shutdown

Hinweis

Dieser Befehl ist nur mit KEY PLUG verfügbar.

Beschreibung

Mit diesem Befehl deaktivieren Sie die Verbindung zum konfigurierten SINEMA RC-Server.

Voraussetzung

Sie befinden sich im SINEMARC-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-sinemarc)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
shutdown
```

Ergebnis

Die Verbindung zum SRC-Server ist beendet.

Weitere Hinweise

Sie aktivieren die Verbindung mit dem Befehl `no shutdown`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show sinemarc` an.

5.5.4.12 no shutdown

Hinweis

Dieser Befehl ist nur mit KEY PLUG verfügbar.

Beschreibung

Mit diesem Befehl bauen Sie eine Verbindung zum konfigurierten SINEMA RC-Server auf.

Voraussetzung

Sie befinden sich im SINEMARC-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-sinemarc)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no shutdown
```

Ergebnis

Die Verbindung ist aktiviert.

Weitere Hinweise

Sie deaktivieren die Verbindung mit dem Befehl `shutdown`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show sinemarc` an.

5.5.4.13 verification cacert

Hinweis

Dieser Befehl ist nur mit KEY PLUG verfügbar.

Beschreibung

Mit diesem Befehl legen Sie das CA-Zertifikat des Servers fest, das zur Signierung des Serverzertifikats verwendet wird.

Voraussetzung

- Das Zertifikat ist geladen.
- Sie befinden sich im SINEMARC-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-sinemarc)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
verification cacert [<name(256)>]
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`name`	Name des Serverzertifikats	Geben Sie den Namen des Serverzertifikats an. Maximal 256 Zeichen.

Ergebnis

Das CA-Zertifikat des Servers ist konfiguriert.

Weitere Hinweise

Sie laden Zertifikate mit dem Befehl `tftp load` an.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show sinemarc` an.

5.5.4.14 verification fingerprint

Hinweis

Dieser Befehl ist nur mit KEY PLUG verfügbar.

Beschreibung

Mit diesem Befehl konfigurieren Sie den Fingerabdruck des Geräts. Der Fingerabdruck wird bei der Inbetriebnahme des SINEMA RC-Servers vergeben. Weiterführende Informationen dazu finden Sie in der Betriebsanleitung zum SINEMA RC-Server.

Voraussetzung

Sie befinden sich im SINEMARC-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-sinemarc)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
verification fingerprint [<string(95)>]
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`string`	Fingerabdruck des Geräts	Geben Sie den Fingerabdruck des Geräts an. Maximal 95 Zeichen

Ergebnis

Der Fingerabdruck ist konfiguriert. Anhand des Fingerabdrucks überprüft das Gerät, ob es sich den korrekten SINEMA RC-Servers handelt.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show sinemarc` an.

5.6 SELECT/SET-Taster

In diesem Kapitel werden Befehle beschrieben, die für das Arbeiten mit dem Taster relevant sind.

Eine detaillierte Beschreibung der Funktion, die über den Taster bedient werden kann, finden Sie in der Betriebsanleitung des Geräts.

5.6.1 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

5.6.1.1 panel-button control-restart

Beschreibung

Mit diesem Befehl aktivieren Sie folgende Funktionen des SET-Tasters:

- Neustart: Diese Funktion entspricht dem Aufruf des Befehls `restart` .
- Zurücksetzen auf Werkseinstellungen: Diese Funktion entspricht dem Aufruf des Befehls `restart` mit dem Parameter `factory`.

Eine detaillierte Beschreibung der Funktionen, finden Sie in der Betriebsanleitung des Geräts.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet :

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
panel-button control-restart
```

Ergebnis

Die Funktionen des SET-Tasters sind aktiviert.

Weitere Hinweise

Sie deaktivieren diese Funktionen mit dem Befehl `no panel-button control-restart`.

5.6.1.2 no panel-button control-restart

Beschreibung

Mit diesem Befehl deaktivieren Sie die Funktionen des SET-Tasters. Der SET-Taster kann nicht zum Neustart oder zum Zurücksetzen auf Werkseinstellungen verwendet werden.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet :

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no panel-button control-restart
```

Ergebnis

Die Funktionen des SET-Tasters sind deaktiviert.

Weitere Hinweise

Sie aktivieren diese Funktionen mit dem Befehl `panel-button control-restart`.

Systemzeit 6

In diesem Abschnitt finden Sie die Kapitel, die den Bezug und die Einstellung der Systemuhrzeit beschreiben.

6.1 System Time Setting

In diesem Kapitel werden Befehle beschrieben, die für die Konfiguration der Systemuhrzeit relevant sind.

6.1.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

6.1.1.1 show dst info

Beschreibung

Dieser Befehl zeigt die im Gerät gespeicherten Einträge für die Sommerzeit an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show dst info
```

Ergebnis

Die Einträge für die Sommerzeit werden angezeigt.

6.1.1.2 show time

Beschreibung

Dieser Befehl zeigt die Einstellungen für die Systemuhr an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show time
```

Ergebnis

Die Einstellungen für die Systemuhr werden angezeigt.

6.1.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

6.1.2.1 time

Beschreibung

Mit diesem Befehl konfigurieren Sie den Bezug der Systemuhrzeit.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
time { manual | ntp | sntp | sinec }
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung
`manual`	Die Systemuhrzeit wird vom Anwender eingegeben.
`ntp`	Die Systemuhrzeit wird vom NTP-Server bezogen.
`sntp`	Die Systemuhrzeit wird vom SNTP-Server bezogen.
`sinec`	Die Systemuhrzeit wird über den SIMATIC Time Client bezogen.

Ergebnis

Der Bezug der Systemuhrzeit ist konfiguriert.

Weitere Hinweise

Sie zeigen die Einstellungen für die Systemuhr mit dem Befehl `show time` an.

Sie stellen die Systemuhrzeit mit dem Befehl `time set`.

6.1.2.2 time dst date

Beschreibung

Mit diesem Befehl konfigurieren Sie den Beginn und das Ende der Sommerzeit.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
time dst date <name(16)> <year (1900-2099)> begin <MMDDhh> end <MMDDhh>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`name`	Bezeichnung des Eintrags	maximal 16 Zeichen
`year`	Jahr	1900 ... 2099
`begin`	Schlüsselwort für den Beginn der Sommerzeit.	-
`MMDDhh`	Zeitpunkt für den Beginn der Sommerzeit.	Zeitpunkt im Format `MM` Monat `DD` Tag `hh` Stunde
`end`	Schlüsselwort für das Ende der Sommerzeit.	-
`MMDDhh`	Zeitpunkt für das Ende der Sommerzeit.	Zeitpunkt im Format `MM` Monat `DD` Tag `hh` Stunde

Ergebnis

Ein Eintrag für den Beginn und das Ende der Sommerzeit wurde erstellt.

Weitere Hinweise

Sie zeigen die Einstellungen für die Umstellung der Sommerzeit mit dem Befehl `show dst info` an.

6.1.2.3 time dst recurring

Beschreibung

Mit diesem Befehl konfigurieren Sie den Beginn und das Ende der Sommerzeit durch eine generische Beschreibung.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
time dst recurring <name(16)> begin {<week(1-5)> | last} <weekday> <month> <hour> end
{<week(1-5)> | last} <weekday> <month> <hour>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`name`	Bezeichnung des Eintrags	maximal 16 Zeichen
`begin`	Schlüsselwort für den Beginn der Sommerzeit.	-
`week`	Kalenderwoche in einem Monat	1 ... 5
`last`	Schlüsselwort für die letzte Kalenderwoche in einem Monat	-
`weekday`	Wochentag	monday, tuesday, wednesday, thursday, friday, saturday, sunday
`month`	Monat	january, february, march, april, may, june, july, august, september, october, november, december
`hour`	Stunde	0 ... 23
`end`	Schlüsselwort für das Ende der Sommerzeit.	-

Ergebnis

Ein Eintrag für den Beginn und das Ende der Sommerzeit wurde erstellt.

Weitere Hinweise

Sie zeigen die Einstellungen für die Umstellung der Sommerzeit mit dem Befehl `show dst info` an.

6.1.2.4 no time dst

Beschreibung

Mit diesem Befehl löschen Sie den Eintrag für Beginn und Ende der Sommerzeit mit dem angegebenen Namen. Wenn Sie keinen Namen als Parameter angeben, werden alle Einträge gelöscht.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no time dst [<name(16)>]
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`name`	Bezeichnung des Eintrags	maximal 16 Zeichen

Ergebnis

Ein Eintrag oder die Einträge für Beginn und Ende der Sommerzeit wurde gelöscht.

Weitere Hinweise

Sie zeigen die Einstellungen für die Umstellung der Sommerzeit mit dem Befehl `show dst info` an.

6.1.2.5 time set

Beschreibung

Mit diesem Befehl stellen Sie die Systemuhrzeit.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
time set hh:mm:ss <day (1-31)>
{january|february|march|april|may|june|july|august|september|october|november|decembe
r}
<year (2000 - 2035)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`hh:mm:ss`	Uhrzeit	Stunde, Minute, Sekunde jeweils durch ":" getrennt
`day`	Tag des Monats	1 ... 31
-	Monat	january, february, march, april, may, june, july, august, september, october, november, december
`year`	Jahr	2000 ... 2035

Ergebnis

Die Systemuhrzeit ist eingestellt.

Weitere Hinweise

Sie zeigen die Einstellungen für die Systemuhr mit dem Befehl `show time` an.

6.2 NTP Client

In diesem Kapitel werden Befehle beschrieben, die für die Konfiguration des NTP-Clients relevant sind.

6.2.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

6.2.1.1 show ntp info

Beschreibung

Dieser Befehl zeigt die aktuellen Einstellungen für das Network Time Protocol (NTP) an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show ntp info
```

Ergebnis

Die aktuellen NTP-Einstellungen werden angezeigt.

6.2.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

6.2.2.1 ntp

Beschreibung

Mit diesem Befehl wechseln Sie in den Konfigurationsmodus des Network Time Protocol (NTP).

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
ntp
```

Ergebnis

Sie befinden sich jetzt im NTP Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ntp)#
```

Weitere Hinweise

Sie verlassen den NTP Konfigurationsmodus mit dem Befehl `end` oder `exit`.

6.2.3 Befehle im NTP Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im NTP Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl `ntp` ein, um in diesen Modus zu wechseln.

- Wenn Sie den NTP Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den NTP Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im NTP Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

6.2.3.1 ntp server id

Beschreibung

Mit diesem Befehl konfigurieren Sie auf dem NTP-Client die Verbindung zu einem Server.

Voraussetzung

Sie befinden sich im NTP Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ntp)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ntp server id <1-3> { ipv4 <ip_addr> | fqdn-name <Fully Qualified Domain Name> }
[port { <1025-36564> | default}] [poll <seconds(64-1024)>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`id`	Nummer des NTP-Servers	1 ... 3
`ipv4`	Schlüsselwort für eine IPv4-Adresse	-
`ip_addr`	Wert für die IPv4-Adresse des Zeitservers	Geben Sie eine gültige IPv4-Adresse an.
`fqdn-name`	Schlüsselwort für einen Domainnamen	-
`FQDN`	Domainname (Fully Qualified Domain Name)	Maximal 100 Zeichen Wenn Sie einen entsprechenden Domainnamen hinterlegt haben, können Sie einen Hostnamen angeben.

Parameter	Beschreibung	Wertebereich/Anmerkung
`port`	UDP-Port des Zeitservers	1025 … 36564
`default`	Defaultwert für den UDP-Port	123
`poll`	Schlüsselwort für die Zeitspanne, nach der die Uhrzeit wieder angefordert wird	-
`seconds`	Wert für die Zeitspanne in Sekunden	64 … 2592000

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Adressen und Schnittstellenbezeichnungen (Seite 42)".

Ergebnis

Die Verbindung zu einem Server ist auf dem NTP-Client konfiguriert.

Weitere Hinweise

Sie löschen die Verbindung zu einem Server mit dem Befehl `no ntp server id`.

Sie hinterlegen einen Domainnamen mit dem Befehl `ip domain name` oder `domain name`.

6.2.3.2 no ntp server id

Beschreibung

Mit diesem Befehl löschen Sie die Verbindung zu einem Server auf einem NTP-Client.

Voraussetzung

Sie befinden sich im NTP Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ntp)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no ntp server id <1-3>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`id`	Nummer des NTP-Servers	1 ... 3

Ergebnis

Die Verbindung zu einem Server ist auf dem NTP-Client gelöscht.

Weitere Hinweise

Sie konfigurieren die Verbindung zu einem Server mit dem Befehl `ntp server id`.

6.2.3.3 ntp server secure

Beschreibung

Mit diesem Befehl konfigurieren Sie die Parameter für die Authentifizierung.

Voraussetzung

Sie befinden sich im NTP Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ntp)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ntp server id <1-3> secure [ntpkeyid <1-65534>] [hashalg {des-cbc|md5|sha1}] [ntp-key
<secret-key-string(1-128)>]
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`id`	NTP-Serverindex, auf den sich die Parameter beziehen	1 ... 3
`secure`	Schlüsselwort für die Authentifizierung	-
`keyid`	ID des Authentifizierungsschlüssels	Auf dem NTP-Server muss der Eintrag vorhanden sein. 1 ... 65534
`hashalg`	Format des Authentifizierungsschlüssel	des-cbc md5 sha1
`ntp-key`	Schlüsselwort für den Authentifizierungsschlüssel	-
`secret-key-string`	Authentifizierungsschlüssel	Die Eingabe muss mit dem auf dem NTP-Server hinterlegten Schlüssel übereinstimmen.

Ergebnis

Die Parameter sind konfiguriert.

Weitere Hinweise

Sie zeigen die Einstellungen und weitere Informationen mit dem Befehl `show ntp server`.

6.2.3.4 ntp secure

Beschreibung

Mit diesem Befehl aktivieren Sie die Funktion "Nur NTP-Client (gesichert)". Das Gerät erhält die Systemzeit von einem Secure NTP-Server.

Voraussetzung

- Sie befinden sich im NTP Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-ntp)#
  ```

- Die Parameter für die Authentifizierung (Schlüssel-ID, Hash-Algorithmus, Schlüssel) sind konfiguriert.

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ntp secure
```

Ergebnis

Die Funktion ist aktiviert.

Weitere Hinweise

Sie deaktivieren die Funktion mit dem Befehl `no ntp secure`.

Sie konfigurieren die Parameter für die Authentifizierung mit dem Befehl `ntp server id`.

6.2.3.5 no ntp secure

Beschreibung

Mit diesem Befehl deaktivieren Sie die Funktion "Nur NTP-Client (gesichert)".

Voraussetzung

Sie befinden sich im NTP Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ntp)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no ntp secure
```

Ergebnis

Die Funktion ist deaktiviert.

Weitere Hinweise

Sie aktivieren die Funktion mit dem Befehl `ntp secure`.

6.2.3.6 ntp time diff

Beschreibung

Mit diesem Befehl konfigurieren Sie die Zeitdifferenz zwischen dem Gerät und dem NTP-Server.

Voraussetzung

Sie befinden sich im NTP Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ntp)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ntp time diff <(+/-hh:mm)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung
+	Zeitzonen westlich der NTP-Server-Zeitzone
-	Zeitzonen östlich der NTP-Server-Zeitzone
hh	Stundenzahl der Differenz
mm	Minutenzahl der Differenz

Geben Sie die Stundenzahl und die Minutenzahl jeweils mit zwei Ziffern ein.

Default: keine Zeitdifferenz.

Ergebnis

Die Zeitdifferenz zwischen dem Gerät und dem NTP-Server ist konfiguriert.

6.3 NTP-Server

In diesem Kapitel werden Befehle beschrieben, die für die Konfiguration des NTP-Servers relevant sind.

6.3.1 show ntp server info

Beschreibung

Dieser Befehl zeigt die aktuellen Einstellungen für NTP-Server an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show ntp server info
```

Ergebnis

Die aktuellen NTP-Server-Einstellungen werden angezeigt.

6.3.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

6.3.2.1 ntp server

Beschreibung

Mit diesem Befehl aktivieren Sie den Dienst NTP-Server.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
ntp server
```

Ergebnis

Der Dienst NTP-Server ist konfiguriert.

Weitere Hinweise

Sie deaktivieren Sie den Dienst mit mit dem Befehl `no ntp server`.

6.3.2.2 no ntp server

Beschreibung

Mit diesem Befehl deaktivieren Sie den Dienst NTP-Server.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no ntp server
```

Ergebnis

Der Dienst NTP-Server ist deaktiviert.

Weitere Hinweise

Sie aktivieren Sie den Dienst mit mit dem Befehl `ntp server`.

6.3.3 Befehle im NTP Server Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im NTP-Server Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl `ntp server configuration` ein, um in diesen Modus zu wechseln.

- Wenn Sie den NTP-Server Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den NTP-Server Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

6.3.3.1 ntp server interface

Beschreibung

Mit diesem Befehl aktivieren Sie den NTP-Server an der gewünschten Schnittstelle. Über diese Schnittstellen können die anderen Geräte die bereitgestellte Zeit abrufen.

Voraussetzung

Sie befinden sich im NTP-Server Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ntp-server)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ntp server interface { <interface-type> <interface-id> | vlan <vlan-id(1-4094)> | all
}
[port {<1025-36564> | default}][secure ntpkeyid <1-65534> hashalg {des-cbc|md5|sha1}
ntp-key <secret-key-string(1-128)>]
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstelle	
`vlan`	Schlüsselwort für eine VLAN-Verbindung	-
`vlan-id`	Nummer des angesprochenen VLAN	1 ... 4094
`all`	Aktiviert auf allen verfügbaren Schnittstellen die Funktion	-
`port`	Port des NTP-Servers	• 1025 ... 36564 • default (123)
`secure`	Die folgenden Parameter sind nur für "NTP (secure)" von Bedeutung.	-
`ntpkeyid`	ID des Authentifizierungsschlüssels	1 ... 65534
`hashalg`	Hash-Algorithmust für den Authentifizierungs-schlüssel	• des-cbc • md5 • sha1
`ntp-key`	Schlüsselwort für Authentifizierungsschlüssel	-
`secret-key-string`	Authentifizierungsschlüssel	Die Länge des Authentifizie-rungsschlüssels ist abhängig vom Hash-Algorithmus. • DES: ASCII 8 Zeichen • MD5: ASCII 16 ... 128 Zeichen • SHA1: ASCII 20 ... 128 Zeichen

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Schnittstellen sind festgelegt, über welche die anderen Geräte die aktuelle Uhrzeit abrufen können.

Weitere Hinweise

Sie zeigen die Einstellungen und weitere Informationen mit dem Befehl `show ntp server info`.

Sie deaktivieren Sie die Funktion mit dem Befehl `no ntp server interface`.

Sie aktivieren "NTP (secure)" mit dem Befehl `ntp server secure interface`.

6.3.3.2 no ntp server interface

Beschreibung

Mit diesem Befehl deaktivieren Sie die Funktion an der Schnittstelle.

Voraussetzung

Sie befinden sich im NTP-Server Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ntp-server)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no ntp server interface {<interface-type> <interface-id> | vlan <vlan-id(1-4094)>}
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstelle	
`vlan`	Schlüsselwort für eine VLAN-Verbindung	-
`vlan-id`	Nummer des angesprochenen VLAN	1 ... 4094

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Funktion an den Schnittstellen ist deaktiviert.

Weitere Hinweise

Sie zeigen die Einstellungen und weitere Informationen mit dem Befehl `show ntp server info`.

Sie aktivieren Sie die Funktion mit dem Befehl `ntp server interface`.

6.3.3.3 ntp server secure interface

Beschreibung

Mit diesem Befehl wird aus dem NTP-Server ein NTP-Server vom Typ "NTP (secure)".

Voraussetzung

Sie befinden sich im NTP-Server Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ntp-server)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ntp server secure interface { vlan <vlan-id(1-4094)> | all }
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstelle	
`vlan`	Schlüsselwort für eine VLAN-Verbindung	-
`vlan-id`	Nummer des angesprochenen VLAN	1 ... 4094
`all`	Aktiviert auf allen verfügbaren Schnittstellen die Funktion	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Der NTP-Server vom Typ "NTP (secure)" ist aktiviert.

Weitere Hinweise

Sie zeigen die Einstellungen und weitere Informationen mit dem Befehl `show ntp server info`.

Sie deaktivieren Sie die Funktion mit dem Befehl `no ntp server secure interface`.

6.3.3.4 no ntp server secure interface

Beschreibung

Mit diesem Befehl deaktivieren Sie NTP (secure).

Voraussetzung

Sie befinden sich im NTP-Server Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ntp-server)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ntp server secure interface {<interface-type> <interface-id> | vlan <vlan-id(1-4094)>}
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstelle	
`vlan`	Schlüsselwort für eine VLAN-Verbindung	-
`vlan-id`	Nummer des angesprochenen VLAN	1 ... 4094

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Funktion an den Schnittstellen ist deaktiviert.

Weitere Hinweise

Sie zeigen die Einstellungen und weitere Informationen mit dem Befehl `show ntp server info`.

Sie aktivieren Sie die Funktion mit dem Befehl `ntp server secure interface`.

6.4 SNTP Client

In diesem Kapitel werden Befehle beschrieben, die für die Konfiguration des SNTP-Client relevant sind.

6.4.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

6.4.1.1 show sntp broadcast-mode status

Beschreibung

Dieser Befehl zeigt die aktuelle Konfiguration des Broadcast-Modus des SNTP an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show sntp broadcast-mode status
```

Ergebnis

Die aktuelle SNTP-Broadcast-Konfiguration wird angezeigt.

6.4.1.2 show sntp status

Beschreibung

Dieser Befehl zeigt die Einstellungen des Simple Network Time Protocol an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show sntp status
```

Ergebnis

Die Einstellungen des SNTP werden angezeigt.

6.4.1.3 show sntp unicast-mode status

Beschreibung

Dieser Befehl zeigt die aktuelle Konfiguration des Unicast-Modus des SNTP an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show sntp unicast-mode status
```

Ergebnis

Die aktuelle SNTP-Unicast-Konfiguration wird angezeigt.

6.4.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

6.4.2.1 sntp

Beschreibung

Mit diesem Befehl wechseln Sie in den SNTP Konfigurationsmodus.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
sntp
```

Ergebnis

Sie befinden sich jetzt im SNTP Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-sntp)#
```

Weitere Hinweise

Sie verlassen den SNTP Konfigurationsmodus mit dem Befehl `end` oder `exit`.

6.4.3 Befehle im SNTP Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im SNTP Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl `sntp` ein, um in diesen Modus zu wechseln.

- Wenn Sie den SNTP Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den SNTP Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im SNTP Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

6.4.3.1 sntp time diff

Beschreibung

Mit diesem Befehl konfigurieren Sie die Zeitdifferenz der Systemuhrzeit relativ zur UTC-Zeit.

Voraussetzung

- Sie befinden sich im SNTP Konfigurationsmodus.
  Die Eingabeaufforderung lautet:
  `cli(config-sntp)#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
sntp time diff <(+/-hh:mm)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung
`+`	Zeitzonen westlich der SNTP-Server-Zeitzone
`-`	Zeitzonen östlich der SNTP-Server-Zeitzone
`hh`	Stundenzahl der Differenz
`mm`	Minutenzahl der Differenz

Geben Sie die Zeitdifferenz folgendermaßen an:

- mit Vorzeichen
- ohne Leerzeichen
- Stunden und Minuten jeweils zweistellig (mit führender Null)

Default: keine Zeitdifferenz

Ergebnis

Die Zeitzone der Systemuhrzeit ist konfiguriert.

Weitere Hinweise

Sie zeigen die Einstellungen dieser Funktion und weitere Informationen mit dem Befehl `show sntp status` an.

6.4.3.2 sntp unicast-server

Beschreibung

Mit diesem Befehl konfigurieren Sie einen SNTP-Unicast-Server.

Voraussetzung

- Der Adressierungsmodus des SNTP-Client ist als "unicast" konfiguriert.
- Sie befinden sich im SNTP Konfigurationsmodus.
  Die Eingabeaufforderung lautet:
  `cli(config-sntp)#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
sntp unicast-server { ipv4 <ucast_addr> | fqdn-name <Fully Qualified Domain
Name(100)> | ipv6 <ip6_addr> }
 [port <(1025-36564)>] [poll <seconds(16-16284)>] [secondary]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ipv4`	Schlüsselwort für eine IP-Adresse	-
`ucast_addr`	Wert für eine IPv4-Unicast-Adresse	Geben Sie eine gültige IPv4-Unicast-Adresse an.
`fqdn-name`	Schlüsselwort für einen Domainnamen	-
`Fully Qualified Domain Name`	Domainname	Maximal 100 Zeichen
`ipv6`	Schlüsselwort für eine IPv6-Adresse	-
`ip6_addr`	Wert für die IPv6-Adresse des Zeitservers	Geben Sie eine gültige IPv6-Adresse an.
`port`	UDP Port des Time Servers	1025 … 36564 Default: 123
`poll`	Schlüsselwort für die Zeitspanne, nach der die Uhrzeit wieder angefordert wird	-

Parameter	Beschreibung	Wertebereich/Anmerkung
`seconds`	Wert für die Zeitspanne in Sekunden	16 ... 16284
`secondary`	Schlüsselwort, um den zweiten SNTP-Server zu hinterlegen	Wenn Sie diesen Parameter nicht angeben, wird der erste SNTP-Server hinterlegt.

Ergebnis

Der SNTP-Unicast-Server ist konfiguriert.

Weitere Hinweise

Sie setzen die Einstellung mit dem Befehl `no sntp unicast-server` auf den voreingestellten Wert zurück.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show sntp unicast-mode status` an.

6.4.3.3 no sntp unicast-server

Beschreibung

Mit diesem Befehl löschen Sie die Attribute für einen SNTP-Unicast-Server und setzen die Adresse zurück.

Voraussetzung

Sie befinden sich im SNTP Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-sntp)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no sntp unicast-server {ipv4 <ucast_addr> | fqdn-name <Fully Qualified Domain
Name(100)> | ipv6 <ip6_addr>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ipv4`	Schlüsselwort für eine IP-Adresse	-
`ucast_addr`	Wert für eine IPv4-Unicast-Adresse	Geben Sie eine gültige IPv4-Unicast-Adresse an
`fqdn-name`	Schlüsselwort für einen Domainnamen	-
`Fully Qualified Domain Name(100)`	Domainname (Fully Qualified Domain Name)	Maximal 100 Zeichen

Parameter	Beschreibung	Wertebereich/Anmerkung
`ipv6`	Schlüsselwort für eine IPv6-Adresse	-
`ip6_addr`	Wert für die IPv6-Adresse des Zeitservers	Geben Sie eine gültige IPv6-Adresse an.

Ergebnis

Der SNTP-Unicast-Server ist auf den voreingestellten Wert zurückgesetzt.

Weitere Hinweise

Sie konfigurieren die Einstellung mit dem Befehl `sntp unicast-server`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show sntp unicast-mode status` an.

6.4.3.4 sntp client addressing-mode

Beschreibung

Mit diesem Befehl konfigurieren Sie den Adressierungsmodus des SNTP-Clients als Unicast oder Broadcast.

Voraussetzung

- Der SNTP-Client ist aktiviert.
- Sie befinden sich im SNTP Konfigurationsmodus.
  Die Eingabeaufforderung lautet:
  `cli(config-sntp)#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
sntp client addressing-mode{unicast|broadcast}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`unicast`	konfiguriert den SNTP-Client im Unicast-Modus	Default: Unicast aktiviert
`broadcast`	konfiguriert den SNTP-Client im Broadcast-Modus	Unterstützt nur IPv4-Adressen

Ergebnis

Der Adressierungsmodus des SNTP-Client ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show sntp status` an.

Sie zeigen die Einstellungen für den Unicast-Modus mit dem Befehl `show sntp unicast-mode status` an.

Sie zeigen die Einstellungen für den Broadcast-Modus mit dem Befehl `show sntp broadcast-mode status` an.

Netzstrukturen 7

7.1 VLAN

In diesem Kapitel werden Befehle zum Konfigurieren und Kontrollieren von virtuellen Netzen (VLANs) beschrieben.

7.1.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

7.1.1.1 show vlan

Beschreibung

Dieser Befehl zeigt die spezifischen Informationen für alle oder für ein ausgewähltes VLAN an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show vlan [brief | id <vlan-range> | summary]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`brief`	zeigt eine kurze Information über alle VLANs an	-
`id`	Schlüsselwort für ein VLAN oder einen VLAN-Bereich	-

Parameter	Beschreibung	Wertebereich/Anmerkung
`vlan-range`	Nummer des angesprochenen VLAN oder VLAN-Bereichs	1 ... 4094 Geben Sie die Bereichsgrenzen mit einem Bindestrich ohne Leerzeichen ein.
`summary`	zeigt eine Zusammenfassung der VLANs an	

Wenn Sie keinen Parameter aus der Parameterliste auswählen, werden die Einträge aller Schnittstellen angezeigt.

Ergebnis

Die Informationen für das gewählte VLAN werden angezeigt.

7.1.1.2 show vlan device info

Beschreibung

Dieser Befehl zeigt alle globalen Informationen an, die für alle VLANs gültig sind.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show vlan device info
```

Ergebnis

Die globalen Informationen werden angezeigt.

7.1.1.3 show vlan learning params

Beschreibung

Dieser Befehl zeigt die Parameter für das automatische Lernen von Adressen für ausgewählte oder alle VLANs (aktive und inaktive VLANs) an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgenden Parametern auf:

```
show vlan learning params [vlan <vlan-range>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vlan`	Schlüsselwort für ein VLAN oder einen VLAN-Bereich	-
`vlan-range`	Nummer des angesprochenen VLAN oder VLAN-Bereichs	1 ... 4094 Geben Sie die Bereichsgrenzen mit einem Bindestrich ohne Leerzeichen ein.

Wenn Sie keinen Parameter aus der Parameterliste auswählen, werden die Einträge aller Schnittstellen angezeigt.

Ergebnis

Die Einstellungen für das automatische Lernen von Adressen werden angezeigt.

7.1.1.4 show vlan port config

Beschreibung

Dieser Befehl zeigt die VLAN spezifischen Informationen für Ports an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show vlan port config [{port <interface-type> <interface-id>}]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`port`	Schlüsselwort für einen Port	-
`interface-type`	Typ der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstelle	

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Wenn Sie keinen Parameter aus der Parameterliste auswählen, werden die Einträge aller Schnittstellen angezeigt.

Ergebnis

Die Informationen der Ports werden angezeigt.

7.1.1.5 show vlan protocols-group

Beschreibung

Dieser Befehl zeigt die Tabelle mit den Protokollgruppen-Einträgen an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show vlan protocols-group
```

Ergebnis

Die Tabelle der Protokollgruppen wird angezeigt.

7.1.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

7.1.2.1 base bridge-mode

Beschreibung

Mit diesem Befehl konfigurieren Sie, ob das Gerät Telegramme mit VLAN-Tags transparent weiterleitet (IEEE 802.1D/VLAN-unaware-Modus) oder VLAN-Informationen berücksichtigt (IEEE 802.1Q/VLAN-aware-Modus).

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgenden Parametern auf:

```
base bridge-mode {dot1d-bridge|dot1q-vlan}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkungen
`dot1d-bridge`	Stellt bei dem Gerät den Modus "VLAN-unaware" ein. VLAN-Tags werden nicht berücksichtigt bzw. verändert, sondern transparent weitergeleitet.	-
`dot1q-vlan`	Stellt bei dem Gerät den Modus "VLAN-aware" ein. VLAN-Informationen werden berücksichtigt.	-

Ergebnis

Der Gerätemodus ist konfiguriert.

Weitere Hinweise

Sie zeigen den Status dieser Funktion und weitere VLAN-Informationen mit dem Befehl `show vlan device info`.

7.1.2.2 interface range

Beschreibung

Mit diesem Befehl können Sie mehrere Schnittstellen oder die Schnittstellen von VLANs zusammenfassen und gemeinsam konfigurieren. Die Konfigurationen sind für alle Schnittstellen des angegebenen Bereiches gültig.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
interface range
(
  {<interface-type> <0/a-b,0/c,...>}
  {vlan <vlan-id(1-4094)> - <vlan-id(2-4094)>}
)
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`interface-type`	Schlüsselwort für eine Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`0/a-b, 0/c,...`	Modul-Nr. und Port-Nr. der Schnittstelle	
`vlan`	Schlüsselwort für eine VLAN-Verbindung	-
`vlan-id`	Nummer des angesprochenen VLAN	1 ... 4094
`vlan-id`	Nummer des angesprochenen VLAN	2 ... 4094

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Wenn Sie mit diesem Befehl mehrere VLANs ansprechen wollen, müssen Sie vor und nach dem Bindestrich ein Leerzeichen einfügen, z. B. `interface range vlan 5 - 10`.

Ergebnis

Die Schnittstellen oder Schnittstellen von VLANs wurden zu einem Schnittstellenbereich zusammengefasst.

Die Eingabeaufforderung lautet:

```
cli(config-if-vlan-range)#
```

Die Konfigurationsbefehle, die Sie in deinem Modus eingeben, gelten für alle Schnittstellen dieses Bereichs.

Weitere Hinweise

Mit dem Befehl `no interface range` entfernen Sie VLANs aus diesem Bereich oder lösen ihn auf.

7.1.2.3 no interface range

Beschreibung

Mit diesem Befehl entfernen Sie die Schnittstellen oder Schnittstellen von VLANs aus dem Schnittstellenbereich oder lösen ihn auf, wenn Sie alle zuvor hinzugefügten Schnittstellen entfernen.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no interface range vlan <vlan-id(1-4094)> - <vlan-id(2-4094)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vlan`	Schlüsselwort für eine VLAN-Verbindung	-
`vlan-id`	Nummer des angesprochenen VLAN	1 ... 4094
`vlan-id`	Nummer des angesprochenen VLAN	2 ... 4094

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Wenn Sie mehrere VLANs ansprechen, müssen Sie vor und nach dem Bindestrich ein Leerzeichen einfügen, z. B. `no interface range vlan 5 - 10`.

Ergebnis

Die VLANs aus dem angegebenen Schnittstellenbereich wurden entfernt.

Weitere Hinweise

Mit dem Befehl `interface range` können Sie mehrere Schnittstellen oder VLANs zur gemeinsamen Konfiguration zusammenfassen.

7.1.2.4 map protocol

Beschreibung

Mit diesem Befehl weisen Sie ein Protokoll einer Protokollgruppe zu.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgenden Parametern auf:

```
map protocol
   {ip | ipv6 | novell | netbios | appletalk | other <aa:aa>}
   enet-v2 protocols-group <group-id (1-100)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ip`	Internet Protokoll v4	`HEX 08:00`
`ipv6`	Internet Protokoll v6	`HEX 86:dd`
`novell`	Novell Netware Protokoll	`HEX 81:38`
`netbios`	Netbios über TCP/IP	`HEX f0:f0`
`appletalk`	Appletalk	`HEX 80:9b`
`other`	Anderes Protokoll.	geben Sie den hexidezimalen Protokollwert ein. • other: `aa:aa` • IPV6: `86:DD` • LLDP: `88:CC` • PTP IEEE1588: `88:F7` • EAP (802.1X): `88:8E`
`enet-v2`	Framestruktur ist Ethernet II	-

Parameter	Beschreibung	Wertebereich/Anmerkung
`protocols-group`	Schlüsselwort für eine Protokollgruppe	-
`group-id`	Nummer der Gruppe	dezimal 1 ... 100

Ergebnis

Die Protokollgruppe ist angelegt.

Weitere Hinweise

Sie löschen die Protokollgruppe mit dem Befehl `no map protocol`.

Sie zeigen den Status dieser Funktion und weitere Informationen mit dem Befehl `show vlan protocols-group` an.

7.1.2.5 no map protocol

Beschreibung

Mit diesem Befehl löschen Sie ein Protokoll aus allen Protokollgruppen.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgenden Parametern auf:

```
no map protocol
   {ip | ipv6 | novell | netbios | appletalk | other <aa:aa>}
   enet-v2
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ip`	Internet Protokoll v4	`HEX 08:00`
`ipv6`	Internet Protokoll v6	`HEX 86:dd`
`novell`	Novell Netware Protokoll	`HEX 81:38`
`netbios`	Netbios über TCP/IP	`HEX f0:f0`
`appletalk`	Appletalk	`HEX 80:9b`

Parameter	Beschreibung	Wertebereich/Anmerkung
`other`	Anderes Protokoll.	geben Sie den hexidezimalen Protokollwert ein. • other: `aa:aa` • IPV6: `86:DD` • LLDP: `88:CC` • PTP IEEE1588: `88:F7` • EAP (802.1X): `88:8E`
`enet-v2`	Framestruktur ist Ethernet II	-

Ergebnis

Das Protokoll ist aus allen Protokollgruppen entfernt.

Weitere Hinweise

Sie legen die Protokollgruppe mit dem Befehl `map protocol` an.

Sie zeigen den Status dieser Funktion und weitere Informationen mit dem Befehl `show vlan protocols-group` an.

7.1.2.6 no protocol-vlan

Beschreibung

Mit diesem Befehl deaktivieren Sie die protokollbasierte Klassifizierung auf allen Schnittstellen.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no protocol-vlan
```

Ergebnis

Die Klassifizierung ist deaktiviert.

Weitere Hinweise

Sie aktivieren die Einstellung mit dem Befehl `protocol-vlan`.

Sie zeigen den Status dieser Funktion und weitere Informationen mit dem Befehl `show vlan device info` an.

7.1.2.7 protocol-vlan

Beschreibung

Mit diesem Befehl aktivieren Sie die protokollbasierte Klassifizierung auf allen Schnittstellen.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
protocol-vlan
```

Ergebnis

Die Klassifizierung ist aktiviert.

Weitere Hinweise

Sie deaktivieren die Einstellung mit dem Befehl `no protocol-vlan`.

Sie zeigen den Status dieser Funktion und weitere Informationen mit dem Befehl `show vlan device info` an.

7.1.2.8 subnet-vlan

Beschreibung

Mit diesem Befehl aktivieren Sie IPv4-Subnetz-basiertes VLAN auf allen Schnittstellen.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
subnet-vlan
```

Ergebnis

Die Klassifizierung ist aktiviert.

Weitere Hinweise

Sie deaktivieren die Einstellung mit dem Befehl `no subnet-vlan`.

Sie zeigen den Status dieser Funktion und weitere Informationen mit dem Befehl `show vlan device info` an.

Sie konfigurieren IPv4-Subnetz-basiertes VLAN mit dem Befehl `map subnet`.

7.1.2.9 no subnet-vlan

Beschreibung

Mit diesem Befehl deaktivieren Sie IPv4-Subnetz-basiertes VLAN auf allen Schnittstellen.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no subnet-vlan
```

Ergebnis

Die Einstellunge ist deaktiviert.

Weitere Hinweise

Sie aktivieren die Einstellung mit dem Befehl `subnet-vlan`.

Sie zeigen den Status dieser Funktion und weitere Informationen mit dem Befehl `show vlan device info` an.

7.1.2.10 vlan

Beschreibung

Mit diesem Befehl legen Sie ein VLAN auf dem Gerät an und wechseln in den VLAN Konfigurationsmodus.

Hinweis

Das Gerät unterstützt bis zu 16 virtuelle Netze.

Im Provider Backbone Bridge Modus werden mit diesem Befehl Anwender-, Service und Backbone-VLANs erstellt.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
vlan <vlan-id(1-4094)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vlan-id`	Nummer des angesprochenen VLAN	1 ... 4094

Geben Sie bei der Nummer des VLANs keine führenden Nullen an.

Ergebnis

Das VLAN ist angelegt.

Sie befinden sich jetzt im VLAN Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-vlan-$$$)#
```

Weitere Hinweise

Sie löschen das VLAN mit dem Befehl `no vlan`.

Sie zeigen die Informationen zum VLAN mit dem Befehl `show vlan` an.

7.1.2.11 no vlan

Beschreibung

Mit diesem Befehl löschen Sie ein VLAN auf dem Gerät.

Voraussetzung

- Das VLAN darf keinem physikalischen Port zugewiesen sein.
- Sie befinden sich im globalen Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config)#
  ```

Syntax

Rufen Sie den Befehl mit folgendem Parameter auf:

```
no vlan <vlan-id(1-4094)>
```

Parameter	Beschreibung	Wertebereich/Anmerkung
`vlan-id`	Nummer des angesprochenen VLAN	1 ... 4094

Das VLAN mit der Nummer 1 kann nicht gelöscht werden.

Ergebnis

Das VLAN ist gelöscht

Weitere Hinweise

Sie legen ein VLAN auf dem Gerät mit dem Befehl `vlan` an.

Sie zeigen die Informationen zum VLAN mit dem Befehl `show vlan` an.

7.1.3 Befehle im Interface Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im Interface Konfigurationsmodus aufrufen können. Abhängig von der eingestellten Schnittstelle sind verschiedene Befehlssätze verfügbar.

Geben Sie im globalen Konfigurationsmodus den Befehl `interface` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im Interface Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

- Wenn Sie den Interface Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den Interface Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im Interface Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

Diese Befehle sind im Interface Konfigurationsmodus der Ethernet-Schnittstellen verfügbar. Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

7.1.3.1 mtu

Beschreibung

Mit diesem Befehl konfigurieren Sie die Größe der Maximum Transmission Unit (MTU) für eine VLAN-Schnittstelle.

Voraussetzung

- Die Schnittstelle muss heruntergefahren sein.
- Sie befinden sich im Interface Konfigurationsmodus.
- Die Eingabeaufforderung lautet:
  `cli(config-if-$$$)#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
mtu <frame-size(90-1500)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`frame-size`	Größe der MTU in Byte	90 ... 1500 Default: 1500

Ergebnis

Die Einstellung für die Größe der MTU ist konfiguriert.

Weitere Hinweise

Sie fahren die Schnittstelle mit dem Befehl `shutdown` herunter.

Sie zeigen diese Einstellung mit dem Befehl `show interface mtu` an.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show interfaces` an.

7.1.3.2 shutdown complete

Beschreibung

Mit diesem Befehl schalten Sie die Schnittstelle ab.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
shutdown complete
```

Ergebnis

Die Schnittstelle ist abgeschaltet. Bei einem abgeschalteten Switch-Port wird weiterhin eine Verbindung angezeigt. Die LED für den Portstatus blinkt zyklisch 3 mal. Allerdings werden keine Daten gesendet oder empfangen.

Weitere Hinweise

Sie schalten die Schnittstelle mit dem Befehl `no shutdown` ein.

Sie zeigen den Status dieser Funktion und weitere Informationen mit dem Befehl `show interfaces` an.

7.1.3.3 no shutdown

Beschreibung

Mit diesem Befehl schalten Sie eine Schnittstelle ein.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no shutdown
```

Ergebnis

Die Schnittstelle ist angeschaltet.

Weitere Hinweise

Sie schalten die Schnittstelle mit dem Befehl `shutdown` aus.

Sie zeigen den Status dieser Funktion und weitere Informationen mit dem Befehl `show interfaces` an.

7.1.3.4 switchport acceptable-frame-type

Beschreibung

Mit diesem Befehl konfigurieren Sie, welche Typen von Frames die Schnittstelle akzeptiert.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgenden Parametern auf:

```
switchport acceptable-frame-type{all|tagged}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung
`all`	alle Frames (mit und ohne VLAN Variable) werden akzeptiert
`tagged`	es werden nur Frames mit VLAN Variablen akzeptiert

Bei Systemstart bzw. bei Verwendung des Befehls `restart` mit der Option `memory` oder `factory` gelten folgende Voreinstellungen:

- Die Funktion ist auf `all` konfiguriert.

Ergebnis

Die Einstellung ist aktiviert.

Weitere Hinweise

Sie zeigen den Status dieser Funktion und weitere Informationen mit dem Befehl `show vlan port config` an.

7.1.3.5 no switchport acceptable-frame-type

Beschreibung

Mit diesem Befehl setzen Sie die Einstellung, welche Arten von Telegrammen die Schnittstelle akzeptiert, auf den voreingestellten Wert zurück.

Der voreingestellte Wert ist `all`.

Die Schnittstelle akzeptiert tagged und untagged Frames.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no switchport acceptable-frame-type
```

Ergebnis

Die Einstellung wurde auf den voreingestellten Wert zurückgesetzt.

Weitere Hinweise

Sie konfigurieren die Einstellung mit dem Befehl `switchport acceptable-frame-type`.

Sie zeigen den Status dieser Funktion und weitere Informationen mit dem Befehl `show vlan port config` an.

7.1.3.6 switchport ingress-filter

Beschreibung

Der Ingress-Filter überprüft bei ankommenden Paketen, ob der Port, auf dem das Paket empfangen wurde, dem sendenden VLAN zugeordnet ist. Wenn das nicht der Fall ist, wird das Paket nicht bearbeitet.

Mit diesem Befehl aktivieren Sie den Ingress-Filter.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
switchport ingress-filter
```

Ergebnis

Der Ingress-Filter ist aktiviert.

Weitere Hinweise

Sie deaktivieren den Filter mit dem Befehl `no switchport ingress-filter`.

Sie zeigen den Status des Ingress-Filters und weitere Einstellungen mit dem Befehl `show vlan port config` an.

7.1.3.7 no switchport ingress-filter

Beschreibung

Mit diesem Befehl deaktivieren Sie den Ingress-Filter.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no switchport ingress-filter
```

Ergebnis

Der Ingress-Filter ist deaktiviert.

Weitere Hinweise

Sie aktivieren den Filter mit dem Befehl `switchport ingress-filter`.

Sie zeigen den Status des Ingress-Filters und weitere Einstellungen mit dem Befehl `show vlan port config` an.

7.1.3.8 switchport mode

Beschreibung

Mit diesem Befehl legen Sie den Betriebsmodus für den Switch-Port fest.

Voraussetzung

- Die Schnittstelle ist als Switch-Port konfiguriert.
- Sie befinden sich im Interface Konfigurationsmodus.
  Die Eingabeaufforderung lautet:
  `cli(config-if-$$$)#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
switchport mode { trunk | hybrid }
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`trunk`	Konfiguriert den Port als Trunk-Port, der nur getaggte Telegramme weiterleitet. Der Port kann nur dann zum Trunk-Port konfiguriert werden, wenn der Port in keinem VLAN eingetragen ist, das ungetaggte Telegramme austauscht. Damit der Trunk-Port die getaggten Telegramme weiterleitet, müssen alle VLAN-IDs hinterlegt werden, an die der Trunk-Port die Telegramme weiterleiten soll. Wenn ein VLAN neu erstellt wird, wird die VLAN-ID automatisch am Trunk-Port eingetragen. Bei einem Trunk-Port erfolgt die VLAN-Zuordnung dynamisch. Statische Konfigurationen können nur durchgeführt werden, wenn der Port zusätzlich zur Eigenschaft Trunk-Port noch statisch als Member in den betreffenden VLANs eingetragen wird. Ein Beispiel für eine statische Konfiguration ist das Zuweisen von Multicastgruppen in bestimmten VLANs. Wenn Sie den Befehl "`acceptable frame-type all`" am Trunk-Port ausführen, empfängt der Port auch ungetaggte Telegramme.	-
`hybrid`	Konfiguriert den Port als Hybrid-Port, der getaggte und ungetaggte Telegramme akzeptiert.	Default: `hybrid`

Ergebnis

Der Betriebsmodus ist konfiguriert.

Weitere Hinweise

Sie setzen die Betriebsart mit Befehl `no switchport mode` auf den voreingestellten Wert zurück.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show vlan port config` an.

Sie konfigurieren die Schnittstelle mit dem Befehl `switchport` als Switch-Port.

7.1.3.9 no switchport mode

Beschreibung

Mit diesem Befehl setzen Sie den Betriebsmodus für den Switch-Port auf den voreingestellten Wert zurück.

Der voreingestellte Wert ist Hybrid.

Voraussetzung

- Die Schnittstelle ist als Switch-Port konfiguriert.
- Sie befinden sich im Interface Konfigurationsmodus.
  Die Eingabeaufforderung lautet:
  `cli(config-if-$$$)#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no switchport mode
```

Ergebnis

Die Einstellung ist auf den voreingestellten Wert zurückgesetzt.

Weitere Hinweise

Sie konfigurieren den Betriebsmodus mit dem Befehl `switchport mode`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show vlan port config` an.

Sie konfigurieren die Schnittstelle mit dem Befehl `switchport` als Switch-Port.

7.1.3.10 switchport priority default

Beschreibung

Mit diesem Befehl konfigurieren Sie die Standardpriorität für die Schnittstelle.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
switchport priority default <(0-7)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
-	Wert für die Standardpriorität	0 ... 7 Default: 0

Ergebnis

Die Einstellung für die Standardpriorität der Schnittstelle ist konfiguriert.

Weitere Hinweise

Sie setzen die Standardpriorität mit dem Befehl `no switchport priority default` auf den voreingestellten Wert zurück.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show vlan port config` an.

7.1.3.11 no switchport priority default

Beschreibung

Mit diesem Befehl setzen Sie die Standardpriorität für die Schnittstelle auf den voreingestellten Wert zurück.

Der voreingestellte Wert ist 0.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no switchport priority default
```

Ergebnis

Die Einstellung ist auf den voreingestellten Wert zurückgesetzt.

Weitere Hinweise

Sie konfigurieren die Standardpriorität mit dem Befehl `switchport priority default`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show vlan port config` an.

7.1.3.12 switchport pvid

Beschreibung

Mit diesem Befehl weisen Sie eine Schnittstelle einem VLAN zu und konfigurieren den Port VLAN Identifier (PVID) dafür. Wenn ein empfangenes Telegramm kein VLAN-Tag hat, so wird es um ein Tag mit der hier angegebenen VLAN-ID ergänzt und entsprechend den Regeln am Port gesendet.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
switchport pvid <vlan-id(1-4094)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vlan-id`	Nummer des angesprochenen VLAN	1 ... 4094

Ergebnis

Der PVID ist konfiguriert

Weitere Hinweise

Sie setzen die Einstellung mit dem Befehl `no switchport pvid` auf den voreingestellten Wert zurück.

Sie konfigurieren die VLAN-ID mit dem Befehl `switchport access vlan`.

Sie zeigen die Einstellung und weitere Informationen mit dem Befehl `show vlan port config` an.

7.1.3.13 no switchport pvid

Beschreibung

Mit diesem Befehl setzen Sie die Einstellung für den Port VLAN Identifier (PVID) für eine Schnittstelle auf den voreingestellten Wert zurück.

Der voreingestellte Wert ist 1.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no switchport pvid
```

Ergebnis

Die Einstellung ist auf den voreingestellten Wert zurückgesetzt.

Weitere Hinweise

Sie konfigurieren die Einstellung mit dem Befehl `switchport pvid`.

Sie konfigurieren die VLAN-ID mit dem Befehl `switchport access vlan`.

Sie zeigen den Status dieser Funktion und weitere Informationen mit dem Befehl `show vlan port config` an.

7.1.4 Befehle im VLAN Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im VLAN Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl `vlan $$$` ein, um in diesen Modus zu wechseln. Dabei müssen Sie den Platzhalter `$$$` durch die entsprechende VLAN-ID ersetzen.

Befehle zu anderen Themen, die im VLAN Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

- Wenn Sie den VLAN Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den VLAN Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im VLAN Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

7.1.4.1 ip address

Beschreibung

Mit diesem Befehl vergeben Sie eine IP-Adresse.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus von VLAN.

Die Eingabeaufforderung lautet:

```
cli(config-if-vlan-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ip address <ip-address> {<subnet-mask>| / <prefix-length(0-32)>}
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ip-address`	IP-Adresse	Geben Sie eine gültige IP-Adresse an.
`subnet-mask`	Subnetzmaske	Geben Sie eine gültige Subnetz-maske an.
`prefix-length`	Dezimale Darstellung der Maske als Anzahl der "1" Bits	0 ... 32

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die IP-Adresse ist vergeben.

Hinweis

Wirksamkeit des Befehls

Dieser Befehl wird sofort wirksam. Wenn Sie die Schnittstelle konfigurieren, über die Sie auf das Gerät zugreifen, geht die Verbindung verloren!

Weitere Hinweise

Sie löschen die Einstellung mit dem Befehl `no ip address`.

7.1.4.2 no ip address

Beschreibung

Mit diesem Befehl löschen Sie die Zuweisung einer IP-Adresse und deaktivieren DHCP.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus von VLAN.

Die Eingabeaufforderung lautet:

```
cli(config-if-vlan-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no ip address [{ <ucast_addr> | dhcp }]
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ucast-addr`	Wert für eine IPv4-Unicast-Adresse	Geben Sie eine gültige IPv4-Unicast-Adresse an.
`dhcp`	Geben sie diesen Parameter an, wenn sie explizit die DHCP-Funktion deaktivieren wollen.	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

War DHCP auf diesem Interface aktiviert, so ist DHCP nun deaktiviert. Eine eventuell vorhandene dynamisch gelernte IP-Adresse wird automatisch in eine statische IP-Adresse umgewandelt.

Waren statische IP-Adressen konfiguriert und wurde keine explizite IP-Adresse als Parameter übergeben, so werden alle statischen IP-Adressen von diesem Interface gelöscht.

Wurde explizit eine statische IP-Adresse angegeben, so wird diese Adresse von diesem Interface gelöscht.

Hinweis

Wirksamkeit des Befehls

Dieser Befehl wird sofort wirksam.

Wenn Sie die Schnittstelle konfigurieren, über die Sie auf das Gerät zugreifen, können Sie die Verbindung verlieren!

Weitere Hinweise

Sie vergeben eine IP-Adresse mit dem Befehl `ip address` bzw. `ip address dhcp`.

7.1.4.3 name

Beschreibung

Mit diesem Befehl weisen Sie dem VLAN einen Namen zu.

Voraussetzung

Sie befinden sich im VLAN Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-vlan-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
name <vlan-name>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vlan-name`	Name der dem VLAN zugewiesen wird	max. 32 Zeichen

Ergebnis

Dem VLAN ist ein Name zugewiesen.

Weitere Hinweise

Sie löschen die Namenszuweisung für ein VLAN mit dem Befehl `no name`.

7.1.4.4 no name

Beschreibung

Mit diesem Befehl löschen Sie die Namenszuweisung für ein VLAN.

Voraussetzung

Sie befinden sich im VLAN Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-vlan-$$$)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no name
```

Ergebnis

Der Name des VLAN ist gelöscht.

Weitere Hinweise

Sie weisen dem VLAN einen Namen mit dem Befehl `name` zu.

7.1.4.5 ports

Beschreibung

Mit diesem Befehl erzeugen Sie eine Liste, die das Verhalten der Schnittstellen festlegt und die vorhandene VLAN-Konfiguration ersetzt.

- Member Ports (Tagged Ports)

  Die Schnittstelle wird in die Liste der ein- und ausgehenden Verbindung permanent hinzugefügt. Übertragen werden getaggte und ungetaggte Telegramme.

- Untagged Ports
  Die Schnittstelle überträgt ungetaggte Telegramme. Bei gesetzter VLAN-ID (PVID) werden die eingehenden ungetaggten Telegramme um ein Tag mit der dort angegebenen VLAN-ID ergänzt. Wenn die empfangenen Telegramme bereits eine VLAN-ID enthalten, werden nur die Telegramme akzeptiert, deren VLAN-ID der gesetzten PVID entspricht. Bei ausgehenden Telegrammen wird der Tag mit der VLAN-ID entfernt.

- Forbidden Ports
  Diese Schnittstelle wird nicht für die Kommunikation in einem VLAN verwendet.

Der "Tagged Port" und der "Untagged Port", die Sie mit diesem Befehl festlegen, werden für den ausgehenden Datenverkehr verwendet.

Voraussetzung

Sie befinden sich im VLAN Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-vlan-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgenden Parametern auf:

```
ports
   (
    [<interface-type><0/a-b,0/c,...>]
    [<interface-type><0/a-b,0/c,...>]
    )
   [
    untagged<interface-type> <0/a-b,0/c,...>
    (
     [<interface-type><0/a-b,0/c,...>]     [all]
    )
   ]
   [
    forbidden<interface-type><0/a-b,0/c,...>
    [<interface-type><0/a-b,0/c,...>]
       ]
   [name<vlan-name>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Werte
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`0/a-b,0/c,...`	a-b und c: Platzhalter für numerische Bezeichnung der Schnittstelle	
`untagged`	Schlüsselwort für Schnittstellen oder Ports, die Datenpakete ohne VLAN Markierung übertragen	-
`all`	gibt an, dass alle Schnittstellen oder Ports auf "untagged" gesetzt werden	-
`forbidden`	Schlüsselwort für gesperrte Schnittstellen oder Ports	-
`name`	Schlüsselwort für die Namenszuweisung	-
`vlan-name`	Name des VLANs	max. 32 Zeichen

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Einstellungen sind aktiviert.

Weitere Hinweise

Sie zeigen die Einstellungen der Funktion mit dem Befehl `show vlan` an.

Sie setzen die Einstellungen mit Befehl `no ports` zurück.

7.1.4.6 no ports

Beschreibung

Mit diesem Befehl setzen Sie Ports für ein VLAN zurück.

Voraussetzung

Sie befinden sich im VLAN Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-vlan-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgenden Parametern auf:

```
no ports
    [<interface-type> <0/a-b,0/c,...>]
```

```
 [<interface-type> <0/a-b,0/c,...>]    [all]
[
 untagged ([<interface-type> <0/a-b,0/c,...>]
   [<interface-type> <0/a-b,0/c,...>]     [all])
]
[
 forbidden ([<interface-type> <0/a-b,0/c,...>
   [<interface-type> <0/a-b,0/c,...>]     [all])
]
[name <vlan-name>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`/a-b,0/c,...`	Port-Nr. der Schnittstelle	
`untagged`	Schlüsselwort für Schnittstellen oder Ports, die Datenpakete ohne VLAN-Markierung übertragen	-
`all`	gibt an, dass alle Schnittstellen oder Ports auf "untagged" gesetzt werden	-
`forbidden`	Schlüsselwort für gesperrte Schnittstellen oder Ports	-
`name`	Schlüsselwort für die Namenszuweisung	-
`vlan-name`	Name des VLANs	max. 32 Zeichen

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Ports sind zurückgesetzt.

Weitere Hinweise

Sie zeigen die Einstellungen der Funktion mit dem Befehl `show vlan` an.

Sie setzen die Einstellung mit dem Befehl `no ports` zurück.

7.1.4.7 tia interface

Beschreibung

Mit diesem Befehl aktivieren bzw. deaktivieren Sie die Eigenschaft TIA-Schnittstelle. Über die TIA-Schnittstelle wird definiert, auf welchem VLAN die PROFINET Funktionalitäten zur Verfügung stehen. Dies betrifft hauptsächlich die Gerätesuche mit oder über DCP.

Voraussetzung

- Die Schnittstelle ist aktiviert.
- Sie befinden sich im Interfaces Konfigurationsmodus der VLAN Schnittstelle:
  Die Eingabeaufforderung lautet:
  `cli (config-if-vlan-$$$) #`

  $$$ bezeichnet die Nummerierung der Schnittstelle

Syntax

Rufen Sie den Befehl ohne Parameter auf:
`tia-interface`

Ergebnis

Die Eigenschaft TIA-Schnittstelle ist exklusiv für das angegebene VLAN aktiviert. Die Funktion wurde auf den übrigen Schnittstellen deaktiviert.

Weitere Hinweise

Beachten Sie, dass nur jeweils eine VLAN-Schnittstelle zur TIA-Schnittstelle werden kann.

7.2 PPP

In diesem Kapitel werden Befehle beschrieben, die für das Verbinden mit dem WAN relevant sind.

7.2.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

7.2.1.1 show ppp information

Beschreibung

Dieser Befehl zeigt die Einstellungen und den Status von PPP an.

Voraussetzung

Sie befinden sich jetzt im Interface Konfigurationsmodus xDSL.

Die Eingabeaufforderung lautet:

```
CLI(config-ppp-X)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show ppp information
```

Ergebnis

Die Informationen werden angezeigt.

7.2.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

7.2.2.1 interface ppp

Beschreibung

Mit diesem Befehl wechseln Sie in den Interface Konfigurationsmodus.

Dort bearbeiten Sie die Einstellungen für jeweils eine Schnittstelle. Sie wählen die Schnittstelle durch die Parametrierung dieses Befehls aus. Die Bezeichnung der ausgewählten Schnittstelle wird in der Eingabeaufforderung angezeigt.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
interface ppp <interface-id>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Werte
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstelle	Geben Sie eine gültige Schnittstelle an.

Ergebnis

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ppp-$)#
```

Dabei ist der Platzhalter `$` durch folgende Modul-Nr. und Port-Nr. der Schnittstelle ersetzt:

Weitere Hinweise

Sie verlassen den Interface Konfigurationsmodus mit dem Befehl `end` oder `exit`.

Sie zeigen den Status und die Konfiguration der Schnittstellen mit dem Befehl `show interface ppp` an.

7.2.3 Befehle im Interface Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im Interface Konfigurationsmodus aufrufen können. Abhängig von der eingestellten Schnittstelle sind verschiedene Befehlssätze verfügbar.

Geben Sie im globalen Konfigurationsmodus den Befehl `interface` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im Interface Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

- Wenn Sie den Interface Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den Interface Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

7.2.3.1 forced disconnect

Beschreibung

Mit diesem Befehl legen Sie fest, ob Sie die Zwangstrennung durch Ihren Provider auf eine bestimmte Uhrzeit verschieben wollen.

Voraussetzung

- Die Funktion "PPPoE Passthrough" ist deaktiviert.
- Sie befinden Sich im Interface Konfigurationsmodus

  Die Eingabeaufforderung lautet:

  ```
  cli(config-ppp-X)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
forced disconnect{enabled | disabled}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`enabled`	Aktiviert die Zwangstrennung	-
`disabled`	Deaktiviert die Zwangstrennung	-

Ergebnis

Die Einstellung ist konfiguriert.

Weitere Hinweise

Sie konfigurieren die Uhrzeit mit dem Befehl `forced disconnect time`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ppp information` an.

7.2.3.2 forced disconnect time

Beschreibung

Mit diesem Befehl legen Sie die Uhrzeit fest zu der Sie die Zwangstrennung des DSL-Anbieters verschieben wollen. Vorausgesetzt, im Gerät ist die korrekte Systemzeit eingestellt.

Voraussetzung

Sie befinden sich im MODEM Interface-Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(config-ppp-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
forced disconnect time <hh:mm:ss>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
-	Uhrzeit	Geben Sie die Uhrzeit im folgenden Format an: hh:mm:ss

Ergebnis

Die Uhrzeit ist festgelegt.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ppp information` an.

Sie aktivieren die Zwangstrennung mit dem Befehl `forced disconnect`.

7.2.3.3 interface vlan

Beschreibung

Mit diesem Befehl legen Sie die Schnittstelle fest, über die die PPP-Verbindung aufgebaut wird.

Voraussetzung

Sie befinden sich im Interface-Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(config-ppp-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
interface vlan <vlan-id (1-4094)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vlan`	Schlüsselwort für eine VLAN-Verbindung.	-
`vlan-id`	Nummer des angesprochenen VLAN	1 ... 4094

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Das Schnittstelle ist zugewiesen.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ppp informations` an.

Sie aktivieren die PPP-Verbindung mit dem Befehl `pool-enable`.

7.2.3.4 ip address

Beschreibung

Mit diesem Befehl weisen Sie der Schnittstelle eine IPv4-Adresse zu.

Voraussetzung

Sie befinden sich im Interface-Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(config-ppp-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ip address <ip-address>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ip-address`	IPv4-Adresse für die Schnittstelle	geben Sie eine gültige IPv4-Adresse an

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die IP-Adresse ist der PPP-Schnittstelle zu gewiesen.

Weitere Hinweise

Sie löschen die IPv4-Adresse mit dem Befehl `no ip address`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ip interface` an.

7.2.3.5 ip address dhcp

Beschreibung

Mit diesem Befehl bezieht die Schnittstelle die IPv4-Adress per DHCP.

Voraussetzung

Sie befinden sich im Interface-Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(config-ppp-X)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
ip address dhcp
```

Ergebnis

Der DHCP weist der Schnittstelle die IPv4-Adresse zu.

Weitere Hinweise

Sie löschen die Einstellungen mit dem Befehl `no ip address`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ip interface` an.

7.2.3.6 no ip address

Beschreibung

Mit diesem Befehl löschen Sie die Zuweisung einer IPv4-Adresse zu einer Schnittstelle und deaktivieren DHCP.

Voraussetzung

Sie befinden sich im Interface-Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(config-ppp-X)#
```

Syntax

Rufen Sie den Befehl ohne Parameter oder mit folgender Parametrierung auf:

```
no ip address [<ip-address> | dhcp]
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ip-address`	IPv4-Adresse für die Schnittstelle, die gelöscht wird	geben Sie eine gültige IPv4-Adresse an
`dhcp`	Geben sie diesen Parameter an wenn sie explizit die DHCP-Funktion deaktivieren wollen.	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Einstellung ist konfiguriert.

Weitere Hinweise

Sie konfigurieren die statische IPv4-Adresse mit dem Befehl `ip address`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ip interface` an.

Sie aktivieren DHCP mit dem Befehl `ip address dhcp`.

7.2.3.7 password

Beschreibung

Mit diesem Befehl konfigurieren Sie das Passwort.

Voraussetzung

Sie befinden sich im Interface-Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(config-ppp-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
password <pw(255)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`pw`	Passwort	Geben Sie das Passwort für den Benutzer an. Das Passwort erhalten Sie von Ihrem DSL-Anbieter. Maximal 255 Zeichen

Ergebnis

Das Passwort ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ppp informations` an.

7.2.3.8 shutdown

Beschreibung

Mit diesem Befehl schalten Sie die Schnittstelle ab.

Voraussetzung

Sie befinden sich im Interface-Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(config-ppp-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
shutdown [complete]
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
ohne Parameter	Die Schnittstelle ist abgeschaltet, aber die Verbindung besteht noch	-
`complete`	Die Schnittstelle ist abgeschaltet und die PPP-Verbindung ist abgebaut	-

Ergebnis

Die WAN-Schnittstelle ist deaktiviert.

Wenn Sie den Befehl ohne Parameter ausführen, wird weiterhin eine Verbindung angezeigt. Die LED für den Portstatus blinkt. Allerdings werden keine Daten gesendet oder empfangen.

Weitere Hinweise

Sie schalten die Schnittstelle mit dem Befehl `no shutdown` ein.

7.2.3.9 no shutdown

Beschreibung

Mit diesem Befehl aktivieren Sie die WAN-Schnittstelle.

Voraussetzung

Sie befinden sich im Interface-Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(config-ppp-X)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no shutdown
```

Ergebnis

Die Schnittstelle ist abgeschaltet.

Weitere Hinweise

Sie deaktivieren die WAN-Schnittstelle mit dem Befehl `shutdown`.

7.2.3.10 type ppo-ex

Beschreibung

Mit diesem Befehl legen Sie fest, dass das Protokoll PPPoE (Point-to-Point over Ethernet) für die PPP-Verbindung verwendet wird.

Voraussetzung

Sie befinden sich im Interface-Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(config-ppp-X)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
type ppo-ex
```

Ergebnis

Das Protokoll PPPoE wird verwendet.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ppp information` an.

7.2.3.11 username

Beschreibung

Mit diesem Befehl konfigurieren Sie den Benutzernamen.

Voraussetzung

Sie befinden sich im Interface-Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(config-ppp-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
username <name(255)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`name`	Benutzername	Geben Sie den Benutzernamen an. Den Benutzernamen erhalten Sie von Ihrem DSL-Anbieter.

Ergebnis

Der Benutzername ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ppp information` an.

Sie konfigurieren das dazugehörige Passwort mit dem Befehl `password`.

7.3 Passive Listening

7.3.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

7.3.1.1 show passive-listening

Beschreibung

Dieser Befehl zeigt an, ob "Passive Listening" aktiviert ist.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show passive-listening
```

Ergebnis

Es wird `disabled` angezeigt, wenn "Passive Listening" deaktiviert ist. Wenn "Passive Listening" aktiviert ist, wird `enabled` angezeigt.

7.3.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

7.3.2.1 passive-listening bpdu-vlan-flood

Beschreibung

Mit diesem Befehl aktivieren Sie, dass BPDUs VLAN-spezifisch weitergeleitet werden, d. h. an allen Ports, die Mitglied eines VLANs sind.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
passive-listening bpdu-vlan-flood
```

Der Defaultwert der Funktion ist "aktiviert".

Ergebnis

BPDUs werden VLAN-spezifisch weitergeleitet.

Weitere Hinweise

Sie deaktivieren diese Funktion mit dem Befehl `no passive-listening bpdu-vlan-flood`.

Sie zeigen den Status von "Passive Listening" mit dem Befehl `show passive-listening` an.

7.3.2.2 no passive-listening bpdu-vlan-flood

Beschreibung

Mit diesem Befehl aktivieren Sie, dass BPDUs an alle verfügbaren Ports des Geräts geflutet werden, unabhängig von den konfigurierten VLANs.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no passive-listening bpdu-vlan-flood
```

Ergebnis

BPDUs werden an alle verfügbaren Ports des Geräts geflutet.

Weitere Hinweise

Sie aktivieren diese Funktion mit dem Befehl `passive-listening bpdu-vlan-flood`.

Sie zeigen den Status von "Passive Listening" mit dem Befehl `show passive-listening` an.

7.3.2.3 passive-listening

Beschreibung

Dieser Befehl aktiviert "Passive Listening".

Voraussetzung

Hinweis
Kein gleichzeitiger Betrieb mit Spanning Tree

"Passive Listening" kann nur aktiviert werden, wenn Spanning Tree ausgeschaltet ist!

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
passive-listening
```

Ergebnis

Die Funktion "Passive Listening" ist aktiviert.

Weitere Hinweise

Sie deaktivieren "Passive Listening" mit dem Befehl `no passive-listening`.

Sie zeigen den Status von "Passive Listening" mit dem Befehl `show passive-listening` an.

7.3.2.4 no passive-listening

Beschreibung

Dieser Befehl deaktiviert "Passive Listening".

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no passive-listening
```

Ergebnis

Die Funktion "Passive Listening" ist deaktiviert.

Weitere Hinweise

Sie aktivieren "Passive Listening" mit dem Befehl `passive-listening`.

Sie zeigen den Status von "Passive Listening" mit dem Befehl `show passive-listening` an.

7.4 Spanning Tree

Das Spanning Tree Protokoll dient dazu, ein LAN auf redundante Verbindungen zu überwachen. Diese werden blockiert und bei Änderungen in der Netztopologie bei Bedarf wieder aktiviert.

In diesem Kapitel werden Befehle des Spanning Tree Protocol (STP), des Rapid Spanning Tree Protocol (RSTP) und des Multiple Spanning Tree Protocol (MSTP)beschrieben.

Hinweis

Vermeiden von Fehlkonfigurationen

Gehen Sie bei der Verwendung der Befehle dieses Kapitels besonders sorgfältig vor, da eine fehlerhafte Konfiguration dieser Funktion das Netzwerk stark beeinträchtigen kann.

7.4.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

7.4.1.1 show spanning-tree

Beschreibung

Dieser Befehl zeigt die Einstellungen für die Spanning Tree-Funktion an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show spanning-tree [{ summary | blockedports | pathcost method }]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung
`summary`	zeigt eine Zusammenfassung an
`blockedports`	zeigt die blockierten Ports an
`pathcost method`	zeigt an, ob bei der Berechnung 16 Bit (short) oder 32 Bit (long) Werte verwendet werden

Ergebnis

Die Einstellungen für die Spanning Tree-Funktion werden angezeigt.

Weitere Hinweise

Sie zeigen weitere Einstellungen für spezielle Aspekte des Spanning Tree-Protokolls mit folgenden Befehlen an:

- `show spanning-tree active`
- `show spanning-tree bridge`
- `show spanning-tree detail`
- `show spanning-tree interface`
- `show spanning-tree root`
- `show spanning-tree mst`

7.4.1.2 show spanning-tree active

Beschreibung

Dieser Befehl zeigt die Einstellungen für die aktiven Ports der Spanning Tree-Funktion an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show spanning-tree active [detail]
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung
`detail`	zeigt Einstellungen im Detail an

Ergebnis

Die Einstellungen für die aktiven Ports der Spanning Tree-Funktion werden angezeigt.

7.4.1.3 show spanning-tree bridge

Beschreibung

Dieser Befehl zeigt die Einstellungen für die Spanning Tree-Funktion der Bridge an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show spanning-tree bridge
 [{ address | forward-time | hello-time | id | max-age | protocol | priority | detail
}]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung
`address`	zeigt die MAC-Adresse der Bridge an
`forward-time`	zeigt die Zeitspanne an, in der sich die Bridge beim Übergang vom Blocking-Modus in den Learning-Modus im Listening-Modus befindet
`hello-time`	zeigt die Zeitspanne an, nach der die Bridge Konfigurationstelegramme (BPDUs) sendet
`id`	zeigt die ID der Bridge an
`max-age`	zeigt das maximale Alter eines Datenpakets an, nach dessen Erreichen es gelöscht wird
`protocol`	zeigt das verwendete Protokoll an
`priority`	zeigt die Priorität der Bridge an
`detail`	zeigt detaillierte Informationen über Spanning Tree-Einstellungen der Bridge an

Ergebnis

Die Einstellungen für die Spanning Tree-Funktion der Bridge werden angezeigt.

7.4.1.4 show spanning-tree detail

Beschreibung

Dieser Befehl zeigt detaillierte Einstellungen für die Spanning Tree-Funktion an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show spanning-tree detail
```

Ergebnis

Detaillierte Einstellungen für die Spanning Tree-Funktion werden angezeigt.

7.4.1.5 show spanning-tree interface

Beschreibung

Dieser Befehl zeigt die Einstellungen der Ports für die Spanning Tree-Funktion an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show spanning-tree interface <interface-type> <interface-id>
 [{ cost | priority | portfast | rootcost | restricted-role |
 restricted-tcn | state | stats | detail }]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstelle	
`cost`	Zeigt die Kosten des Ports an, die zur Berechnung des günstigsten Pfades verwendet werden.	-
`priority`	Zeigt die Priorität des Ports an.	-
`portfast`	Zeigt an, ob `spanning-tree portfast` aktiviert ist.	-
`rootcost`	Zeigt die Kosten des Pfades zur Root Bridge an.	-
`restricted-role`	Zeigt an, ob `spanning-tree restricted-role` aktiviert ist.	-
`restricted-tcn`	Zeigt an, ob `spanning-tree restricted-tcn` aktiviert ist.	-
`state`	Zeigt den Status der Schnittstelle an.	-
`stats`	Zeigt die Zähler der verschiedenen BPDU-Übertragungen an.	-
`detail`	Zeigt detaillierte Informationen über Spanning Tree-Einstellungen der Schnittstelle an.	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Einstellungen der Ports für die Spanning Tree-Funktion werden angezeigt.

7.4.1.6 show spanning-tree interface layer2-gateway-port

Beschreibung

Dieser Befehl zeigt die Einstellungen für Layer 2 Gateway Port (L2GP) an. Angezeigt werden z. B. die Priorität, die MAC-Adresse und der Status von L2GP.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show spanning-tree interface
[<interface-type><interface-id>]
layer2-gateway-port
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstelle	

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Einstellungen für Layer 2 Gateway Port (L2GP) werden angezeigt.

7.4.1.7 show spanning-tree root

Beschreibung

Dieser Befehl zeigt die Einstellungen der Root Bridge für die Spanning Tree-Funktion an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show spanning-tree root
   [{address|cost|forward-time|id|max-age|port|priority|detail}]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung
`address`	zeigt die MAC-Adresse der Root Bridge an
`cost`	zeigt die Kosten der Verbindung zur Root Bridge an.
`forward-time`	zeigt die Zeitspanne, in der sich die Bridge beim Übergang vom Blocking-Modus in den Learning-Modus im Listening-Modus befindet

Parameter	Beschreibung
`id`	zeigt die ID der Root Bridge an
`max-age`	zeigt das maximale Alter eines Datenpakets an, nach dessen Erreichen es gelöscht wird
`port`	zeigt die Schnittstelle an, über die der Spanning Tree aufgebaut wird
`priority`	zeigt die Priorität der Bridge an
`detail`	zeigt detaillierte Informationen über die Root Bridge an

Ergebnis

Die Einstellungen der Root Bridge für die Spanning Tree-Funktion werden angezeigt.

7.4.2 clear spanning-tree detected protocols

Beschreibung

Mit diesem Befehl starten Sie den Protokoll-Übertragungsprozess auf einer bestimmten bzw. auf allen Schnittstellen neu und erzwingen ein erneutes Aushandeln der Verbindungseinstellungen mit den benachbarten Geräten.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
clear spanning-tree detected protocols
   [{interface<interface-type><interface-id>}]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`interface`	Schlüsselwort für eine Schnittstellenbeschreibung	-
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstelle	

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Wenn Sie keinen Parameter aus der Parameterliste auswählen, wird der Prozess für alle Schnittstellen neu gestartet.

Ergebnis

Die Verbindungseinstellungen für Spanning Tree werden neu ausgehandelt.

7.4.3 clear spanning-tree counters

Beschreibung

Mit diesem Befehl setzen Sie alle statistischen Zähler der Spanning Tree-Funktion auf Geräte- und auf Portebene zurück.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
clear spanning-tree counters
```

Ergebnis

Die Spanning Tree-Zähler sind zurückgesetzt.

7.4.4 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

7.4.4.1 spanning-tree

Beschreibung

Das Spanning Tree-Protokoll dient dazu, ein LAN auf redundante Verbindungen zu überwachen. Diese werden blockiert und bei Änderungen in der Netztopologie bei Bedarf wieder aktiviert.

Mit diesem Befehl aktivieren Sie die Spanning Tree-Funktion.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
spanning-tree
```

Ergebnis

Die Spanning Tree-Funktion ist aktiviert.

Weitere Hinweise

Der Defaultwert der Funktion ist "aktiviert".

Sie deaktivieren die Spanning Tree-Funktion mit dem Befehl `no spanning-tree`.

Sie zeigen den Status dieser Funktion und weitere Informationen mit dem Befehl `show spanning-tree detail` an.

Sie zeigen Informationen über aktive Ports mit dem Befehl `show spanning-tree active` an.

7.4.4.2 no spanning-tree

Beschreibung

Mit diesem Befehl deaktivieren Sie die Spanning Tree-Funktion.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no spanning-tree
```

Ergebnis

Die Spanning Tree-Funktion ist deaktiviert.

Weitere Hinweise

Sie aktivieren die Spanning Tree-Funktion mit dem Befehl `spanning-tree`.

Sie zeigen den Status dieser Funktion und weitere Informationen mit dem Befehl `show spanning-tree detail` an.

Sie zeigen Informationen über aktive Ports mit dem Befehl `show spanning-tree active` an.

7.4.4.3 spanning-tree (Zeiteinstellungen)

Beschreibung

Mit diesem Befehl konfigurieren Sie verschiedene Zeiteinstellungen der Spanning Tree-Funktion:

- Mit der Option `forward-time` konfigurieren Sie die Zeitspanne, nach der ein Port seinen Spanning Tree-Status von "Blocking" nach "Forwarding" umschaltet.
- Mit der Option `hello-time` konfigurieren Sie die Zeitspanne, nach der die Bridge ihre Konfigurationstelegramme (BPDUs) sendet.
- Mit der Option `max-age` konfigurieren Sie die Zeitspanne, nach der die Informationen der BPDUs ungültig werden.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
spanning-tree{forward-time<seconds(4-30)>|hello-time<seconds(1-2)>|
                    max-age<seconds(6-40)>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`forward-time`	Schlüsselwort für die Zeitspanne, nach der ein Port seinen Spanning Tree-Status von "Blocking" nach "Forwarding" umschaltet	-
`seconds`	Zeitspanne, nach der die Umschaltung erfolgt	4 ... 30 Default: 15
`hello-time`	Schlüsselwort für die Zeitspanne, nach der die Bridge ihre Konfigurations-BPDUs sendet	-
`seconds`	Zeitspanne, nach der die Sendung erfolgt	1 ... 6 Default: 2
`max-age`	Schlüsselwort für die Zeitspanne, nach der die Informationen der BPDUs ungültig werden	-
`seconds`	maximales Alter der BPDUs in Sekunden	6 ... 55 Default: 20

Hinweis

Abhängigkeiten beim Einstellen des Timings

Wenn Sie die Zeiteinstellungen für Spanning Tree festlegen, müssen Sie die beiden folgenden Regeln einhalten:

- 2 * (`forward-time` - 1) ≥ `max-age`
- `max-age` ≥ 2 * (`hello-time` + 1)

Ergebnis

Die gewählte Einstellung für die Zeitspanne ist konfiguriert.

Weitere Hinweise

Sie setzen die Zeiteinstellungen mit den Befehlen `no spanning-tree forward-time`, `no spanning-tree hello-time` bzw. `no spanning-tree max-age` auf die voreingestellten Werte zurück.

Wenn Sie den Befehl `no spanning-tree` ohne Parameter aufrufen, deaktivieren Sie die Spanning Tree-Funktion. Die konfigurierten Zeiteinstellungen bleiben erhalten.

Wenn Sie den Befehl `restart factory` aufrufen, startet das System mit werkseitigen Konfigurationseinstellungen neu. Alle Zeiteinstellungen sind zurückgesetzt.

Sie zeigen diese Einstellungen und weitere Informationen mit den Befehlen an, die mit `show spanning-tree ...` beginnen.

7.4.4.4 no spanning-tree (Zeiteinstellungen)

Beschreibung

Mit diesem Befehl in Verbindung mit dem entsprechenden Parameter setzen Sie die Zeiteinstellungen der Spanning Tree-Funktion auf den voreingestellten Wert zurück.

Wenn Sie den Befehl ohne Parameter aufrufen, deaktivieren Sie die Spanning Tree-Funktion. Die konfigurierten Zeiteinstellungen bleiben erhalten.

Wenn Sie den Befehl `restart factory` aufrufen, startet das System mit werkseitigen Konfigurationseinstellungen neu. Alle Zeiteinstellungen sind zurückgesetzt.

Die voreingestellten Werte sind:

Parameter	voreingestellter Wert
`forward-time`	15 Sekunden
`hello-time`	2 Sekunden
`max-age`	20 Sekunden

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no spanning-tree{forward-time|hello-time|max-age}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung
`forward-time`	Zeitspanne, nach der ein Port seinen Spanning Tree-Status von "Blocking" nach "Forwarding" umschaltet
`hello-time`	Zeitspanne, nach der die Bridge ihre Konfigurationstelegramme (BPDUs) sendet
`max-age`	Zeitspanne, nach der die Informationen der BPDUs ungültig werden

Ergebnis

Die gewählte Einstellung für die Zeitspanne ist auf den voreingestellten Wert zurückgesetzt.

Weitere Hinweise

Sie konfigurieren die Zeitspanne mit dem Befehl `spanning-tree` (Zeiteinstellungen).

Sie zeigen diese Einstellungen und weitere Informationen mit den Befehlen an, die mit `show spanning-tree ...` beginnen.

7.4.5 Befehle im Interface Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im Interface Konfigurationsmodus aufrufen können. Abhängig von der eingestellten Schnittstelle sind verschiedene Befehlssätze verfügbar.

Geben Sie im globalen Konfigurationsmodus den Befehl `interface` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im Interface Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

- Wenn Sie den Interface Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den Interface Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im Interface Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

7.4.5.1 spanning-tree

Beschreibung

Mit diesem Befehl konfigurieren Sie verschiedene Eigenschaften der Spanning Tree-Funktion:

- Mit der Option `cost` konfigurieren Sie die Kosten des Ports, die zur Berechnung des günstigsten Pfades verwendet werden.
- Mit der Option `disable` sperren Sie die Schnittstelle für die Spanning Tree-Funktion.
- Mit der Option `link-type` konfigurieren Sie den Verbindungsstatus des folgenden Netzwerksegments. Folgende Einstellungen sind möglich:
  - `point-to-point` – die Schnittstelle kommuniziert mit genau einer Netzwerkkomponente
  - `shared` – die Schnittstelle ist mit mehreren Netzwerkkomponenten verbunden
- Mit der Option `portfast` aktivieren Sie die PortFast-Funktion auf der Schnittstelle. Die Schnittstelle ist mit einem Endgerät verbunden und kann daher die Wartezeit vor dem Wechsel in den Forwarding-Modus ignorieren.
- Mit der Option `port-priority` konfigurieren Sie die Priorität der Schnittstelle für das Aushandeln einer Spanning Tree-Konfiguration.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
spanning-tree {cost <0-200000000>|disable|
               link-type{point-to-point|shared}|portfast|
               port-priority<0-240>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`cost`	Schlüsselwort Beschreibt die Kosten des Ports zur Berechnung des günstigsten Pfades.	0 ... 200000000 Default: wenn die dynamische Berechnung der Pfadkosten nicht aktiviert ist: • 200000 für physikalische Schnittstellen • 199999 für Port-Channels
`disable`	sperrt die Schnittstelle für Spanning Tree	- Default: die Spanning Tree-Funktion ist auf der Schnittstelle aktiv
`link-type`	Verbindungsstatus des folgenden Netzwerksegments	• `point-to-point` • `shared` Default: • `point-to-point` die Verbindung ist als `full-duplex` konfiguriert • `shared` in allen anderen Fällen
`portfast`	aktiviert die PortFast-Funktion	- Default: deaktiviert
`port-priority`	Priorität der Schnittstelle	0 ... 240 in Schritten von 16 Default: 128

Hinweis

Mehrere Eigenschaften konfigurieren

Bei jedem Aufruf des Befehls können Sie genau eine Eigenschaft konfigurieren.
Wenn Sie mehrere Eigenschaften konfigurieren möchten, rufen Sie den Befehl mehrmals auf.

Ergebnis

Die gewählte Eigenschaft ist konfiguriert.

Weitere Hinweise

Sie setzen die Einstellung mit dem Befehl `no spanning-tree` (Eigenschaften) auf den voreingestellten Wert zurück.

Sie zeigen diese Einstellungen und weitere Informationen mit den Befehlen an, die mit `show spanning-tree ...` beginnen.

7.4.5.2 no spanning-tree

Beschreibung

Mit diesem Befehl setzen Sie verschiedene Eigenschaften der Spanning Tree-Funktion auf den voreingestellten Wert zurück:

Die voreingestellten Werte sind:

Parameter	voreingestellter Wert
`cost`	wenn die dynamische Berechnung der Pfadkosten nicht aktiviert ist: • 200000 für physikalische Schnittstellen • 199999 für Port-Channels
`disable`	die Spanning Tree-Funktion ist auf der Schnittstelle aktiv
`link-type`	• `point-to-point` die Verbindung ist als `full-duplex` konfiguriert • `shared` in allen anderen Fällen
`portfast`	deaktiviert
`port-priority`	128

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no spanning-tree {cost|disable|link-type|portfast|port-priority}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung
`cost`	Schlüsselwort für die Kosten des Ports zur Berechnung des günstigsten Pfades.
`disable`	Gibt die Schnittstelle für Spanning Tree frei.

Parameter	Beschreibung
`link-type`	Verbindungsstatus des folgenden Netzwerksegments
`portfast`	Deaktiviert die PortFast-Funktion.
`port-priority`	Schlüsselwort für die Priorität der Schnittstelle

Hinweis

Mehrere Eigenschaften konfigurieren

Bei jedem Aufruf des Befehls können Sie genau eine Eigenschaft konfigurieren.
Wenn Sie mehrere Eigenschaften konfigurieren möchten, rufen Sie den Befehl mehrmals auf.

Ergebnis

Die gewählte Einstellung wurde auf den voreingestellten Wert zurückgesetzt.

Weitere Hinweise

Sie konfigurieren die Einstellung mit dem Befehl `spanning-tree` (Eigenschaften).

Sie zeigen diese Einstellungen und weitere Informationen mit den Befehlen an, die mit `show spanning-tree ...` beginnen.

7.4.5.3 spanning-tree auto-edge

Beschreibung

Mit diesem Befehl aktivieren Sie automatische Erkennung einer Bridge, die an der Schnittstelle angeschlossen ist.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
spanning-tree auto-edge
```

Ergebnis

Die automatische Erkennung einer Bridge an der Schnittstelle ist aktiviert.

Weitere Hinweise

Sie deaktivieren die automatische Erkennung einer Bridge an der Schnittstelle mit dem Befehl `no spanning-tree auto-edge`.

7.4.5.4 no spanning-tree auto-edge

Beschreibung

Mit diesem Befehl deaktivieren Sie automatische Erkennung einer Bridge, die an der Schnittstelle angeschlossen ist.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no spanning-tree auto-edge
```

Ergebnis

Die automatische Erkennung einer Bridge an der Schnittstelle ist deaktiviert.

Weitere Hinweise

Sie aktivieren die automatische Erkennung einer Bridge an der Schnittstelle mit dem Befehl `spanning-tree auto-edge`.

Netzwerk-Protokolle 8

In diesem Abschnitt finden Sie die Kapitel, die Befehle zum Arbeiten mit den verschiedenen Netzwerkprotokollen beschreiben.

8.1 Protocol IPv4

In diesem Kapitel werden Befehle des Internet Protocol (IP) Version 4 beschrieben.

8.1.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.1.1.1 show ip dns

Beschreibung

Dieser Befehl zeigt Informationen zum DNS-Client an, beispielsweise der Status des DNS-Clients und Parameter für Anfragen beim DNS-Server.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show ip dns
```

Ergebnis

Informationen zum DNS-Client werden angezeigt.

8.1.1.2 show dcp forwarding

Beschreibung

Dieser Befehl zeigt die Übersicht über das DCP-Forwarding-Verhalten einer oder aller Schnittstellen an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show dcp forwarding [port <interface-type> <interface-id>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`port`	Schlüsselwort für eine Schnittstellen-beschreibung	-
`interface-type`	Typ bzw. Geschwindigkeit der Schnitt-stelle	Geben Sie eine gültige Schnitt-stelle an.
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstel-le	

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Übersicht über das DCP-Forwarding-Verhalten wird angezeigt.

8.1.1.3 show dcp server

Beschreibung

Dieser Befehl zeigt an, ob die DCP-Funktion auf dem Gerät aktiviert ist.

Wenn die DCP-Funktion aktiviert ist, werden die Lese- und Schreibrechte angezeigt.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show dcp server
```

Ergebnis

Die Übersicht über den Status der DCP-Funktion und die Zugriffsrechte wird angezeigt.

8.1.1.4 show ip route

Beschreibung

Dieser Befehl zeigt die Routen an, die aktuell verwendet werden.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show ip route[{<ip-address>[<mask>]|connected|static}]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich
`ip-address`	Zeigt die Informationen für eine bestimmte IP Adresse an.	Geben Sie eine gültige IP Adresse an
`mask`	Definiert einen Adressbereich über die Subnetzmaske.	/8, /16 oder /24
`connected`	Zeigt die Direktverbindungen an.	-
`static`	Zeigt die statischen Verbindungen an.	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Routing-Tabelle wird angezeigt.

8.1.1.5 show ip routing

Beschreibung

Diese Befehl zeigt an, ob die Funktion "Routing" aktiviert ist.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show ip routing
```

Ergebnis

Die Funktion "Routing" ist aktiviert.

8.1.1.6 show ip static route

Beschreibung

Dieser Befehl zeigt die Routen an, die statisch erzeugt wurden.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show ip static route
```

Ergebnis

Die statischen Routen werden angezeigt.

8.1.1.7 show ip telnet

Beschreibung

Dieser Befehl zeigt den Admin-Status und die Port-Nummer des Telnet-Servers an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show ip telnet
```

Ergebnis

Der Admin-Status und die Port-Nummer des Telnet-Servers werden angezeigt.

8.1.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.1.2.1 dcp server

Beschreibung

Mit diesem Befehl konfigurieren Sie die Lese- und Schreibrechte für den DCP-Server und aktivieren ihn.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
dcp server {read-only|read-write}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`read-only`	auf dem DCP-Server darf nur gelesen werden	-
`read-write`	auf dem DCP-Server darf gelesen und geschrieben werden	Default: `read-write`

Ergebnis

Die Lese- und Schreibrechte für den DCP-Server sind konfiguriert.

Der DCP-Server ist aktiviert.

Weitere Hinweise

Sie deaktivieren den DCP-Server mit dem Befehl `no dcp server`.

8.1.2.2 no dcp server

Beschreibung

Mit diesem Befehl deaktivieren Sie den DCP-Server.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no dcp server
```

Ergebnis

Der DCP-Server ist deaktiviert.

Weitere Hinweise

Sie aktivieren und konfigurieren den DCP-Server mit dem Befehl `dcp server`.

8.1.2.3 ip echo-reply

Beschreibung

Um die Verfügbarkeit eines Netzwerkteilnehmers zu prüfen, können an ihn Pakete des Internet Control Message Protocol (ICMP) gesendet werden. Diese Pakete vom Typ 8 fordern den Empfänger auf, ein Paket an den Sender zurück zu schicken (Echo Reply).

Mit diesem Befehl aktivieren Sie, dass der Netzwerkteilnehmer auf Ping-Anfragen reagiert.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
ip echo-reply
```

Ergebnis

"ICMP Echo Reply Messages" sind aktiviert. Der Netzwerkteilnehmer reagiert auf Ping-Anfragen.

Weitere Hinweise

Sie deaktivieren die Einstellung mit dem Befehl `no ip echo-reply`.

8.1.2.4 no ip echo-reply

Beschreibung

Mit diesem Befehl deaktivieren Sie, dass der Netzwerkteilnehmer auf Ping-Anfragen reagiert.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no ip echo-reply
```

Ergebnis

"ICMP Echo Reply Messages" sind deaktiviert. Der Netzwerkteilnehmer reagiert nicht auf Ping-Anfragen.

Weitere Hinweise

Sie ändern die Einstellung mit dem Befehl `ip echo-reply`.

8.1.2.5 ip route

Beschreibung

Mit diesem Befehl konfigurieren Sie einen statischen Eintrag in die IP-Routing-Tabelle.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ip route <prefix> <mask> <next-hop> [<distance (1-255)>] [ interface { vlan <short
(1-4094)> } ]
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`prefix`	gibt die IP-Adresse bzw. den Adressbereich an	geben Sie eine gültige IP-Adresse an
`mask`	gibt die Subnetzmaske an, die auf `prefix` angewendet wird. Verwenden Sie die dezimale Schreibweise.	geben Sie eine gültige Subnetzmaske an
`next-hop`	gibt die IP-Adresse an, auf die die ausgewählten Adressen weitergeleitet werden.	geben Sie eine gültige IP-Adresse an
`distance`	Der Wert für die administrative Distanz.	1 ... 255
`interface`		
`vlan`	Schlüsselwort für eine VLAN Verbindung	-
`short`	Nummer des angesprochenen VLAN	1 ... 4094

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Der Eintrag in die IP-Routing-Tabelle ist konfiguriert.

Weitere Hinweise

Sie löschen einen Eintrag aus der IP-Routing-Tabelle mit dem Befehl `no ip route`.

Sie zeigen die IP-Routing-Tabelle mit dem Befehl `show ip route` an.

8.1.2.6 no ip route

Beschreibung

Mit diesem Befehl löschen Sie einen statischen Eintrag aus der IPv4-Routingtabelle.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no ip route <prefix> <mask> <next-hop>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`prefix`	gibt die IP-Adresse bzw. den Adressbereich an	geben Sie eine gültige IPv4-Adresse an
`mask`	gibt die Subnetzmaske an, die auf `prefix` angewendet wird. Verwenden Sie die dezimale Schreibweise.	geben Sie eine gültige Subnetzmaske an
`next-hop`	gibt die IP-Adresse an, auf die die ausgewählten Adressen weitergeleitet wurden.	geben Sie eine gültige IPv4-Adresse an

Ergebnis

Der Eintrag ist gelöscht.

Weitere Hinweise

Sie löschen einen Eintrag aus der IPv4-Routing-Tabelle mit dem Befehl `no ip route`.

Sie zeigen die IPv4-Routingtabelle mit dem Befehl `show ip route` an.

Sie zeigen die statische Routen mit dem Befehl `show ip static route` an.

8.1.2.7 ip routing

Beschreibung

Mit diesem Befehl aktivieren Sie die Funktion "Routing" für IPv4.

Hinweis

Dieser Befehl ist nur bei Layer 3 verfügbar. DHCP darf auf keinem IP-Interface aktiviert sein.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
ip routing
```

Ergebnis

Die Funktion "Routing" ist aktiviert.

Weitere Hinweise

Sie deaktivieren die Funktion mit dem Befehl `no ip routing`.

Sie zeigen die Einstellung mit dem Befehl `show ip route` an.

8.1.2.8 no ip routing

Beschreibung

Mit diesem Befehl deaktivieren Sie im Gerät IPv4-Routing.

Hinweis

IPv6-Routing

Ist am Gerät auch IPv6-Routing aktiviert, wird dies ebenfalls mit dieser Funktion deaktiviert.

Hinweis

Dieser Befehl ist nur bei Layer 3 verfügbar.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no ip routing
```

Ergebnis

IPv4-Routing ist deaktiviert.

Weitere Hinweise

Sie aktivieren die Funktion mit dem Befehl `ip routing`.

Sie zeigen die Einstellung mit dem Befehl `show ip route` an.

8.1.2.9 telnet-server

Beschreibung

Mit diesem Befehl aktivieren Sie den Telnet-Server.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
telnet-server
```

Der Defaultwert der Funktion ist "aktiviert".

Ergebnis

Der Telnet-Server ist aktiviert.

Weitere Hinweise

Sie deaktivieren den Telnet-Server mit dem Befehl `no telnet-server`.

8.1.2.10 no telnet-server

Beschreibung

Mit diesem Befehl deaktivieren Sie den Telnet-Server.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no telnet-server
```

Ergebnis

Der Telnet-Server ist deaktiviert.

Weitere Hinweise

Sie aktivieren den Telnet-Server mit dem Befehl `telnet-server`.

8.1.3 Befehle im Interface Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im Interface Konfigurationsmodus aufrufen können. Abhängig von der eingestellten Schnittstelle sind verschiedene Befehlssätze verfügbar.

Geben Sie im globalen Konfigurationsmodus den Befehl `interface` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im Interface Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

- Wenn Sie den Interface Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den Interface Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im Interface Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.1.3.1 dcp forwarding

Beschreibung

Mit diesem Befehl konfigurieren Sie das Forwarding-Verhalten der Schnittstelle für DCP-Telegramme.

Hinweis

PROFINET-Konfiguration

Da es sich bei DCP um ein PROFINET-Protokoll handelt, ist die hier vorgenommene Konfiguration nur in dem mit dem TIA-Interface assoziierten VLAN wirksam.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
dcp forwarding {block|forward}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`block`	DCP-Telegramme werden verworfen	-
`forward`	DCP-Telegramme werden weitergeleitet	Default: `forward`

Ergebnis

Das Forwarding-Verhalten der Schnittstelle für DCP-Telegramme ist konfiguriert.

8.1.3.2 ip address

Beschreibung

Mit diesem Befehl weisen Sie der Schnittstelle eine IPv4-Adresse bzw. ein IPv4-Subnetz zu.

Voraussetzung

- DHCP wurde mit dem Befehl `no ip address` ausgeschaltet.
- Sie befinden sich im Interface Konfigurationsmodus von VLAN oder einem Router-Port

  Die Eingabeaufforderung lautet:

  ```
  cli(config-if-vlan-$$$)#
  ```

  oder bei einem Router-Port:

  ```
  cli(config-RPort-if-Int$-$)
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ip address <ip-address> {<subnet-mask>|/<prefix-length(0-32)>}[secondary]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ip-address`	IPv4-Adresse für die Schnittstelle	geben Sie eine gültige IPv4-Adresse an
`subnet-mask`	Subnetzmaske des zugehörigen Subnetzes	geben Sie eine gültige Subnetzmaske an
`prefix-length`	Dezimale Darstellung der Maske als Anzahl der "1" Bits	0 ... 32
`secondary`	Weiteres Subnetz für diese Schnittstelle	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die IPv4-Adresse ist der VLAN-Schnittstelle oder dem Router-Port zugewiesen.

Hinweis

Wirksamkeit des Befehls

Dieser Befehl wird sofort wirksam.

Wenn Sie die Schnittstelle konfigurieren, über die Sie auf das Gerät zugreifen, geht die Verbindung verloren!

Weitere Hinweise

Sie löschen die IPv4-Adresse mit dem Befehl `no ip address`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ip interface` an.

8.1.3.3 ip address dhcp

Beschreibung

Mit diesem Befehl bezieht die VLAN-Schnittstelle die IPv4-Adresse per DHCP.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus von VLAN.

Die Eingabeaufforderung lautet:

```
cli(config-if-vlan-$$$)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
ip address dhcp
```

Ergebnis

Der DHCP weist der VLAN-Schnittstelle die IP-Adresse zu.

Weitere Hinweise

Sie löschen die Einstellungen mit dem Befehl `no ip address`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ip interface` an.

8.1.3.4 no ip address

Beschreibung

Mit diesem Befehl löschen Sie die Zuweisung einer IP-Adresse zu einer VLAN-Schnittstelle.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus von VLAN.

Die Eingabeaufforderung lautet:

```
cli(config-if-vlan-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no ip address [{ <ucast_addr>|dhcp}]
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ucast_addr`	IP-Adresse der VLAN-Schnittstelle, die gelöscht wird	geben Sie eine gültige IP Adresse an
`dhcp`	Geben Sie diesen Parameter an, wenn Sie den Bezug der IP-Adresse von einem DHCP-Server aufheben wollen.	

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Zuweisung der IP-Adresse zu einer VLAN-Schnittstelle ist gelöscht und DHCP ist deaktiviert.

Hinweis

Wirksamkeit des Befehls

Dieser Befehl wird sofort wirksam.

Wenn Sie die Schnittstelle konfigurieren, über die Sie auf das Gerät zugreifen, können Sie die Verbindung verlieren!

Weitere Hinweise

Sie konfigurieren die Einstellung mit dem Befehl `ip address`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ip interface` an.

8.2 ARP

In diesem Kapitel werden Befehle des Address Resolution Protocol (ARP) beschrieben.

8.2.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.2.1.1 show ip arp

Beschreibung

Mit diesem Befehl zeigen Sie die ARP-Tabelle an. Die ARP-Tabelle enthält die eindeutige Zuordnung von MAC-Adresse zu IPv4-Adresse.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show ip arp [{vlan <vlan-id (1-4094)> | <interface-type> <interface-id> | <ip-address> | <mac-address> | summary | information}]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vlan`	Schlüsselwort für eine VLAN-Verbindung	-
`vlan-id`	Nummer des angesprochenen VLAN	1 ... 4094
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstelle	
`ip-address`	zeigt die IPv4-Adressen der Einträge in der ARP-Tabelle an	-
`mac-address`	zeigt die MAC-Adressen der Einträge in der ARP-Tabelle an	-

Parameter	Beschreibung	Wertebereich/Anmerkung
`summary`	zeigt eine Zusammenfassung der Einträge in der ARP-Tabelle an	-
`information`	zeigt Informationen über die ARP-Konfiguration an	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Wenn Sie keinen Parameter aus der Parameterliste auswählen, werden allen Parameter der ARP-Tabelle angezeigt.

Ergebnis

Die ARP-Tabelle wird angezeigt.

8.3 DHCP-Client

In diesem Kapitel werden Befehle des Dynamic Host Configuration Protocol (DHCP) beschrieben.

8.3.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.3.1.1 show ip dhcp client

Beschreibung

Mit diesem Befehl zeigen Sie die Konfigurationseinstellungen des DHCP-Client an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show ip dhcp client
```

Ergebnis

Die Konfigurationseinstellungen des DHCP-Clients werden angezeigt.

8.3.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.3.2.1 ip dhcp config-file-request

Beschreibung

Wenn die Option "DHCP config file request" gesetzt ist, fordert das Gerät beim DHCP-Server die TFTP-Adresse und den Namen einer Konfigurationsdatei an. Wenn das Gerät nach dem abgeschlossenen Herunterladen neu gestartet wird, werden die Konfigurationseinstellungen aus dieser Datei gelesen.

Mit diesem Befehl aktivieren Sie die Option "DHCP config file request".

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
ip dhcp config-file-request
```

Ergebnis

Die Option "DHCP config file request" ist aktiviert.

Weitere Hinweise

Sie deaktivieren die Option "DHCP config file request" mit dem Befehl `no ip dhcp config-file-request`.

8.3.2.2 no ip dhcp config-file-request

Beschreibung

Mit diesem Befehl deaktivieren Sie die Option "DHCP config file request".

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no ip dhcp config-file-request
```

Ergebnis

Die Option "DHCP config file request" ist deaktiviert.

Weitere Hinweise

Sie aktivieren die Option "DHCP config file request" mit dem Befehl `ip dhcp config-file-request`.

8.3.2.3 ip dhcp client mode

Beschreibung

Mit diesem Befehl konfigurieren Sie, mit welcher Art von Kennung sich der DHCP-Client bei seinem DHCP-Server anmeldet.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ip dhcp client mode {mac | client-id <client-id> | sysname  | iaid-duid }
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`mac`	Der Client meldet sich mit seiner MAC-Adresse an	-
`client-id`	Der Client meldet sich mit der zugewiesenen ID an	-
`client-id`	Name der zugewiesenen ID	max. 32 Zeichen
`sysname`	Der Client meldet sich mit dem zugewiesenen Systemnamen an	-
`iaid-duid`	Der Client meldet sich mit der IAID (Interface Association Identifier) und der DUID (DHCP Unique Identifier) an.	-

Ergebnis

Der Anmeldemodus des DHCP-Client ist konfiguriert.

Weitere Hinweise

Sie konfigurieren den DUID-Typ mit dem Befehl `dhcp duid type`.

8.3.2.4 dhcp duid type

Beschreibung

Mit diesem Befehl legen Sie den DUID-Typ.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
dhcp duid type {llt | en | ll}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`llt`	DUID basiert auf der Link-layer Adresse der Schnittstelle und einem Zeitstempel	-
`en`	DUID wird vom Hersteller (EN = Enterprise number) vergeben	-
`ll`	DUID basiert auf der Link-layer Adresse der Schnittstelle	-

Ergebnis

Der DUID-Typ ist festgelegt.

8.4 DHCP-Server

Das Gerät können Sie als DHCP-Server betreiben. Damit ist es möglich, den angeschlossenen Geräten automatisch IP-Adressen zuzuweisen. Die IP-Adressen werden entweder dynamisch aus einem von Ihnen vergebenen Adressband (Pool) verteilt oder es wird eine bestimmte IP-Adresse einem bestimmten Gerät zugewiesen.

Sowohl bei der dynamischen als auch bei der statischen Zuweisung wird ein Pool anhand folgender Kriterien ausgewählt:

1. Bei der DHCP-Anfrage ist die Option 82 aktiviert.

   Der DHCP-Server prüft, ob es einen Pool mit Option 82 gibt. Sie konfigurieren dieses Kriterium mit dem Befehl `relay-information`.

2. Die DHCP-Anfrage wurde über einen Relay Agent empfangen.

   Der DHCP-Server prüft, ob der Relay Agent im Subnetz eines Pools liegt.

3. Der Port, über den die DHCP-Anfrage empfangen wurde, ist im Port-Bereich aktiviert.

   Der DHCP-Server prüft, ob die IP-Schnittstelle des Ports im Subnetz eines Pools liegt. Sie konfigurieren dieses Kriterium mit dem Befehl `ip address`.

In diesem Kapitel werden Befehle beschrieben, die für das Konfigurieren des DHCP-Servers relevant sind.

Voraussetzung

Die angeschlossenen Geräte sind so konfiguriert, dass diese die IPv4-Adresse von einem DHCP-Server beziehen.

8.4.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.4.1.1 show ip dhcp-server bindings

Beschreibung

Dieser Befehl zeigt die aktuellen Zuordnungen von IPv4-Adressen des DHCP-Servers an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show ip dhcp-server bindings
```

Ergebnis

Die Informationen werden angezeigt.

8.4.1.2 show ip dhcp-server pools

Beschreibung

Der Befehl zeigt die DHCP-Server-Konfiguration eines bestimmten IPv4-Adressbands oder aller IPv4-Adressbänder und den dazugehörenden DHCP-Optionen an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show ip dhcp-server pools [pool-id (1-5)]
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`pool-id`	ID des angesprochenen IPv4-Adressbands	1 ... 5

Ergebnis

Die Konfiguration des DHCP-Servers und der DHCP-Optionen wird angezeigt.

8.4.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.4.2.1 ip dhcp-server

Beschreibung

Mit diesem Befehl aktivieren Sie den DHCP-Server auf dem Gerät.

Hinweis

Damit keine Konflikte mit IPv4-Adressen entstehen, darf im Netzwek nur ein Gerät als DHCP-Server konfiguriert sein.

Hinweis

Maximale Anzahl der IP-Adressen

Die maximale Anzahl der IPv4-Adressen, die der DHCP-Server unterstützt, ist 100. D. h. insgesamt 100 IPv4-Adressen (dynamisch + statisch).

Bei den statischen Zuordnungen können Sie maximal 20 Einträge anlegen.

Voraussetzung

- Sie befinden sich im globalen Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config)#
  ```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
ip dhcp-server
```

Ergebnis

Der DHCP-Server ist aktiviert.

Weitere Hinweise

Sie deaktivieren den DHCP-Server mit dem Befehl `no ip dhcp-server`.

8.4.2.2 no ip dhcp-server

Beschreibung

Mit diesem Befehl deaktivieren Sie den DHCP-Server auf dem Gerät.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no ip dhcp-server
```

Ergebnis

Der DHCP-Server ist deaktiviert.

Weitere Hinweise

Sie aktivieren den DHCP-Server mit dem Befehl `ip dhcp-server`.

8.4.2.3 no ip dhcp-server icmp-probe

Beschreibung

Mit diesem Befehl deaktivieren Sie die Funktion "Adresse vor dem Anbieten mit ICMP-Echo prüfen".

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no ip dhcp-server icmp-probe
```

Ergebnis

Die Funktion ist deaktiviert.

Weitere Hinweise

Sie aktivieren die Funktion mit dem Befehl `ip dhcp-server icmp-probe`.

8.4.2.4 ip dhcp-server icmp-probe

Beschreibung

Mit diesem Befehl aktivieren Sie die Funktion "Adresse vor dem Anbieten mit ICMP-Echo prüfen". Der DHCP-Server prüft, ob die IPv4-Adresse schon vergeben ist. Wenn keine Antwort zurückkommt, kann der DHCP-Server die IPv4-Adresse vergeben.

Hinweis

Bei statischen Zuordnungen wird diese Prüfung nicht durchgeführt.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
ip dhcp-server icmp-probe
```

Ergebnis

Die Funktion ist aktiviert.

Weitere Hinweise

Sie deaktivieren die Funktion mit dem Befehl `no ip dhcp-server icmp-probe`.

8.4.2.5 ip dhcp-server pool

Beschreibung

Mit diesem Befehl haben Sie drei Möglichkeiten in den DHCPPOOL-Konfigurationsmodus zu wechseln und dem IPv4-Adressband eine Schnittstelle zu zuweisen.

1. Wenn Sie den Befehl `ip dhcp-server pool` mit dem Parameter `pool-id (1-8)` aufrufen, wechseln Sie in den entsprechenden DHCPPOOL-Konfigurationsmodus. Die entsprechende Pool-ID muss bereits angelegt sein.
2. Wenn Sie den Befehl `ip dhcp-server pool` mit dem Parameter `vlan` oder `interface-type/interface-id` aufrufen, wird ein IPv4-Adressband mit der nächsten freien Pool-ID angelegt und diesem direkt die angegebene Schnittstelle zugewiesen. Anschließend erfolgt ein Wechsel in den entsprechenden DHCPPOOL-Konfigurationsmodus. Die weiteren Einstellungen konfigurieren Sie dann im DHCPPOOL-Konfigurationsmodus.
3. Wenn Sie den Befehl `ip dhcp-server pool` ohne Parameter aufrufen, wird ein IPv4-Adressband mit der nächsten freien Pool-ID angelegt und Sie wechseln direkt in den entsprechenden DHCPPOOL-Konfigurationsmodus.

   Die Schnittstelle und die weiteren Einstellungen konfigurieren Sie dann im DHCPPOOL-Konfigurationsmodus.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ip dhcp-server pool [{ <pool-id (1-8)> | [{ vlan <vlan-id (1-4094)> | <interface-
type> <interface-id> }]}]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`pool-id`	ID des angesprochenen IPv4-Adressbands	1 ... 8
`vlan`	Schlüsselwort für eine VLAN-Verbindung	-
`vlan-id`	Nummer des angesprochenen VLAN	1 ... 4094
`interface-type`	Typ der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstelle	

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die ID des angesprochenen IPv4-Adressbands ist konfiguriert.

Sie befinden sich jetzt im DHCPPOOL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-dhcp-pool-<ID>)#
```

Weitere Hinweise

Sie verlassen den DHCPPOOL-Konfigurationsmodus mit dem Befehl `exit`.

Sie löschen den Eintrag mit dem Befehl `no ip dhcp-server pool`.

8.4.2.6 no ip dhcp-server pool

Beschreibung

Mit diesem Befehl löschen Sie das gewünschte IPv4-Adressband.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no ip dhcp-server pool <pool-id (1-8)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`pool-id`	ID des angesprochenen IPv4-Adressbands	1 ... 8

Ergebnis

Das gewünschte IPv4-Adressband ist gelöscht.

Weitere Hinweise

Sie legen das IPv4-Adressband mit dem Befehl `ip dhcp-server pool` an.

8.4.3 Befehle im DHCPPOOL Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im DHCPPOOL-Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl `ip dhcp-server pool` ein, um in diesen Modus zu wechseln.

- Wenn Sie den DHCPPOOL-Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den DHCPPOOL-Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im DHCPPOOL-Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.4.3.1 lease-time

Beschreibung

Mit diesem Befehl legen Sie fest, wie lange die vergebene IPv4-Adresse gültig bleibt. Nachdem die Gültigkeitsdauer zur Hälfte abgelaufen ist, kann der DHCP-Client die vergebene IPv4-Adresse verlängern. Nach Ablauf der gesamten Zeitdauer muss der DHCP-Client eine neue IPv4-Adresse anfordern.

Voraussetzung

Sie befinden sich im DHCPPOOL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
lease-time <seconds (60-31536000)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`seconds`	Zeitdauer bis zur Erneuerung der vergebenen IPv4-Adresse in Sekunden	60 ... 31536000

Ergebnis

Die Zeitdauer ist konfiguriert.

Weitere Hinweise

Sie zeigen die Einstellung mit dem Befehl `show ip dhcp-server pools` an.

8.4.3.2 network

Beschreibung

Mit diesem Befehl konfigurieren Sie das IPv4-Adressband, aus der DHCP-Client eine beliebige IPv4-Adresse erhält.

Hinweis

Maximale Anzahl der IP-Adressen

Die maximale Anzahl der IPv4-Adressen, die der DHCP-Server unterstützt, ist 100. D. h. insgesamt 100 IPv4-Adressen (dynamisch + statisch).

Bei den statischen Zuordnungen können Sie maximal 20 Einträge anlegen.

Vergabe der IP-Adressen

Voraussetzung für die Vergabe ist, dass die IPv4-Adresse der Schnittstelle innerhalb des IPv4-Adressbandes liegt. Wenn das nicht der Fall ist, vergibt die Schnittstelle keine IPv4-Adressen

---

Voraussetzung

Sie befinden sich im DHCPPOOL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
network <lower-IP> <upper-IP> { <subnet-mask> | / <prefix-length (1-32)> }
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`lower-IP`	Anfang des IPv4-Adressebands	Geben Sie eine gültige IPv4-Adresse an.
`upper-IP`	Ende des IPv4-Adressebands	Geben Sie eine gültige IPv4-Adresse an.
`subnet-mask`	Subnetzmaske des zugehörigen Subnetzes	Geben Sie eine gültige Subnetzmaske an
`prefix-length`	Dezimale Darstellung der Maske als Anzahl der "1" Bits	1 ... 32

Ergebnis

Das IPv4-Adressband ist konfiguriert. Die DHCP-Optionen 1, 3, 6, 66 und 67 werden automatisch angelegt. Mit Ausnahme der Option 1 sind die Optionen löschbar.

Hinweis

Unterstützte DHCP-Optionen

Die DHCP-Optionen 1, 2, 3. 4. 5, 6, 42, 66, 67 werden unterstützt.

Weitere Hinweise

Sie zeigen die Einstellung mit dem Befehl `show ip dhcp-server pools` an.

Sie konfigurieren die DHCP-Optionen 1, 3, 4, 5, 6, 42 und 66 mit dem Befehl `option` (IP-Adresse).

Sie konfigurieren die DHCP-Option 2 mit dem Befehl `option value-hex`.

Sie konfigurieren die DHCP-Option 66 und 67 mit dem Befehl `option value-string`.

Sie weisen dem Adressband mit dem Befehl `set interface` eine Schnittstelle zu.

Sie löschen die DHCP-Option mit dem Befehl `no option`.

8.4.3.3 option (IP-Adresse)

Beschreibung

Mit diesem Befehl konfigurieren Sie für die DHCP-Optionen 1, 3, 4, 5, 6, 42 und 66. Wenn die DHCP-Option nicht vorhanden sind, wird der entsprechende Eintrag erstellt.

Voraussetzung

Sie befinden sich im DHCPPOOL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
option <option-code> { <ip-address-list> | int-ip }
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`option-code`	Code der DHCP-Option	Geben Sie eine gültige DHCP-Option an. • 1 - Subnetzmaske • 3 - Router • 4 - Zeitserver • 5 - Namenserver • 6 - DNS Servers • 42 - NTP-Server • 66 - TFTP-Server
`ip-adress-list`	IPv4-Adresse oder IPv4-Adressliste	-
`int-ip`	Verwendet die IPv4-Adresse der Schnittstelle, die dem IPv4-Adressband zugewiesen ist.	Geben Sie die IPv4-Adresse oder die IPv4-Adressliste in. Mehrere IPv4-Adressen werden durch Komma getrennt.

Ergebnis

Die DHCP-Option ist konfiguriert.

Weitere Hinweise

Sie zeigen die Einstellung mit dem Befehl `show ip dhcp-server pools` an.

Sie deaktivieren das IPv4-Adressband mit dem Befehl `no pool-enable`.

Sie löschen die DHCP-Option mit dem Befehl `no option`.

Sie konfigurieren die Schnittstelle mit dem Befehl `set interface`.

8.4.3.4 option value-hex

Beschreibung

Mit diesem Befehl legen Sie DHCP-Optionen an, die als DHCP-Parameter einen hexadezimalen Wert enthalten. Die verschiedenen DHCP-Optionen sind im RFC 2132 definiert.

Ausgenommen davon sind die DHCP-Optionen: 1, 3, 12, 66 und 67. Die DHCP-Optionen 3, 6 und 66 konfigurieren Sie mit dem Befehl `option` (IP-Adresse) und die DHCP-Optionen 12 und 67 mit dem Befehl `option value-string`.

Voraussetzung

Sie befinden sich im DHCPPOOL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
option <option-code> value-hex <dhcp-param>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`option-code`	Code der DHCP-Option	Geben Sie eine gültige DHCP-Option an. Folgende DHCP-Optionen werden nicht unterstützt: • 50 - 60 • 255
`dhcp-param`	DHCP-Parameter in hexadezimal	Geben Sie einen gültigen hexadezimal Wert an. Format: XXXXX z. B. C0A86402

Ergebnis

Die DHCP-Option ist konfiguriert. Insgesamt sind maximal 20 DHCP-Optionen möglich.

Weitere Hinweise

Sie zeigen die Einstellung mit dem Befehl `show ip dhcp-server-pools` an.

Sie deaktivieren das IPv4-Adressband mit dem Befehl `no pool-enable`.

Sie löschen die DHCP-Option mit dem Befehl `no option`.

8.4.3.5 option value-string

Beschreibung

Mit diesem Befehl konfigurieren Sie DHCP-Optionen 12, 66 und 67, die als DHCP-Parameter einen String enthalten. Die DHCP-Optionen 66 und 67 werden automatisch beim Erstellen des IPv4-Adressbands angelegt.

Voraussetzung

Sie befinden sich im DHCPPOOL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
option <option-code> value-string <dhcp-param>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`option-code`	Code der DHCP-Option	• 12 - Hostname • 66 - TFTP-Server • 67 - Bootfilename
`dhcp-param`	Name der Datei	Geben Sie den Namen im String-Format an.

Ergebnis

Die DHCP-Option ist konfiguriert.

Weitere Hinweise

Sie zeigen die Einstellung mit dem Befehl `show ip dhcp-server pools` an.

Sie löschen die DHCP-Option mit dem Befehl `no option`.

Sie konfigurieren die DHCP-Optionen 3 und 6 mit dem Befehl `option` (IP-Adresse).

Sie deaktivieren das IPv4-Adressband mit dem Befehl `no pool-enable`.

8.4.3.6 no option

Beschreibung

Mit diesem Befehl löschen Sie die DHCP-Option mit der angegebenen Nummer.

Voraussetzung

Sie befinden sich im DHCPPOOL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no option <option-code>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`option-code`	Code der DHCP-Option	Geben Sie einen gültigen DHCP-Optionscode an. • 2 - Offset-Zeit • 3 - Router • 4 - Zeitserver • 5 - Namenserver • 6 - DNS Servers • 42 - NTP-Server • 66 - TFTP-Server • 67 - Bootfilename

Ergebnis

Die angegebene DHCP-Option ist gelöscht.

Weitere Hinweise

Sie konfigurieren die DHCP-Optionen mit einem String mit dem Befehl `option value-string`.

Sie konfigurieren DHCP-Optionen mit hexadezimalen Wert mit dem Befehl `option value-hex`.

Sie konfigurieren die DHCP-Optionen mit IPv4-Adresse mit dem Befehl `option (IP-Adresse)`.

8.4.3.7 pool-enable

Beschreibung

Mit diesem Befehl legen Sie fest, dass dieses IPv4-Adressband verwendet wird.

Voraussetzung

Sie befinden sich im DHCPPOOL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
pool-enable
```

Ergebnis

Die Einstellung ist aktiviert.

Hinweis

Wenn das IPv4-Adressband aktiviert ist, lassen sich folgende Parameter nicht mehr editieren:

- DHCP-Optionen (`option` ...)
- Statische Zurodnungen (`static-lease`)

Weitere Hinweise

Sie zeigen die Einstellung mit dem Befehl `show ip dhcp-server pools` an.

Sie deaktivieren die Einstellung mit dem Befehl `no pool-enable`.

8.4.3.8 no pool-enable

Beschreibung

Mit diesem Befehl legen Sie fest, dass dieses IPv4-Adressband nicht verwendet wird.

Hinweis

DHCP-Server-Zuordnungen löschen

Wenn Sie ein IPv4-Adressband deaktivieren bzw. löschen oder den DHCP-Server aus- und wieder einschalten, werden die DHCP-Server-Zuordnungen gelöscht. Sie zeigen die DHCP-Server-Zuordnungen mit dem Befehl `show ip dhcp-server bindings` an.

Voraussetzung

Sie befinden sich im DHCPPOOL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no pool-enable
```

Ergebnis

Die Einstellung ist deaktiviert.

Weitere Hinweise

Sie zeigen die Einstellung mit dem Befehl `show ip dhcp-server pools` an.

Sie aktivieren die Einstellung mit dem Befehl `pool-enable`.

8.4.3.9 set-interface

Beschreibung

Mit diesem Befehl legen Sie die Schnittstelle fest, über die die IPv4-Adressen dynamisch vergeben werden.

Hinweis

Vergabe der IP-Adressen

Bei der Vergabe von IP-Adressen aus einem lokalen Adressband, muss die IPv4-Adresse der Schnittstelle innerhalb des IPv4-Adressbands liegt. Wenn das nicht der Fall ist, vergibt die Schnittstelle keine IPv4-Adressen.

Die IP-Adresse der Schnittstelle muss nicht innerhalb des IPv4-Adressbands liegen, wenn für das Adressband Relay Agent-Informationen konfiguriert sind.

Voraussetzung

Sie befinden sich im DHCPPOOL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
set-interface {vlan <vlan-id (1-4094)> | <interface-type> <interface-id> }
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vlan`	Schlüsselwort für eine VLAN-Verbindung	-
`vlan-id`	Nummer des angesprochenen VLAN	1 ... 4094
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an
`interface-id`	Modul-Nr.und Port-Nr. der Schnittstelle	

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Das Schnittstelle ist zugewiesen. Damit das IPv4-Adressband verwendet wird, muss es noch aktiviert werden.

Weitere Hinweise

Sie zeigen die Einstellung mit dem Befehl `show ip dhcp-server pools` an.

Sie aktivieren das IPv4-Adressband mit dem Befehl `pool-enable`.

8.4.3.10 static-lease

Beschreibung

Mit diesem Befehl legen Sie fest, dass bestimmten Geräten eine bestimmte IP-Adresse zugeordnet wird. Die Adresszuordnung erfolgt anhand der MAC-Adresse, anhand der Client-ID oder anhand der DUID.

Voraussetzung

- Die Zuordnung ist noch nicht angelegt.
- Sie befinden sich im DHCPPOOL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-dhcp-pool-<ID>)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
static-lease {mac <mac-address> | client-id <string> | client-id-duid <hex_str> }
<ip-address>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`mac`	Schlüsselwort für eine MAC-Adresse	-
`mac-address`	Unicast MAC-Adresse	Geben Sie die MAC-Adresse an. aa:bb:cc:dd:ee:ff
`client-id`	Schlüsselwort für eine DHCP-Client-ID	-
`string`	Frei definierbare DHCP-Client-ID	Geben Sie die gewünschte Bezeichnung ein. Maximal 254 Zeichen
`client-id-duid`	Schlüsselwort für eine DUID	-

Parameter	Beschreibung	Wertebereich/Anmerkung
`hex_str`	DHCP Unique Identifier	Geben Sie die DUID an.
`ip-address`	Unicast IPv4-Adresse	Geben Sie eine gültige IPv4-Adresse an. Die IPv4-Adresse muss zum Subnetz des IPv4-Adressbands passen.

Ergebnis

Die Zuordnung ist festgelegt.

Weitere Hinweise

Sie zeigen die Einstellung mit dem Befehl `show ip dhcp dhcp-server bindings` an.

Sie deaktivieren das IPv4-Adressband mit dem Befehl `no pool-enable`.

Sie löschen die Zuordnung mit dem Befehl `no static-lease`.

8.4.3.11 no static-lease

Beschreibung

Mit diesem Befehl löschen Sie die Zuordnung einer IPv4-Adresse.

Voraussetzung

Sie befinden sich im DHCPPOOL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no static-lease { mac <mac-address> | client-id <string> | client-id-duid <hex_str> }
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`mac`	Schlüsselwort für eine MAC-Adresse	-
`mac-address`	Unicast MAC-Adresse	Geben Sie die MAC-Adresse an. aa:bb:cc:dd:ee:ff
`client-id`	Schlüsselwort für eine DHCP-Client-ID	-
`string`	Frei definierbare DHCP-Client-ID	Geben Sie die gewünschte Bezeichnung ein.
`client-id-duid`	Schlüsselwort für eine DUID	-
`hex_str`	DHCP Unique Identifier	Geben Sie die DUID an.

Ergebnis

Die Zuordnung ist gelöscht.

Weitere Hinweise

Sie konfigurieren die Zuordnung mit dem Befehl `static-lease`.

8.5 DNS

In diesem Kapitel werden Befehle des Domain Name System (DNS) beschrieben.

8.5.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.5.1.1 show dnsclient information

Beschreibung

Dieser Befehl zeigt die Konfiguration des DNS-Clients an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show dnsclient information
```

Ergebnis

Die Informationen werden angezeigt.

8.5.1.2 show ddnsclient information

Beschreibung

Dieser Befehl zeigt die Konfiguration des dynamischen DNS-Clients an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show ddnsclient overview
```

Ergebnis

Die Konfiguration wird angezeigt.

8.5.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.5.2.1 dnsclient

Beschreibung

Mit diesem Befehl wechseln Sie in den DNS CLIENT-Konfigurationsmodus.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
dnsclient
```

Ergebnis

Sie befinden sich jetzt im DNS CLIENT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-dnsclient)#
```

Weitere Hinweise

Sie verlassen den DNS CLIENT-Konfigurationsmodus mit dem Befehl `end` oder `exit`.

8.5.2.2 dnsproxy

Beschreibung

Mit diesem Befehl wechseln Sie in den DNS PROXY-Konfigurationsmodus.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
dnsproxy
```

Ergebnis

Sie befinden sich jetzt im DNS PROXY-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-dnsproxy)#
```

Weitere Hinweise

Sie verlassen den DNS PROXY-Konfigurationsmodus mit dem Befehl `end` oder `exit`.

8.5.2.3 ddnsclient

Beschreibung

Mit diesem Befehl wechseln Sie in den DDNS Client-Konfigurationsmodus.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
ddnsclient
```

Ergebnis

Sie befinden sich jetzt im DDNS Client-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ddnsclient)#
```

Weitere Hinweise

Sie verlassen den DDNS Client-Konfigurationsmodus mit dem Befehl `end` oder `exit`.

8.5.3 Befehle im DNS CLIENT-Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im DNS CLIENT-Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl `dnsclient` ein, um in diesen Modus zu wechseln.

- Wenn Sie den DNS CLIENT-Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den DNS CLIENT-Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

8.5.3.1 manual srv

Beschreibung

Mit diesem Befehl legen Sie einen manuell projektierten DNS-Server fest. Maximal drei DNS-Server sind projektierbar.

Voraussetzung

Sie befinden sich im DNS CLIENT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-dnsclient)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
manual srv <ip_addr>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ip_addr`	IPv4-Adresse	Geben Sie eine gültige IPv4-Adresse an.

Ergebnis

Der DNS-Server ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show dnsclient informationen` an.

Sie konfigurieren den DNS-Servertyp mit dem Befehl `server type`.

Sie löschen den DNS-Server mit dem Befehl no `manual`.

8.5.3.2 no manual srv

Beschreibung

Mit diesem Befehl löschen Sie einen bestimmten DNS-Server oder alle DNS-Server.

Voraussetzung

Sie befinden sich im DNS CLIENT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-dnsclient)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no manual {srv <ip_addr>|all}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`srv`	Schlüsselwort für DNS-Server	-
`ip address`	IPv4-Adresse	Geben Sie die IPv4-Adresse des DNS-Servers an.
`all`	Löscht alle DNS-Server	-

Ergebnis

Der angegebene DNS-Server ist gelöscht.

Weitere Hinweise

Sie erstellen einen DNS-Server-Eintrag mit dem Befehl `manual srv`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show dnsclient information` an.

8.5.3.3 server type

Beschreibung

Mit diesem Befehl legen Sie fest, welche DNS-Server das Gerät verwendet.

Voraussetzung

Sie befinden sich im DNS CLIENT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-dnsclient)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
server type {all | manual | learned}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`all`	Das Gerät verwendet alle verfügbaren DNS-Server.	Default
`manual`	Das Gerät verwendet nur die manuell projektierten DNS-Server.	-
`learned`	Das Gerät verwendet die DNS-Server, die automatisch übermittelt werden.	-

Ergebnis

Das Gerät verwendet die festgelegten DNS-Server.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show dnsclient information` an.

Sie erstellen einen manuell projektierten DNS-Server mit dem Befehl `manual srv`.

8.5.3.4 shutdown

Beschreibung

Mit diesem Befehl beenden Sie den DNS-Client.

Voraussetzung

Sie befinden sich im DNS CLIENT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-dnsclient)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
shutdown
```

Ergebnis

Der DNS-Client ist beendet.

Weitere Hinweise

Sie starten den DNS-Client mit dem Befehl `no shutdown`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show dnsclient information` an.

8.5.3.5 no shutdown

Beschreibung

Mit diesem Befehl starten Sie den DNS-Client des Geräts. Um diese Funktion nutzen zu können, muss ein DNS-Server erreichbar sein.

Voraussetzung

Sie befinden sich im DNS CLIENT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-dnsclient)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no shutdown
```

Ergebnis

Der DNS-Client des Geräts ist aktiviert und richtet bei Bedarf Anfragen an den DNS-Server.

Weitere Hinweise

Sie beenden den DNS-Client mit dem Befehl `shutdown`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show dnsclient information` an.

8.5.4 Befehle im DNS PROXY-Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im DNS PROXY-Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl `dnsproxy` ein, um in diesen Modus zu wechseln.

- Wenn Sie den DNS PROXY-Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den DNS PROXY-Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

8.5.4.1 cachenxdomain

Beschreibung

Mit diesem Befehl aktivieren Sie das Zwischenspeichern von NXDOMAIN-Antworten. Damit verbleiben die Domain-Namen im Cache, die dem DNS-Server unbekannt waren.

Voraussetzung

Sie befinden sich im DNS PROXY-Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(config-dnsproxy)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
cache nxdomain
```

Ergebnis

Die Einstellung ist aktiviert.

Weitere Hinweise

Sie deaktivieren die Einstellung mit dem Befehl `no cachenxdomain`.

8.5.4.2 no cachenxdomain

Beschreibung

Mit diesem Befehl deaktivieren Sie das Zwischenspeichern von NXDOMAIN-Antworten.

Voraussetzung

Sie befinden sich im DNS PROXY-Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(config-dnsproxy)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no cache nxdomain
```

Ergebnis

Die Einstellung ist deaktiviert.

Weitere Hinweise

Sie aktivieren die Einstellung mit dem Befehl `cachenxdomain`.

8.5.4.3 shutdown

Beschreibung

Mit diesem Befehl deaktivieren Sie den Proxy des DNS-Servers.

Voraussetzung

Sie befinden sich im DNS PROXY-Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(config-dnsproxy)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
shutdown
```

Ergebnis

Die Einstellung ist deaktiviert.

Weitere Hinweise

Sie aktivieren die Einstellung mit dem Befehl `no shutdown`.

8.5.4.4 no shutdown

Beschreibung

Mit diesem Befehl aktivieren Sie den Proxy des DNS-Servers.

Voraussetzung

Sie befinden sich im DNS PROXY-Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(config-dnsproxy)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no shutdown
```

Ergebnis

Die Einstellung ist aktiviert.

Weitere Hinweise

Sie deaktivieren die Einstellung mit dem Befehl `shutdown`.

8.5.5 Befehle im DDNS Client-Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im DDNS CLIENT-Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl `ddnsclient` ein, um in diesen Modus zu wechseln.

- Wenn Sie den DDNS CLIENT-Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den DDNS CLIENT-Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

8.5.5.1 service

Beschreibung

Mit diesem Befehl aktivieren Sie den dynamischen DNS-Anbieter.

Voraussetzung

Sie befinden sich im DDNS Client-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ddnsclient)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
service {show-services | <index>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich
`show-services`	Listet die verfügbaren Anbieter auf.	-
`index`	Nummer, die einem bestimmten Anbieter entspricht.	Geben Sie eine gültige Nummer an.

Ergebnis

Der angegebene Eintrag ist aktiviert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ddnsclient information` an.

Sie deaktivieren einen Eintrag mit dem Befehl `no service`.

8.5.5.2 no service

Beschreibung

Mit diesem Befehl deaktivieren Sie den dynamischen DNS-Anbieter.

Voraussetzung

Sie befinden sich im DDNS Client-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ddnsclient)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no service {show-services | <index>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich
`show-services`	Listet die verfügbaren Anbieter auf.	-
`index`	Nummer, die einem bestimmten Anbieter entspricht.	Geben Sie eine gültige Nummer an.

Ergebnis

Der angegebene Eintrag ist deaktiviert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ddnsclient information` an.

Sie aktivieren einen Eintrag mit dem Befehl `no service`.

8.5.5.3 userhost

Beschreibung

Mit diesem Befehl konfigurieren Sie den Hostnamen, den Sie für das Gerät mit Ihrem dynamischen DNS-Anbieter vereinbart haben, z. B. example.no-ip.com.

Voraussetzung

Sie befinden sich im DDNS Client-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ddnsclient)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
userhost {show-services | <index> <host>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`show-services`	Listet die verfügbaren Anbieter auf.	-
`index`	Nummer, die einem bestimmten Anbieter entspricht.	Geben Sie eine gültige Nummer an.
`host`	Hostnamen	Geben Sie den vereinbarten Hostnamen an.

Ergebnis

Der Hostname ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ddnsclient information` an.

Sie konfigurieren den Benutzernamen mit dem Befehl `username`.

Sie konfigurieren das Passwort mit dem Befehl `password`.

8.5.5.4 username

Beschreibung

Mit diesem Befehl konfigurieren Sie den Benutzernamen, mit dem sich das Gerät am dynamischen DNS-Server anmeldet.

Voraussetzung

Sie befinden sich im DDNS Client-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ddnsclient)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
username {show-services | <index> <username>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`show-services`	Listet die verfügbaren Anbieter auf.	-
`index`	Nummer, die einem bestimmten Anbieter entspricht.	Geben Sie eine gültige Nummer an.
`username`	Benutzernamen	Geben Sie den vereinbarten Benutzernamen an.

Ergebnis

Der Benutzername ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ddnsclient information` an.

Sie konfigurieren das Passwort mit dem Befehl `password`.

8.5.5.5 password

Beschreibung

Mit diesem Befehl konfigurieren Sie das Passwort, mit dem sich das Gerät am dynamischen DNS-Server anmeldet.

Voraussetzung

Sie befinden sich im DDNS Client-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ddnsclient)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
password {show-services | <index> <password>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`show-services`	Listet die verfügbaren Anbieter auf.	-
`index`	Nummer, die einem bestimmten Anbieter entspricht.	Geben Sie eine gültige Nummer an.
`password`	Passwort	Geben Sie das vereinbarte Passwort an.

Ergebnis

Das Passwort ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ddnsclient information` an.

Sie konfigurieren den Benutzernamen mit dem Befehl `username`.

8.6 SNMP

In diesem Kapitel werden Befehle des Simple Network Management Protocol (SNMP) beschrieben.

Beispielkonfiguration

IP-Konfiguration

Legen Sie die IP-Adresse des Geräts fest, die zu dem verwendeten SNMP-Trap-Empfänger passt.

Führen Sie folgende Befehle aus:

```
configure terminal
int vlan 1
no ip address
ip address 192.168.1.1 255.255.255.0
end
```

Trap-Konfiguration für SNMPv2c-Benachrichtigungen

Um den Versand von SNMP-Traps zu konfigurieren, wird zunächst eine SNMP-Community benötigt.

Diese Community wird zusammen mit weiteren SNMP-Parametern benutzt, um Traps an einen Trap-Empfänger zu senden.

Die Auswahl des Trap-Empfängers erfolgt über Tags, die beim Aufruf von SNMP-Benachrichtigungen gesetzt werden.

Führen Sie folgende Befehle aus:

```
configure terminal
snmp community index v2trapindex name public security v2secname
snmp targetaddr trapringer param pav2c ipv4 192.168.1.254 taglist publictrapv2tag
snmp targetparams pav2c user v2secname security-model v2c message-processing v2c
snmp notify testnotify tag publictrapv2tag type trap
end
```

Event-Konfiguration

Aktivieren Sie den Versand von Traps.

Führen Sie folgende Befehle aus:

```
configure terminal
events
client config trap
end
```

Für Systemmeldungen werden immer alle konfigurierten SNMP-Benachrichtigungen aufgerufen.

Bei RMON-Events muss die aufzurufende SNMP-Benachrichtigung explizit konfiguriert werden, siehe hierzu Kapitel "RMON".

8.6.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.6.1.1 show snmp

Beschreibung

Dieser Befehl zeigt die Statusinformationen des SNMP an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show snmp
```

Ergebnis

Die Statusinformationen werden angezeigt.

8.6.1.2 show snmp community

Beschreibung

Dieser Befehl zeigt die Details der konfigurierten SNMP-Communities an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show snmp community
```

Ergebnis

Die Details der konfigurierten SNMP-Communities werden angezeigt.

8.6.1.3 show snmp engineID

Beschreibung

Dieser Befehl zeigt die SNMP-Identifikationsnummer des Geräts an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show snmp engineID
```

Ergebnis

Die SNMP-Identifikationsnummer des Geräts wird angezeigt.

8.6.1.4 show snmp filter

Beschreibung

Dieser Befehl zeigt die konfigurierten SNMP-Filter an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show snmp filter
```

Ergebnis

Die konfigurierten SNMP-Filter werden angezeigt.

8.6.1.5 show snmp group

Beschreibung

Dieser Befehl zeigt die konfigurierten SNMP-Gruppen an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show snmp group
```

Ergebnis

Die konfigurierten SNMP-Gruppen werden angezeigt.

8.6.1.6 show snmp group access

Beschreibung

Dieser Befehl zeigt die Rechte der konfigurierten SNMP-Gruppen an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show snmp group access
```

Ergebnis

Die Rechte der konfigurierten SNMP-Gruppen werden angezeigt.

8.6.1.7 show snmp inform statistics

Beschreibung

Dieser Befehl zeigt die Statistik der "Inform Messages" an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show snmp inform statistics
```

Ergebnis

Die Statistik der "Inform Messages" wird angezeigt.

8.6.1.8 show snmp notif

Beschreibung

Mit diesem Befehl zeigen Sie die konfigurierten SNMP-Benachrichtigungstypen an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show snmp notif
```

Ergebnis

Die konfigurierten SNMP-Benachrichtigungstypen werden angezeigt.

8.6.1.9 show snmp targetaddr

Beschreibung

Dieser Befehl zeigt die konfigurierten SNMP-Zieladressen an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show snmp targetaddr
```

Ergebnis

Die konfigurierten SNMP-Zieladressen werden angezeigt.

8.6.1.10 show snmp targetparam

Beschreibung

Dieser Befehl zeigt die konfigurierten SNMP-Zielparameter an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show snmp targetparam
```

Ergebnis

Die konfigurierten SNMP-Zielparameter werden angezeigt.

8.6.1.11 show snmp tcp

Beschreibung

Dieser Befehl zeigt die Konfiguration für SNMP über TCP an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show snmp tcp
```

Ergebnis

Die Konfiguration für SNMP über TCP wird angezeigt.

8.6.1.12 show snmp user

Beschreibung

Dieser Befehl zeigt die Einstellungen für die SNMP-Benutzer an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show snmp user
```

Ergebnis

Die Einstellungen für die SNMP-Benutzer werden angezeigt.

8.6.1.13 show snmp viewtree

Beschreibung

Dieser Befehl zeigt die Einstellungen für die SNMP-Baumansicht an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show snmp viewtree
```

Ergebnis

Die Einstellungen für die SNMP-Baumansicht werden angezeigt.

8.6.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.6.2.1 snmpagent

Beschreibung

Mit diesem Befehl aktivieren Sie die SNMP Agent-Funktion.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
snmpagent
```

Ergebnis

Die SNMP Agent-Funktion ist aktiviert.

Weitere Hinweise

Sie deaktivieren die SNMP Agent-Funktion mit dem Befehl `no snmpagent`.

8.6.2.2 no snmpagent

Beschreibung

Mit diesem Befehl deaktivieren Sie die SNMP Agent-Funktion.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no snmpagent
```

Ergebnis

Die SNMP Agent-Funktion ist deaktiviert.

Weitere Hinweise

Sie aktivieren die SNMP Agent-Funktion mit dem Befehl `snmpagent`.

8.6.2.3 snmp agent version

Beschreibung

Mit diesem Befehl konfigurieren Sie, ob alle SNMP-Anfragen oder nur SNMPv3-Anfragen bearbeitet werden.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
snmp agent version {v3only|all}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`v3only`	Nur SNMPv3-Anfragen werden bearbeitet.	-
`all`	Alle SNMP-Anfragen werden bearbeitet.	Default: all

Ergebnis

Die Einstellung ist konfiguriert.

8.6.2.4 snmp access

Beschreibung

Mit diesem Befehl konfigurieren Sie den Zugang zu einer SNMP-Gruppe.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
snmp access <GroupName> {v1|v2c|v3 {auth|noauth|priv}}
 [read <ReadView|none>][write <WriteView|none>][notify <NotifyView|none>]
 [{volatile|nonvolatile}]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`GroupName`	Name der Gruppe, zu der der Zugang konfiguriert wird	max. 32 Zeichen
Version	Wählt die verwendete Version des Protokolls aus.	• `v1` • `v2c` • `v3`

Parameter	Beschreibung	Wertebereich/Anmerkung
Authentifizierung	Wählt die Authentifizierungsmethode aus.	• `auth` Aktiviert MD5 oder SHA als Authentifizierungsmethode • `noauth` Keine Authentifizierung • `priv` Aktiviert Authentifizierung und Verschlüsselung
`read`	Die Daten können gelesen werden. Schlüsselwort	• `ReadView` • `none`
`write`	Die Daten können gelesen und geschrieben werden. Schlüsselwort	• `WriteView` • `none`
`notify`	Änderungen können als Tag versendet werden. Schlüsselwort	• `NotifyView` • `none`
Storage Type	Gibt an, ob die Einstellungen nach einem Neustart bestehen bleiben.	• `volatile` (flüchtig): Bei einem Neustart gehen die Einstellungen verloren. • `nonvolatile` (nicht flüchtig): Bei einem Neustart bleiben die Einstellungen erhalten.

Die Schlüsselworte müssen angegeben werden.

Wenn beim Konfigurieren einer Gruppe optionale Parameter nicht angegeben werden, wird der voreingestellte Wert verwendet.

Ergebnis

Die Einstellungen für den Zugang zu einer SNMP-Gruppe sind konfiguriert.

Weitere Hinweise

Sie löschen den Zugang zu einer SNMP-Gruppe mit dem Befehl `no snmp access`.

Sie zeigen die konfigurierten SNMP-Gruppen mit dem Befehl `show snmp group` an.

Sie zeigen Zugangskonfigurationen zu SNMP-Gruppen mit dem Befehl `show snmp group access` an.

Sie zeigen die konfigurierten SNMP-Baumansichten mit dem Befehl `show snmp viewtree` an.

8.6.2.5 no snmp access

Beschreibung

Mit diesem Befehl löschen Sie den Zugang zu einer SNMP-Gruppe.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no snmp access <GroupName> {v1|v2c|v3 {auth|noauth|priv}}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`GroupName`	Name der Gruppe, zu der der Zugang gelöscht wird	max. 32 Zeichen
Version	Wählt die verwendete Version des Protokolls aus.	• `v1` • `v2c` • `v3`
Authentifizierung	Wählt die Authentifizierungsmethode aus.	• `auth` • `noauth` • `priv`

Ergebnis

Der Zugang zu einer SNMP-Gruppe ist gelöscht.

Weitere Hinweise

Sie konfigurieren die Einstellung mit dem Befehl `snmp access`.

Sie zeigen die konfigurierten SNMP-Gruppen mit dem Befehl `show snmp group` an.

Sie zeigen Zugangskonfigurationen zu SNMP-Gruppen mit dem Befehl `show snmp group access` an.

Sie zeigen die konfigurierten SNMP-Baumansichten mit dem Befehl `show snmp viewtree` an.

8.6.2.6 snmp community index

Beschreibung

Mit diesem Befehl konfigurieren Sie die Details einer SNMP-Community.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
snmp community index <CommunityIndex> name <CommunityName>
   security <SecurityName> [context <Name>][{volatile|nonvolatile}]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`CommunityIndex`	Index der Community	Max. 256 Zeichen
`name`	Schlüsselwort für den Namen der Community	-
`CommunityName`	Name der Community	Max. 256 Zeichen
`security`	Schlüsselwort für den Sicherheitsnamen	-
`SecurityName`	Sicherheitsname	Max. 32 Zeichen
`context`	Schlüsselwort für den Kontextnamen	-
`Name`	Kontextname	Max. 32 Zeichen
Storage Type	Gibt an, ob die Einstellungen nach einem Neustart bestehen bleiben.	• `volatile` (flüchtig): Bei einem Neustart gehen die Einstellungen verloren. • `nonvolatile` (nicht flüchtig): Bei einem Neustart bleiben die Einstellungen erhalten.

Wenn beim Konfigurieren einer Community optionale Parameter nicht angegeben werden, gelten die voreingestellten Werte.

Hinweis

Community String

Verwenden Sie aus Sicherheitsgründen nicht die Standardwerte "public" oder "private". Ändern Sie die Community Strings nach der Erst-Installation.

Die empfohlene Mindestlänge für Community Strings sind 6 Zeichen.

Ergebnis

Die Einstellungen sind konfiguriert.

Weitere Hinweise

Sie löschen die Details einer SNMP-Community mit dem Befehl `no snmp community index`.

Sie zeigen die Details einer SNMP-Community mit dem Befehl `show snmp community` an.

Sie zeigen die Statusinformationen der SNMP-Kommunikation mit dem Befehl `show snmp` an.

8.6.2.7 no snmp community index

Beschreibung

Mit diesem Befehl löschen Sie die Details einer SNMP-Community.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no snmp community index <CommunityIndex>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`CommunityIndex`	Name der Community	max. 32 Zeichen

Ergebnis

Die Details einer SNMP-Community sind gelöscht.

Weitere Hinweise

Sie konfigurieren die Details einer SNMP-Community mit dem Befehl `snmp community index`.

Sie zeigen die Details einer SNMP-Community mit dem Befehl `show snmp community` an.

Sie zeigen die Statusinformationen der SNMP-Kommunikation mit dem Befehl `show snmp` an.

8.6.2.8 snmp filterprofile

Beschreibung

Mit diesem Befehl konfigurieren Sie einen Filter, der die Zugriffsrechte auf den MIB Baum beschreibt.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
snmp filterprofile <profile-name> <OIDTree> [mask<OIDMask>]
     {included|excluded}[{volatile|nonvolatile}]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`profile-name`	Name des Filterprofils	max. 32 Zeichen
`OIDTree`	Objekt ID	Pfadangabe des MIB Baums
`mask`	Schlüsselwort für die OID Maske	-
`OIDMask`	Maske, die den Zugriff auf die Elemente des MIB Baums filtert	Folge von "`0`" und "`1`", durch Punkte getrennt, entsprechend der Pfadangabe des MIB-Baums
-	gibt an, ob die gefilterten Elemente verwendet oder ausgeschlossen werden	• `included` • `excluded`
-	gibt an, ob die Einstellungen nach einem Neustart bestehen bleiben:	• `volatile` (flüchtig): bei einem Neustart werden die Standardeinstellungen verwendet • `nonvolatile` (nicht flüchtig): bei einem Neustart werden die gespeicherten Einstellungen verwendet

Beachten Sie, dass die Bedeutung der Filtermaske in Abhängigkeit vom "`included`/`excluded`" Parameter wechselt:

- ...`0`... und "`included`" bedeutet: Zugriff verweigert
- ...`0`... und "`excluded`" bedeutet: Zugriff gestattet
- ...`1`... und "`included`" bedeutet: Zugriff gestattet
- ...`1`... und "`excluded`" bedeutet: Zugriff verweigert

Ergebnis

Der Filter ist erstellt.

Weitere Hinweise

Sie löschen einen Filter mit dem Befehl `no snmp filterprofile`.

Sie zeigen die erstellten Filter mit dem Befehl `show snmp filter` an.

8.6.2.9 no snmp filterprofile

Beschreibung

Mit diesem Befehl löschen Sie einen Filter.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no snmp filterprofile <profilename> <OIDTree>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`profilename`	Name des Filterprofils	max. 32 Zeichen
`OIDTree`	Objekt ID	Pfadangabe des MIB Baums

Ergebnis

Der Filter ist gelöscht.

Weitere Hinweise

Sie erstellen einen Filter mit dem Befehl `snmp filterprofile`.

Sie zeigen die erstellten Filter mit dem Befehl `show snmp filter` an.

8.6.2.10 snmp group

Beschreibung

Mit diesem Befehl konfigurieren Sie die Details einer SNMP-Gruppe.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
snmp group <GroupName> user <UserName> security-model {v1|v2c|v3}
   [{volatile|nonvolatile}]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`GroupName`	Bezeichnung des Gruppennamen	max. 32 Zeichen
`user`	Schlüsselwort für den Usernamen	-
`UserName`	Bezeichnung des Usernamen	max. 32 Zeichen
`security-model`	Gibt an, welche Sicherheitseinstellungen verwendet werden.	• `v1` • `v2c` • `v3`
Storage Type	Gibt an, ob die Einstellungen nach einem Neustart bestehen bleiben.	• `volatile` (flüchtig): Bei einem Neustart gehen die Einstellungen verloren. • `nonvolatile` (nicht flüchtig): Bei einem Neustart bleiben die Einstellungen erhalten.

Wenn beim Konfigurieren einer Gruppe optionale Parameter nicht angegeben werden, gelten die voreingestellten Werte.

Ergebnis

Die Details der Gruppe sind konfiguriert.

Weitere Hinweise

Sie löschen die Details einer SNMP-Gruppe mit dem Befehl `no snmp group`.

Sie zeigen die erstellten SNMP-Gruppen mit dem Befehl `show snmp group` an.

Sie zeigen die erstellten SNMP-Benutzer mit dem Befehl `show snmp user` an.

8.6.2.11 no snmp group

Beschreibung

Mit diesem Befehl löschen Sie die Details einer SNMP-Gruppe.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no snmp group <GroupName> user <UserName> security-model {v1|v2c|v3}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`GroupName`	Bezeichnung des Gruppennamen	max. 32 Zeichen
`user`	Schlüsselwort für den Usernamen	-
`UserName`	Bezeichnung des Usernamen	max. 32 Zeichen
`security-model`	Gibt an, mit welchen Sicherheitseinstellungen gesendet wird.	• `v1` • `v2c` • `v3`

Ergebnis

Die Details der Gruppe sind gelöscht.

Weitere Hinweise

Sie ändern die Details einer SNMP-Gruppe mit dem Befehl `snmp group`.

Sie zeigen die erstellten SNMP-Gruppen mit dem Befehl `show snmp group` an.

Sie zeigen die erstellten SNMP-Benutzer mit dem Befehl `show snmp user` an.

8.6.2.12 snmp notify

Beschreibung

Mit diesem Befehl konfigurieren Sie die Details der SNMP-Benachrichtigungen.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
snmp notify <NotifyName> tag <TagName> type {Trap|Inform}
   [{volatile|nonvolatile}]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`NotifyName`	Name der SNMP-Benachrichtigung	max. 32 Zeichen
`tag`	Schlüsselwort für einen Zielschlüssel	-
`TagName`	Name des Zielschlüssel	max. 32 Zeichen
`Type`	Typ der SNMP-Benachrichtigung	• `Trap` Generiert einen Trap. • `Inform` Erzeugt einen Logbucheintrag bzw. sendet einen Eintrag an den Log-Server.
Storage Type	Gibt an, ob die Einstellungen nach einem Neustart bestehen bleiben.	• `volatile` (flüchtig): Bei einem Neustart gehen die Einstellungen verloren. • `nonvolatile` (nicht flüchtig): Bei einem Neustart bleiben die Einstellungen erhalten.

Ergebnis

Die Details der SNMP-Benachrichtigungen sind konfiguriert.

Weitere Hinweise

Sie löschen die Details einer SNMP-Benachrichtigung mit dem Befehl `no snmp notify`.

Sie zeigen die konfigurierten SNMP-Benachrichtigungen mit dem Befehl `show snmp notif` an.

Sie zeigen die konfigurierten SNMP-Zieladressen mit dem Befehl `show snmp targetaddr` an.

8.6.2.13 no snmp notify

Beschreibung

Mit diesem Befehl löschen Sie die Details der SNMP-Benachrichtigungen.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no snmp notify <NotifyName>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`NotifyName`	Name der Benachrichtigung	max. 32 Zeichen

Ergebnis

Die Details der SNMP-Benachrichtigungen sind gelöscht.

Weitere Hinweise

Sie ändern die Details einer SNMP-Gruppe mit dem Befehl `snmp notify`.

Sie zeigen die konfigurierten SNMP-Benachrichtigungen mit dem Befehl `show snmp notif` an.

Sie zeigen die konfigurierten SNMP-Zieladressen mit dem Befehl `show snmp targetaddr` an.

8.6.2.14 snmp targetaddr

Beschreibung

Mit diesem Befehl konfigurieren Sie die SNMP-Zieladresse.

Voraussetzung

Die SNMP-Zielparameter sind konfiguriert.

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
snmp targetaddr <TargetAddressName> param <ParamName>  {ipv4<IPAddress>}
 [timeout <Seconds(1-1500)] [retries <RetryCount(1-3)]
 [taglist <TagIdentifier | none>]  [{volatile | nonvolatile}]
 [port <integer (1-65535)>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich
`TargetAddressName`	Name der Zieladresse	max. 32 Zeichen
`param`	Schlüsselwort für den Parameternamen	-
`ParamName`	Name der Zieladresse bzw. Bezeichnung des Parameternamens	max. 32 Zeichen
`ipv4`	Schlüsselwort für eine IPv4-Adresse	-
`IPAddress`	Wert für eine IPv4-Unicast-Adresse	Geben Sie eine gültige IPv4-Unicast-Adresse an.
`timeout`	Schlüsselwort für die Zeit, die der SNMP Agent auf eine Antwort wartet, bevor er die Inform Request Message erneut sendet	-
`Seconds`	Zeit in Sekunden	1 ... 1500
`retries`	Schlüsselwort für die maximale Anzahl der Versuche, eine Antwort auf eine Inform Request Message zu erhalten	-
`RetryCount`	Anzahl der Versuche	1 ... 3
`taglist`	Schlüsselwort für Tagliste	-
`TagIdentifier`	Tag-Identifier, der die Zieladresse für das SNMP wählt	Geben Sie den Tag-Identifier an.
`none`	Kein Tag-Identifier	-
Storage Type	Gibt an, ob die Einstellungen nach einem Neustart bestehen bleiben.	• `volatile` (flüchtig): Bei einem Neustart werden die Standardeinstellungen verwendet. • `nonvolatile` (nicht flüchtig): Bei einem Neustart werden die gespeicherten Einstellungen verwendet.

Parameter	Beschreibung	Wertebereich
`port`	Schlüsselwort für die Portnummer, auf der der SNMP Manager Traps und Inform Messages empfängt	-
`integer`	Portnummer	1 ... 65535

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Wenn beim Konfigurieren optionale Parameter nicht angegeben werden, gelten folgende Voreinstellungen:

Parameter	voreingestellter Wert
`taglist`	snmp
Storage Type	`volatile`
`port`	162

Ergebnis

Die SNMP-Zieladresse ist konfiguriert.

Weitere Hinweise

Sie löschen die SNMP-Zieladresse mit dem Befehl `no snmp targetaddr`.

Sie zeigen die SNMP-Zieladresse mit dem Befehl `show snmp targetaddr` an.

Sie konfigurieren die SNMP-Zielparameter mit dem Befehl `snmp targetparams`.

Sie zeigen die SNMP-Zielparameter mit dem Befehl `show snmp targetparam` an.

8.6.2.15 no snmp targetaddr

Beschreibung

Mit diesem Befehl löschen Sie die SNMP-Zieladresse.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no snmp targetaddr <TargetAddressName>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`TargetAddressName`	SNMP-Zieladresse	max. 32 Zeichen

Ergebnis

Die SNMP-Zieladresse ist gelöscht.

Weitere Hinweise

Sie ändern die SNMP-Zieladresse mit dem Befehl `snmp targetaddr`.

Sie zeigen die SNMP-Zieladresse mit dem Befehl `show snmp targetaddr` an.

8.6.2.16 snmp targetparams

Beschreibung

Mit diesem Befehl konfigurieren Sie die SNMP-Zielparameter.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
snmp targetparams <ParamName>
   user <UserName>
   security-model {v1|v2c|v3 {auth|noauth|priv}}
   message-processing {v1|v2c|v3}[{volatile|nonvolatile}]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ParamName`	Name des SNMP-Parameters	max. 32 Zeichen
`user`	Schlüsselwort für den Usernamen	-
`UserName`	Wert für den Usernamen	max. 32 Zeichen

Parameter	Beschreibung	Wertebereich/Anmerkung
security-model	Gibt an, welche SNMP-Version verwendet wird. Bei SNMPv3 ist zusätzlich eine Sicherheitsstufe (Authentifizierung, Verschlüsselung) konfigurierbar.	• SNMP-Version – v1 – v2c – v3 • Sicherheitsstufe für v3 – auth Authentifizierung aktiviert / keine Verschlüsselung aktiviert – noauth Keine Authentifizierung aktiviert / keine Verschlüsselung aktiviert – priv Authentifizierung aktiviert / Verschlüsselung aktiviert
message-processing	Gibt an, welche SNMP-Version für die Bearbeitung der Meldungen verwendet wird und ob die Einstellungen nach einem Neustart bestehen bleiben.	• SNMP-Version – v1 – v2c – v3 • Einstellungen nach dem Neustart – volatile (flüchtig): Bei einem Neustart gehen die Einstellungen verloren. – nonvolatile (nicht flüchtig): Bei einem Neustart bleiben die Einstellungen erhalten.

Schlüsselworte müssen angegeben werden.

Wenn beim Konfigurieren optionale Parameter nicht angegeben werden, gelten die voreingestellten Werte.

Ergebnis

Die SNMP-Zielparameter sind konfiguriert.

Weitere Hinweise

Sie löschen die SNMP-Zielparameter mit dem Befehl `no snmp targetparams`.

Sie zeigen die Einstellungen dieser Funktion mit dem Befehl `show snmp targetparam` an.

Sie konfigurieren ein Anwenderprofil mit dem Befehl `snmp user`.

Sie zeigen die Liste der Anwender mit dem Befehl `show snmp user` an.

8.6.2.17 no snmp targetparams

Beschreibung

Mit diesem Befehl löschen Sie die SNMP-Zielparameter.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no snmp targetparams <ParamName>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ParamName`	Name des SNMP-Parameters	max. 32 Zeichen

Ergebnis

Die SNMP-Zielparameter sind gelöscht.

Weitere Hinweise

Sie ändern die SNMP-Zielparameter mit dem Befehl `snmp targetparams`.

Sie zeigen die Einstellungen dieser Funktion mit dem Befehl `show targetparam` an.

8.6.2.18 snmp v1-v2 readonly

Beschreibung

Mit diesem Befehl sperren Sie den Schreibzugriff für SNMPv1- und SNMPv2-PDUs.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
snmp v1-v2 readonly
```

Ergebnis

Der Schreibzugriff für SNMPv1- und SNMPv2-PDUs ist gesperrt.

Weitere Hinweise

Sie geben den Schreibzugriff für SNMPv1- und SNMPv2-PDUs mit dem Befehl `no snmp v1-v2 readonly` frei.

8.6.2.19 no snmp v1-v2 readonly

Beschreibung

Mit diesem Befehl geben Sie den Schreibzugriff für SNMPv1- und SNMPv2-PDUs frei.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no snmp v1-v2 readonly
```

Ergebnis

Der Schreibzugriff für SNMPv1- und SNMPv2-PDUs ist freigegeben.

Weitere Hinweise

Sie sperren den Schreibzugriff für SNMPv1- und SNMPv2-PDUs mit dem Befehl `snmp v1-v2 readonly`.

8.6.2.20 snmp user

Beschreibung

Mit diesem Befehl konfigurieren Sie die Details eines SNMP-Benutzers.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
snmp user <UserName> [auth {md5|sha} <passwd> [priv DES <passwd>]]
   [{volatile|nonvolatile}]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`UserName`	Name des Benutzers	max. 32 Zeichen
`auth`	Gibt an, dass eine Authentifizierung stattfindet und welcher Algorithmus verwendet wird.	• `md5` (Message Digest 5) • `sha` (Secure Hash Algorithm) Default: Keine Authentifizierung
`passwd`	Passwort für die Authentifizierung	max. 32 Zeichen
`priv DES`	Gibt an, dass eine Verschlüsselung stattfindet.	- Default: Keine Verschlüsselung
`passwd`	Wert für das Passwort der Verschlüsselung	max. 32 Zeichen
Storage Type	Gibt an, ob die Einstellungen nach einem Neustart bestehen bleiben.	• `volatile` (flüchtig): Bei einem Neustart werden die Standardeinstellungen verwendet. • `nonvolatile` (nicht flüchtig): Bei einem Neustart werden die gespeicherten Einstellungen verwendet.

Wenn beim Konfigurieren eines SNMP-Benutzers optionale Parameter nicht angegeben werden, gelten die voreingestellten Werte.

Ergebnis

Die Details eines SNMP-Benutzers sind konfiguriert.

Weitere Hinweise

Sie löschen die Einstellungen mit dem Befehl `no snmp user`.

Sie zeigen die konfigurierten Benutzer mit dem Befehl `show snmp user` an.

8.6.2.21 no snmp user

Beschreibung

Mit diesem Befehl löschen Sie die Details eines SNMP-Benutzers.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no snmp user <UserName>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`UserName`	Name des Benutzers	max. 32 Zeichen

Ergebnis

Die Details eines SNMP-Benutzers sind gelöscht.

Weitere Hinweise

Sie ändern die Einstellungen mit dem Befehl `snmp user`.

Sie zeigen die konfigurierten Benutzer mit dem Befehl `show snmp user` an.

8.6.2.22 snmp view

Beschreibung

Mit diesem Befehl konfigurieren Sie einen SNMP-View.

Voraussetzung

- Eine SNMP-Gruppe ist angelegt
- Der Zugang zur Gruppe ist mit `snmp access` konfiguriert
- Sie befinden sich im globalen Konfigurationsmodus.
  Die Eingabeaufforderung lautet:
  `cli(config)#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
snmp view <ViewName> <OIDTree> [mask<OIDMask>] {included|excluded}
   [{volatile|nonvolatile}]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ViewName`	Name des SNMP-Views	max. 32 Zeichen
`OIDTree`	Objekt-ID	Pfadangabe des MIB-Baums
`mask`	Schlüsselwort für die OID-Maske	-
`OIDMask`	Maske, die den Zugriff auf die Elemente des MIB-Baums filtert	Folge von "`0`" und "`1`", durch Punkte getrennt, entsprechend der Pfadangabe des MIB-Baums
View type	Gibt an, ob die gefilterten Elemente verwendet oder ausgeschlossen werden.	• `included` (Default) • `excluded`
Storage type	Gibt an, ob die Einstellungen nach einem Neustart bestehen bleiben.	• `volatile`(flüchtig): Bei einem Neustart gehen die Einstellungen verloren. • `nonvolatile`(nicht flüchtig): Bei einem Neustart bleiben die Einstellungen erhalten (Default).

Wenn beim Konfigurieren optionale Parameter nicht angegeben werden, gelten die voreingestellten Werte.

Ergebnis

Der SNMP-View ist konfiguriert.

Weitere Hinweise

Sie löschen den View mit dem Befehl `no snmp view`.

Sie zeigen die konfigurierten SNMP-Baumansichten mit dem Befehl `show snmp viewtree` an.

Sie zeigen die Zugriffsrechte der SNMP-Gruppen mit dem Befehl `show snmp group access` an.

Sie konfigurieren die Zugriffsrechte der SNMP-Gruppen mit dem Befehl `snmp access`.

8.6.2.23 no snmp view

Beschreibung

Mit diesem Befehl löschen Sie einen SNMP-View.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no snmp view <ViewName> <OIDTree>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ViewName`	Name des View	max. 32 Zeichen
`OIDTree`	Objekt-ID	Pfadangabe des MIB-Baums

Ergebnis

Der SNMP-View ist gelöscht.

Weitere Hinweise

Sie konfigurieren einen View mit dem Befehl `snmp view`.

Sie zeigen die konfigurierten SNMP-Baumansichten mit dem Befehl `show snmp viewtree` an.

8.7 HTTP-Server

In diesem Kapitel werden Befehle des Hypertext Transfer Protocol (HTTP) beschrieben.

8.7.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.7.1.1 show ip http server status

Beschreibung

Dieser Befehl zeigt den Status des HTTP-Servers an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show ip http server status
```

Ergebnis

Der Status des HTTP-Servers wird angezeigt.

8.7.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.7.2.1 ip http

Beschreibung

Mit diesem Befehl aktivieren Sie HTTP auf dem Gerät.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
ip http
```

Der Defaultwert der Funktion ist "aktiviert".

Ergebnis

HTTP ist auf dem Gerät aktiviert.

Weitere Hinweise

Sie zeigen die Einstellung dieser Funktion und weitere Informationen mit dem Befehl `show ip http server status` an.

Sie deaktivieren HTTP auf dem Gerät mit dem Befehl `no ip http`.

8.7.2.2 no ip http

Beschreibung

Mit diesem Befehl deaktivieren Sie den Zugriff über HTTP. Sie können nur noch über HTTPS auf das WBM des Geräts zugreifen.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no ip http
```

Ergebnis

Nur noch der Zugriff über HTTPS auf das WBM ist möglich.

Weitere Hinweise

Sie zeigen die Einstellung dieser Funktion und weitere Informationen mit dem Befehl `show ip http server status` an.

Sie aktivieren HTTP mit dem Befehl `ip http`.

8.8 HTTPS-Server

In diesem Kapitel werden Befehle des Hypertext Transfer Protocol Secure (HTTPS) beschrieben.

8.8.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.8.1.1 show ip http secure server status

Beschreibung

Dieser Befehl zeigt den Status des HTTPS-Servers an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show ip http secure server status
```

Ergebnis

Der Status, die Cipher Suite und die Version des HTTPS-Servers werden angezeigt.

8.8.1.2 show ssl server-cert

Beschreibung

Dieser Befehl zeigt das SSL-Server-Zertifikat an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show ssl server-cert
```

Ergebnis

Das SSL-Server-Zertifikat wird angezeigt.

8.8.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.8.2.1 ip http secure minimum tls-version

Beschreibung

Mit diesem Befehl definieren Sie, welche Version von TLS mindestens verwendet wird.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ip http secure minimum tls-version {v10 | v11 | v12}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`v10`	TLS ab Version 1.0 kann verwendet werden	-
`v11`	TLS ab Version 1.1 kann verwendet werden	Werkseinstellung
`v12`	TLS ab Version 1.2 kann verwendet werden	-

Ergebnis

HTTP ist auf dem Gerät aktiviert.

Weitere Hinweise

Sie zeigen die Einstellung dieser Funktion und weitere Informationen mit dem Befehl `show ip http secure server status` an.

8.8.2.2 ip http https redirection

Beschreibung

Mit diesem Befehl aktivieren Sie die Umleitung von HTTP auf HTTPS.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
ip http https redirection
```

Der Defaultwert der Funktion ist "aktiviert".

Ergebnis

Die Umleitung ist auf dem Gerät aktiviert.

Weitere Hinweise

Sie zeigen die Einstellung dieser Funktion und weitere Informationen mit dem Befehl `show ip http server status` an.

8.9 Proxy-Server

In diesem Kapitel werden Befehle zum Proxy-Server beschrieben.

8.9.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.9.1.1 show proxyserver table

Beschreibung

Dieser Befehl zeigt die Konfiguration des Proxy-Servers an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show proxyserver table
```

Ergebnis

Die Konfiguration wird angezeigt.

8.9.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.9.2.1 proxyserver

Beschreibung

Mit diesem Befehl wechseln Sie in den PROXYSERVER-Konfigurationsmodus.

Voraussetzung

Sie befinden sich jetzt im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
proxyserver
```

Ergebnis

Sie befinden sich jetzt im PROXYSERVER-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-proxysrv)#
```

Weitere Hinweise

Sie verlassen den PROXYSERVER-Konfigurationsmodus mit dem Befehl `end` oder `exit`.

8.9.3 Befehle im PROXYSERVER-Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im PROXYSERVER-Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl proxyserver ein, um in diesen Modus zu wechseln.

- Wenn Sie den PROXYSERVER-Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den PROXYSERVER-Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

8.9.3.1 srv name

Beschreibung

Mit diesem Befehl erstellen Sie einen Proxy-Servereintrag. Sie vergeben einen Namen und konfigurieren die Parameter.

Voraussetzung

Sie befinden sich im PROXYSERVER-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-proxysrv)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
srv name <name(128)> type {http|socks} port <num(0-65535)> auth {basic|ntlm|none}
[addr <ip_addr|dns(255)>] [user <string(255)>] [pw <string(255)>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`name`	Proxy-Servername	Geben Sie einen eindeutigen Namen für den Proxy-Server an. Maximal 128 Zeichen
`type`	Schlüsselwort für die Art des Proxy-Servers	-
`http`	Proxy-Server nur für Zugriffe über HTTP	-
`socks`	Universeller Proxy-Server	-
`port`	Schlüsselwort für Port	-
`num`	Portnummer	0 ... 65535 Geben Sie den Port an, auf dem der Proxydienst läuft.
`auth`	Schlüsselwort für Authentifizierungsmethode	-
`basic`	Standardauthentifizierung. Benutzernamen und Passwort werden unverschlüsselt gesendet	-

Parameter	Beschreibung	Wertebereich / Anmerkung
`ntlm`	Authentifizierung nach NTML Standard (Windows-Benutzeranmeldung)	-
`none`	Ohne Authentifizierung	-
`addr`	Schlüsselwort für IPv4-Adresse	-
`ip_addr`	IPv4-Adresse	Geben Sie die IPv4-Adresse des Proxy-Servers an.
`dns`	DNS-Hostnamen	Geben Sie den DNS-Hostnamen des Proxy-Servers an.
`user`	Schlüsselwort für Benutzernamen	-
`string`	Name	Geben Sie den Benutzernamen für den Zugang zum Proxy-Server an. Maximal 255 Zeichen
`pw`	Schlüsselwort für Passwort	-
`string`	Passwort	Geben Sie das Passwort für den Zugang zum Proxy-Server an. Maximal 255 Zeichen

Ergebnis

Der Proxy-Server ist konfiguriert.

Weitere Hinweise

Sie löschen diesen Proxy-Server mit dem Befehl `no srv`.

Die Parameter ändern Sie mit den Befehlen `srv name...`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show proxyserver table` an.

8.9.3.2 no srv

Beschreibung

Mit diesem Befehl löschen Sie einen bestimmten Proxy-Server oder alle Proxy-Server.

Voraussetzung

- Der entsprechende Proxy-Servername ist angelegt und wird nirgendwo verwendet.
- Sie befinden sich im PROXYSERVER-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-proxysrv)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no srv {name <string(128)> | all}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`name`	Schlüsselwort für Proxy-Servername	-
`string`	Proxy-Servername	Geben Sie einen gültigen Proxy-Servernamen an. Maximal 128 Zeichen
`all`	Löscht alle Proxy-Server	-

Ergebnis

Der angegebene Proxy-Server ist gelöscht.

Weitere Hinweise

Sie legen den Proxy-Server mit dem Befehl `srv name` an.

Sie zeigen die verfügbaren Proxy-Servernamen mit dem Befehl `srv show-names` an.

8.9.3.3 srv name addr

Beschreibung

Mit diesem Befehl ändern Sie die Adresse des Proxy-Servers.

Voraussetzung

- Der Proxy-Servername ist angelegt.
- Sie befinden sich im PROXYSERVER-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-proxysrv)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
srv name <string(128)> addr <ip_addr|dns(50)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`string`	Proxy-Servername	Geben Sie den Proxy-Servernamen an. Maximal 128 Zeichen
`ip_addr`	IPv4-Adresse	Geben Sie die IPv4-Adresse des Proxy-Servers an.
`dns`	DNS-Hostname	Geben Sie den DNS-Hostnamen des Proxy-Servers an. Maximal 50 Zeichen

Ergebnis

Die IPv4-Adresse des Proxy-Servers ist geändert.

Weitere Hinweise

Sie zeigen die verfügbaren Proxy-Servernamen mit dem Befehl `srv show-names` an.

Sie legen den Proxy-Server mit dem Befehl `srv name` an.

8.9.3.4 srv name auth

Beschreibung

Mit diesem Befehl ändern Sie die Authentifizierungsmethode des Proxy-Servers..

Voraussetzung

- Der Proxy-Servername ist angelegt.
- Sie befinden sich im PROXYSERVER-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-proxysrv)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
srv name <string(128)> auth <none|basic|ntlm>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`string`	Proxy-Servername	Geben Sie den Proxy-Servernamen an. Maximal 128 Zeichen
`none`	Ohne Authentifizierung	-

Parameter	Beschreibung	Wertebereich / Anmerkung
`basic`	Standardauthentifizierung Der Benutzername und das Passwort werden unverschlüsselt gesendet.	-
`ntlm`	Authentifizierung nach NTML Standard (Windows-Benutzeranmeldung)	-

Ergebnis

Die Authentifizierungsmethode ist geändert.

Weitere Hinweise

Sie zeigen die verfügbaren Proxy-Servernamen mit dem Befehl `srv show-names` an.

Sie legen den Proxy-Server mit dem Befehl `srv name` an.

8.9.3.5 srv name port

Beschreibung

Mit diesem Befehl ändern Sie den Port des Proxy-Servers.

Voraussetzung

- Der Proxy-Servername ist angelegt.
- Sie befinden sich im PROXYSERVER-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-proxysrv)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
srv name <string(128)> port <number(0-65535)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`string`	Proxy-Servername	Geben Sie den Proxy-Servernamen an. Maximal 128 Zeichen
Port	Portnummer	Geben Sie die Portnummer an, auf dem der Proxydienst läuft. 0 - 65535

Ergebnis

Der Port ist geändert.

Weitere Hinweise

Sie zeigen die verfügbaren Proxy-Servernamen mit dem Befehl `srv show-names` an.

Sie legen den Proxy-Server mit dem Befehl `srv name` an.

8.9.3.6 srv name pw

Beschreibung

Mit diesem Befehl ändern Sie das Passwort für den Zugang zum Proxy-Server.

Voraussetzung

- Bei der Auswahl der Authentifizierungsmethode wird `basic` verwendet.
- Der Proxy-Servername ist angelegt.
- Sie befinden sich im PROXYSERVER-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-proxysrv)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
srv set name <string(255)> pw <name(255)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`string`	Proxy-Servername	Geben Sie den Proxy-Servernamen an. Maximal 128 Zeichen
`pw`	Passwort	Geben Sie das geänderte Passwort für den Zugang zum Proxy-Server an. Maximal 255 Zeichen

Ergebnis

Das Passwort ist geändert.

Weitere Hinweise

Sie zeigen die verfügbaren Proxy-Servernamen mit dem Befehl `srv show-names` an.

Sie legen den Proxy-Server mit dem Befehl `srv name` an.

8.9.3.7 srv name type

Beschreibung

Mit diesem Befehl ändern Sie die Art des Proxy-Servers.

Voraussetzung

- Der Proxy-Servername ist angelegt.
- Sie befinden sich im PROXYSERVER-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-proxysrv)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
srv name <string(128)> type <http|socks>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`string`	Proxy-Servername	Geben Sie den Proxy-Servernamen an. Maximal 128 Zeichen
`http`	Universeller Proxy-Server	-
`socks`	Schlüsselwort für Port	-

Ergebnis

Die Art des Proxy-Servers ist geändert.

Weitere Hinweise

Sie zeigen die verfügbaren Proxy-Servernamen mit dem Befehl `srv show-names` an.

Sie legen den Proxy-Server mit dem Befehl `srv name` an.

8.9.3.8 srv name user

Beschreibung

Mit diesem Befehl ändern Sie den Benutzernamen für den Zugang zum Proxy-Server.

Voraussetzung

- Bei der Auswahl der Authentifizierungsmethode wird `basic` verwendet.
- Der Proxy-Servername ist angelegt.
- Sie befinden sich im PROXYSERVER-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-proxysrv)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
srv name <string(128)> user <name(255)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`string`	Proxy-Servername	Geben Sie den Proxy-Servernamen an. Maximal 128 Zeichen
`name`	Benutzername	Geben Sie den Benutzernamen für den Zugang zum Proxy-Server an. Maximal 255 Zeichen.

Ergebnis

Der Benutzername ist geändert.

Weitere Hinweise

Sie zeigen die verfügbaren Proxy-Servernamen mit dem Befehl `srv show-names` an.

Sie legen den Proxy-Server mit dem Befehl `srv name` an.

8.9.3.9 srv show-names

Beschreibung

Mit diesem Befehl zeigen Sie die verfügbaren Proxy-Servernamen an.

Voraussetzung

Sie befinden sich im PROXYSERVER-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-proxysrv)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
srv show-names
```

Ergebnis

Die Proxy-Servernamen werden aufgelistet.

Weitere Hinweise

Sie legen einen Proxyserver mit dem Befehl `srv name` an.

8.10 SMTP-Client

In diesem Kapitel werden Befehle des Simple Mail Transfer Protocol (SMTP) beschrieben.

8.10.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.10.1.1 show events smtp-server

Beschreibung

Dieser Befehl zeigt die konfigurierten SMTP Server an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show events smtp-server
```

Ergebnis

Die konfigurierten SMTP Server werden angezeigt.

8.10.1.2 show events sender email

Beschreibung

Dieser Befehl zeigt die konfigurierte Email-Absenderadresse an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show events sender email
```

Ergebnis

Die konfigurierte Email-Absenderadresse wird angezeigt.

8.10.1.3 show events smtp-port

Beschreibung

Dieser Befehl zeigt den konfigurierten SMTP-Port an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show events smtp-port
```

Ergebnis

Der konfigurierte SMTP-Port wird angezeigt.

8.10.2 Befehle im Events Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im EVENTS Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl `events` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

- Wenn Sie den EVENTS Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den EVENTS Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im EVENTS Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.10.2.1 send test mail

Beschreibung

Mit diesem Befehl senden Sie eine E-Mail entsprechend den aktuell konfigurierten SMTP-Einstellungen.

Voraussetzung

Sie befinden sich im EVENTS Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-events)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
send test mail
```

Ergebnis

Eine E-Mail entsprechend den aktuell konfigurierten SMTP-Einstellungen wurde gesendet.

Weitere Hinweise

Die Anzeige der aktuellen SMTP-Einstellungen rufen Sie mit dem Befehl `show events emailserver` auf.

8.10.2.2 smtp-server

Beschreibung

Mit diesem Befehl wechseln Sie in den SMTP-Server Konfigurationsmodus. Dabei gibt es zwei Möglichkeiten:

- Neunanlage

  Wenn es noch keinen Eintrag mit dieser Adresse gibt, wird ein neuner SMTP-Servereintrag erstellt und in den SMTP-Server Konfigurationsmodus gewechselt. Dort konfigurieren Sie die weiteren Einstellungen des SMTP-Servers.

- Konfiguraton ändern

  Wenn es den Eintrag bereits gibt, wird in den SMTP-Server Konfigurationsmodus gewechselt. Dort können Sie die Einstellungen des SMTP-Servers ändern.

Voraussetzung

Sie befinden sich im EVENTS Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-events)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
smtp-server { ipv4 <ucast_addr> | fqdn-name <FQDN>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ipv4`	Schlüsselwort für eine IPv4-Adresse	-
`ucast_addr`	IPv4-Adresse des SMTP-Servers	Geben Sie eine gültige IPv4-Unicast-Adresse an.
`fqdn-name`	Schlüsselwort für einen Domainnamen	-
`FQDN`	Domainname (Fully Qualified Domain Name)	Maximal 100 Zeichen

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Adressen und Schnittstellenbezeichnungen (Seite 42)".

Ergebnis

Ein Eintrag für den SMTP-Server ist erstellt.

Sie befinden sich jetzt im SMTP-Server Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(events-smtp-server)#
```

Weitere Hinweise

Sie löschen den SMTP-Servereintrag mit dem Befehl `no smtp-server`.

Sie zeigen die Konfigurtion des SMTP-Servers mit dem Befehl `show events smtp-server`.

8.10.2.3 no smtp-server

Beschreibung

Mit diesem Befehl löschen Sie einen SMTP-Servereintrag.

Voraussetzung

Sie befinden sich im EVENTS Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-events)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no smtp-server { ipv4 <ucast_addr> | fqdn-name <FQDN)>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ipv4`	Schlüsselwort für eine IPv4-Adresse	-
`ucast_addr`	IPv4-Adresse des SMTP-Servers	Geben Sie eine gültige IPv4-Unicast-Adresse an.
`fqdn-name`	Schlüsselwort für einen Domainnamen	-
`FQDN`	Domainname (Fully Qualified Domain Name)	Maximal 100 Zeichen

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Adressen und Schnittstellenbezeichnungen (Seite 42)".

Ergebnis

Der SMTP-Servereintrag ist gelöscht.

Weitere Hinweise

Sie konfigurieren einen SMTP-Servereintrag mit dem Befehl `smtp-server`.

8.10.3 Befehle im STMP-Server Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im SMTP-Server Konfigurationsmodus aufrufen können.

Geben Sie im Events-Konfigurationsmodus den Befehl `smtp-server` ein, um in diesen Modus zu wechseln.

- Wenn Sie den SMTP-Server Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im Events- Konfigurationsmodus.
- Wenn Sie den SMTP-Server Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

8.10.3.1 auth username

Beschreibung

Mit diesem Befehl konfigurieren Sie die Benutzerdaten (Benutzernamen und Passwort), die zur Authentifizierung am SMTP-Server verwendet werden.

Voraussetzung

Sie befinden sich im SMTP-Server Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(events-smtp-server)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
auth username <username> password <password>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`username`	Schlüsselwort für Benutzername	-
`username`	Benutzername	Geben Sie den Benutzernamen ein, der zur Authentifizierung am SMTP-Server verwendet wird.
`password`	Schlüsselwort für ein Passwort	-
`password`	Passwort	Geben Sie das Passwort ein, das zur Authentifizierung am SMTP-Server verwendet wird.

Ergebnis

Die Benutzerdaten sind konfiguriert.

Weitere Hinweise

Sie löschen die Benutzerdaten mit dem Befehl `no auth username`.

Sie zeigen diese Einstellung mit dem Befehl `show events smtp-server` an.

8.10.3.2 no auth username

Beschreibung

Mit diesem Befehl löschen Sie die Benutzerdaten.

Voraussetzung

Sie befinden sich im SMTP-Server Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(events-smtp-server)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no auth username
```

Ergebnis

Der SMTP-Port ist auf den voreingestellten Wert zurückgesetzt.

Weitere Hinweise

Sie konfigurieren die Benutzerdaten mit dem Befehl `auth username`.

Sie zeigen diese Einstellung mit dem Befehl `show events smtp-server` an.

8.10.3.3 port

Beschreibung

Mit diesem Befehl konfigurieren Sie den Port, über den der SMTP-Server erreichbar ist.

Voraussetzung

Sie befinden sich im SMTP-Server Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(events-smtp-server)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
port <smtp-port(1-65535)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
smtp-port	Wert für den SMTP-Port	1 ... 65535 Default: 25

Ergebnis

Der SMTP-Port ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung mit dem Befehl `show events smtp-server` an.

Sie setzen die Einstellung mit dem Befehl `no port` auf den voreingestellten Wert zurück.

8.10.3.4 no port

Beschreibung

Mit diesem Befehl setzen Sie den SMTP-Port auf den voreingestellten Wert zurück.
Der voreingestellte Wert ist 25.

Voraussetzung

Sie befinden sich im SMTP-Server Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(events-smtp-server)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no port
```

Ergebnis

Der SMTP-Port ist auf den voreingestellten Wert zurückgesetzt.

Weitere Hinweise

Sie konfigurieren die Einstellung mit dem Befehl `port`.

Sie zeigen diese Einstellung mit dem Befehl `show events smtp-server` an.

8.10.3.5 receiver-address

Beschreibung

Mit diesem Befehl legen Sie fest, wer beim Auftreten eines Ereignisses eine E-Mail bekommt.

Voraussetzung

- Beim entsprechenden Ereignis ist "email" aktiviert.
- Sie befinden sich im SMTP-Server Konfigurationsmodus

  Die Eingabeaufforderung lautet:

  ```
  cli(events-smtp-server)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
receiver-address <mail-address> [shutdown]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`mail-address`	E-Mail-Adresse des Empfängers	max. 100 Zeichen
`shutdown`	Deaktiviert das Senden der E-Mail. Beim Auftreten eines Ereignisses erhält dieser Empfänger keine E-Mail.	-

Ergebnis

Ein Empfänger ist konfiguriert.

Weitere Hinweise

Sie löschen den Empfänger mit dem Befehl `no receiver-address`.

Sie zeigen diese Einstellung mit dem Befehl `show events smtp-server` an.

Sie konfigurieren die Einstellung "`email`" mit dem Befehl `event config`.

8.10.3.6 no receiver-address

Beschreibung

Mit diesem Befehl löschen Sie einen Empfänger.

Voraussetzung

Sie befinden sich im SMTP-Server Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(events-smtp-server)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no receiver-address <mail-address>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`mail-address`	E-Mail-Adresse des Empfängers	max. 100 Zeichen

Ergebnis

Der Empfänger ist gelöscht.

Weitere Hinweise

Sie erstellen einen Empfänger mit dem Befehl `receiver-address`

Sie zeigen diese Einstellung mit dem Befehl `show events smtp-server` an.

8.10.3.7 security

Beschreibung

Mit diesem Befehl konfigurieren Sie das Verfahren für die verschlüsselte Übertragung der E-Mail vom Gerät zum SMTP-Server.

Voraussetzung

Sie befinden sich im SMTP-Server Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(events-smtp-server)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
security {ssltls | starttls}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ssltls`	Verwendet SSL/TLS	-
`starttls`	Verwendet STARTTLS	-

Ergebnis

Das Verfahren für die Übertragung ist konfiguriert.

Weitere Hinweise

Sie deaktivieren die Einstellung mit dem Befehl `no security`.

Sie zeigen diese Einstellung mit dem Befehl `show events smtp-server` an.

8.10.3.8 no security

Beschreibung

Mit diesem Befehl legen Sie fest, dass die E-Mail unverschlüsselt übertragen wird.

Voraussetzung

Sie befinden sich im SMTP-Server Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(events-smtp-server)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no security
```

Ergebnis

Die Übertragung der E-Mail vom Gerät zum SMTP-Server ist unverschlüsselt.

Weitere Hinweise

Sie konfigurieren die Einstellung mit dem Befehl `security`.

Sie zeigen diese Einstellung mit dem Befehl `show events smtp-server` an.

8.10.3.9 sender address

Beschreibung

Mit diesem Befehl konfigurieren Sie den Absender, der in der E-Mail angegeben wird.

Voraussetzung

Sie befinden sich im SMTP-Server Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(events-smtp-server)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
sender-address <mail-address>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`mail-address`	E-Mail-Adresse des Absenders	max. 100 Zeichen

Ergebnis

Der E-Mail-Adresse des Absenders ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung mit dem Befehl `show events smtp-server` an.

Sie löschen den Absender mit dem Befehl `no sender-address`.

8.10.3.10 no sender address

Beschreibung

Mit diesem Befehl löschen Sie den Absender.

Voraussetzung

Sie befinden sich im SMTP-Server Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(events-smtp-server)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no sender-address
```

Ergebnis

Der E-Mail-Name des Absenders ist gelöscht.

Weitere Hinweise

Sie konfigurieren einen Absender mit dem Befehl `sender-address`.

Sie zeigen diese Einstellung mit dem Befehl `show events smtp-server` an.

8.10.3.11 test

Beschreibung

Mit diesem Befehl senden Sie eine Test-E-Mail an die konfigurierten Empfänger.

Voraussetzung

Sie befinden sich im SMTP-Server Konfigurationsmodus

Die Eingabeaufforderung lautet:

```
cli(events-smtp-server)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
test
```

Ergebnis

An die konfigurierten Empfänger wurde eine Test-E-Mail gesendet. Das Testergebnis wird in der Ausgabe der Konsole angezeigt. Wenn das Senden nicht erfolgreich war, enthält die Meldung mögliche Ursachen.

8.11 SSH-Server

In diesem Kapitel werden Befehle des Secure Shell (SSH) Server beschrieben.

8.11.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.11.1.1 show ip ssh

Beschreibung

Dieser Befehl zeigt die Einstellungen des SSH-Servers an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show ip ssh
```

Ergebnis

Die Einstellungen des SSH-Servers werden angezeigt.

8.11.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

8.11.2.1 ssh-server

Beschreibung

Mit diesem Befehl aktivieren Sie das SSH-Protokoll auf dem Gerät.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
ssh-server
```

Der Defaultwert der Funktion ist "aktiviert".

Ergebnis

Das SSH-Protokoll ist auf dem Gerät aktiviert.

Weitere Hinweise

Sie deaktivieren das SSH-Protokoll mit dem Befehl `no ssh-server`.

8.11.2.2 no ssh-server

Beschreibung

Mit diesem Befehl deaktivieren Sie das SSH-Protokoll auf dem Gerät.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no ssh-server
```

Ergebnis

Das SSH-Protokoll ist auf dem Gerät deaktiviert.

Weitere Hinweise

Sie aktivieren das SSH-Protokoll mit dem Befehl `ssh-server`.

Lastkontrolle 9

In diesem Abschnitt finden Sie die Kapitel, die Funktionen zur Kontrolle und Verteilung der Netzlast beschreiben.

9.1 Flow Control

Die Flow-Control-Funktion überwacht den eingehenden Datenverkehr eines Ports. Bei Überlastung ("Congestion", "Overflow") sendet sie ein Signal an den Verbindungspartner. Wenn die Flow-Control-Funktion auf der Senderseite dieses Signal erhält, stoppt sie die Datenübertragung, um einen Datenverlust zu vermeiden.

In diesem Kapitel werden Befehle der Flow-Control-Funktion beschrieben.

9.1.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

9.1.1.1 show flow-control

Beschreibung

Dieser Befehl zeigt die Einstellungen der Flow-Control-Funktion an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show flow-control [interface <interface-type><interface-id>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`interface`	Schlüsselwort für eine Schnittstellenbeschreibung	-
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstelle	

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Wenn Sie keinen Parameter aus der Parameterliste auswählen, wird die Information für den Router angezeigt.

Ergebnis

Die Einstellungen der Flow-Control-Funktion werden dargestellt.

9.1.2 Befehle im Interface Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im Interface Konfigurationsmodus aufrufen können. Abhängig von der eingestellten Schnittstelle sind verschiedene Befehlssätze verfügbar.

Geben Sie im globalen Konfigurationsmodus den Befehl `interface` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im Interface Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

- Wenn Sie den Interface Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den Interface Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im Interface Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

9.1.2.1 flowcontrol

Beschreibung

Die Flow-Control-Funktion (Flusskontrolle) überwacht auf der empfangenden Seite einer Verbindung, dass nicht mehr Daten empfangen werden als verarbeitet werden können. Stellt Flow-Control einen drohenden Datenüberlauf fest, wird dem Partner auf der sendenden Seite signalisiert, die Sendung zu stoppen.

Mit diesem Befehl konfigurieren Sie die Flow-Control-Funktion für eine Schnittstelle.

Voraussetzung

Sie befinden sich im Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-if-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
flowcontrol {on|off}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`on`	aktiviert die Funktion	Sie können die Flusskontrolle nur aktivieren oder deaktivieren, wenn die Funktion "Auto Negotiation" ausgeschaltet ist. Sie können "Auto Negotiation" danach wieder aktivieren.
`off`	deaktiviert die Funktion	-

Ergebnis

Die Einstellungen für die Flow-Control-Funktion sind konfiguriert.

Weitere Hinweise

Sie zeigen den Status dieser Funktion mit dem Befehl `show flow-control` an.

Sie deaktivieren "Auto Negotiation" mit dem Befehl `no negotiation`.

Sie aktivieren "Auto Negotiation" mit dem Befehl `negotiation`.

9.2 Dynamic MAC Aging

In diesem Kapitel werden Befehle beschrieben, mit denen die Lebensdauer von dynamisch gelernten Einträgen in einer MAC-Adressliste konfiguriert wird.

9.2.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

9.2.1.1 show mac-address-table aging-time

Beschreibung

Um die Aktualität der Adresseinträge sicher zu stellen, werden MAC-Adressen nur für eine festgelegte Zeitspanne in der Adresstabelle gehalten.

Dieser Befehl zeigt die Zeitspanne an, nach der die MAC-Adressen aus der Adresstabelle entfernt werden.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show mac-address-table aging-time
```

Ergebnis

Die Zeitspanne wird angezeigt.

9.2.1.2 show mac-address-table aging-status

Beschreibung

Dieser Befehl zeigt an, ob MAC Aging aktiviert ist oder nicht.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show mac-address-table aging-status
```

Ergebnis

Der Status des MAC Aging wird angezeigt.

9.2.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

9.2.2.1 mac-address-table aging

Beschreibung

Mit diesem Befehl aktivieren Sie die Funktion "Aging". Die Funktion "Aging" sorgt dafür, dass ein dynamisch gelernter Eintrag in der MAC-Adressliste nach einer bestimmten Zeitspanne wieder gelöscht wird.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
mac-address-table aging
```

Ergebnis

Die Funktion "Aging" ist aktiviert.

Weitere Hinweise

Sie konfigurieren mit dem Befehl `mac-address-table aging-time` die Zeitspanne.

Sie deaktivieren die Funktion "Aging" mit dem Befehl `no mac-address-table aging`.

9.2.2.2 no mac-address-table aging

Beschreibung

Mit diesem Befehl deaktivieren Sie die Funktion "Aging".

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no mac-address-table aging
```

Ergebnis

Die Funktion "Aging" ist deaktiviert.

Weitere Hinweise

Sie aktivieren die Funktion "Aging" mit dem Befehl `mac-address-table aging`.

9.2.2.3 mac-address-table aging-time

Beschreibung

Mit diesem Befehl konfigurieren Sie die Lebensdauer eines dynamisch gelernten Eintrags in der MAC-Adressliste.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
mac-address-table aging-time <seconds(15-630)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`seconds`	Lebensdauer des Eintrags in Sekunden	15 ... 630 Default: 300 Geben Sie die Zeitspanne in Sekunden in 15er-Schritten ein. Beachten Sie bei der Eingabe der Aging Time, dass auf korrekte Werte gerundet wird. Wenn Sie einen Wert eingeben, der nicht durch 15 teilbar ist, wird der Wert automatisch abgerundet.

Ergebnis

Der Wert für die Lebensdauer eines dynamisch gelernten Eintrags ist konfiguriert.

Weitere Hinweise

Sie setzen die Einstellung mit dem Befehl `no mac-address-table aging-time` auf den voreingestellten Wert zurück.

Sie zeigen die Einstellung mit dem Befehl `show mac-address-table aging-time` an.

Layer 3-Funktionen 10

10.1 VRRPv3 (IPv4)

In diesem Kapitel werden Befehle beschrieben, die für das Arbeiten mit Routing über VRRPv3 relevant sind. Die Version 3 von VRRP basiert auf der Version 2.

Hinweis

- Aktivieren Sie Routing, um VRRPv3 zu nutzen.
- Die Befehle sind nur in Verbindung mit VLAN-Schnittstellen verwendbar.

VRRP und DHCP-Server

VRRP und DHCP-ServerWenn Sie auf den Geräten einer VRRP-Gruppe einen DHCP-Server betreiben wollen, muss der DHCP-Server auf dem Master-Router konfiguriert sein. Backup-Router reagieren nicht auf DHCP-Anfragen. Stellen Sie sicher, dass der Master-Router statisch konfiguriert ist und nach einem Ausfall wieder zum Master der VRRP-Gruppe wird.

10.1.1 clear vrrp3 statistics

Beschreibung

Mit diesem Befehl setzen Sie die Zähler auf Null zurück.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
clear vrrp3 statistics
```

Ergebnis

Die Zähler sind zurückgesetzt.

Weitere Hinweise

Sie zeigen die Tabelle mit den Befehlen `show vrrp3 interface` und `show vrrp3 interface -vrid` an.

10.1.2 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

10.1.2.1 show vrrp3

Beschreibung

Dieser Befehl zeigt die Einstellungen eines virtuellen Routers an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show vrrp3 [interface vlan <vlan-id(1-4094)> <VrId(1-255)>]
[{brief|detail|statistics}]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vlan`	Schlüsselwort für eine VLAN-Verbindung	-
`vlan-id`	Nummer des angesprochenen VLANs	1 ... 4094
`VrId`	ID des virtuellen Routers	1 ... 255
`brief`	zeigt kurze Informationen zu VRRP an	-
`detail`	zeigt detaillierte Informationen zu VRRP an.	-
`statistics`	zeigt die Statistiken des VRRP-Protokolls	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Einstellungen des virtuellen Routers werden angezeigt.

10.1.2.2 show vrrp3 interface

Beschreibung

Dieser Befehl zeigt die Einstellungen von VRRP3 für die Schnittstelle an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show vrrp3 interface [vlan <vlan-id(1-4094)>] [{brief|detail|statistics}]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vlan`	Schlüsselwort für eine VLAN-Verbindung	-
`VlanId`	Nummer des angesprochenen VLANs	1 ... 4094
`brief`	zeigt kurze Informationen zu VRRP an	-
`detail`	zeigt detaillierte Informationen zu VRRP an.	-
`statistics`	zeigt die Statistiken des VRRP-Protokolls an	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Einstellungen für die Schnittstelle werden angezeigt.

10.1.2.3 show vrrp3 track

Beschreibung

Mit diesem Befehl zeigen Sie konfigurierte Schnittstellenüberwachungen an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show vrrp3 track
```

Ergebnis

Die konfigurierten Schnittstellenüberwachungen werden angezeigt.

10.1.3 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

10.1.3.1 router vrrp3

Beschreibung

Mit diesem Befehl aktivieren Sie das Routing über VRRPv3 und wechseln in den VRRP3 Router Konfigurationsmodus.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
router vrrp3
```

Ergebnis

Das Routing über VRRP3 ist aktiviert.

Sie befinden sich jetzt im VRRP3 Router Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli (config-vrrp-v3)#
```

Weitere Hinweise

Sie deaktivieren das Routing über VRRP mit dem Befehl `no router vrrp3`.

10.1.3.2 no router vrrp3

Beschreibung

Mit diesem Befehl deaktivieren Sie das Routing über VRRPv3.

Hinweis

Dieser Befehl ist nur bei Layer 3 verfügbar.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no router vrrp3
```

Ergebnis

Das Routing über VRRPv3 ist deaktiviert.

Weitere Hinweise

Sie aktivieren das Routing über VRRPv3 mit dem Befehl `router vrrp3`.

10.1.4 Befehle im VRRP3 Router Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im VRRP3 Router Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl `router vrrp3` ein, um in diesen Modus zu wechseln.

- Wenn Sie den VRRP3 Router Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den VRRP3 Router Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im VRRP3 Router Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

10.1.4.1 interface

Beschreibung

Mit diesem Befehl bestimmen Sie das Interface, das Sie im VRRP3 Router Konfigurationsmodus parametrieren wollen.

Dort bearbeiten Sie die Einstellungen für jeweils eine VRRP3-Schnittstelle. Sie wählen die VRRP3-Schnittstelle durch die Parametrierung dieses Befehls aus.

Voraussetzung

Sie befinden sich im VRRP3 Router Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli (config-vrrp-v3)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
interface vlan <vlan-id(1-4094)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vlan`	Schlüsselwort für eine VLAN-Verbindung	-
`vlan-id`	Nummer des angesprochenen VLAN	1 … 4094

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Sie befinden sich jetzt im VRRP3 Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-vrrp-v3-if-$$$)#
```

Weitere Hinweise

Sie verlassen den VRRP3 Interface Konfigurationsmodus mit dem Befehl `end` oder `exit`.

Sie löschen eine VRRP3-Schnittstelle mit dem Befehl `no interface`.

Sie zeigen den Status und die Konfiguration der VRRP3-Schnittstellen mit dem Befehl `show vrrp3` oder `show vrrp3 interface` an.

10.1.4.2 no interface

Beschreibung

Mit diesem Befehl löschen Sie eine VRRP3-Schnittstelle.

Voraussetzung

Sie befinden sich im VRRP3 Router Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli (config-vrrp-v3)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no interface vlan <vlan-id(1-4094)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vlan`	Schlüsselwort für eine VLAN-Verbindung	-
`vlan-id`	Nummer des angesprochenen VLAN	1 … 4094

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die VRRP3-Schnittstelle ist gelöscht.

Weitere Hinweise

Sie konfigurieren eine VRRP3-Schnittstelle mit dem Befehl `interface`.

Sie zeigen den Status und die Konfiguration der VRRP3-Schnittstelle mit dem Befehl `show vrrp3` oder `show vrrp3 interface` an.

10.1.4.3 track interface

Beschreibung

Mit diesem Befehl konfigurieren Sie die Überwachung von Schnittstellen.

Wenn sich der Link einer oder mehrerer überwachter Schnittstellen von "up" nach "down" ändert, wird die Priorität der zugeordneten VRRP-Schnittstelle verringert. Wenn sich der Link der Schnittstelle wieder von "down" nach "up" ändert, wird die unsprüngliche Priorität der VRRP-Schnittstelle wiederhergestellt.

Voraussetzung

Sie befinden sich im VRRP Router Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-vrrp-v3)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
track <group-index> interface { {vlan <vlan-id (1-4094)> | {ppp | usb} <intf-num(0-4)>} | <interface-type> <interface-id> }
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`group-index`	ID der Schnittstellenüberwachung	-
`vlan`	Schlüsselwort für eine VLAN-Verbindung	-
`vlan-id`	Nummer des angesprochenen VLAN	1 … 4094
`ppp`	WAN-Schnittstelle EGPRS, GPRS, UMTS	-
`usb`	WAN-Schnittstelle LTE	-
`intf-num`	Nummer der angesprochenen Schnittstelle	0 ... 4
`interface-type`	Typ der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstelle	

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die ausgewählte Schnittstelle wird überwacht.

Weitere Hinweise

Sie löschen eine Schnittstellenüberwachung mit dem Befehl `no interface interface`.

Sie zeigen die konfigurierten Schnittstellenüberwachungen mit dem Befehl `show vrrp track` an.

Sie ordnen einer Schnittstellenüberwachung eine VRRP-Schnittstelle mit dem Befehl `vrrp track decrement` zu.

Um welchen Wert die Priorität verringt wird, konfigurieren Sie mit dem Befehl `vrrp track decrement`.

Wie viele der überwachten Schnittstellen ihren Zustand ändern müssen, bevor die Priorität der zugeordneten VRRP-Schnittstelle geändert wird, konfigurieren Sie mit dem Befehl `track links`.

10.1.4.4 no track interface

Beschreibung

Mit diesem Befehl löschen Sie die Überwachung von Schnittstellen.

Voraussetzung

Sie befinden sich im VRRP Router Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-vrrp-v3)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no track <group-index> interface { {vlan <vlan-id (1-4094)> | {ppp | usb} <intf-
num(0-4)>} | <interface-type> <interface-id> }
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`group-index`	ID der Schnittstellenüberwachung	-
`vlan`	Schlüsselwort für eine VLAN-Verbindung	-
`vlan-id`	Nummer des angesprochenen VLAN	1 … 4094
`ppp`	WAN-Schnittstelle EGPRS, GPRS, UMTS	-
`usb`	WAN-Schnittstelle LTE	-

Parameter	Beschreibung	Wertebereich/Anmerkung
`intf-num`	Nummer der angesprochenen Schnittstelle	0 ... 4
`interface-type`	Typ der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`interface-id`	Modul-Nr. und Port-Nr. der Schnittstelle	

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Schnittstellenüberwachung ist gelöscht.

Weitere Hinweise

Sie konfigurieren eine Schnittstellenüberwachung mit dem Befehl `track interface`.

Sie zeigen die konfigurierten Schnittstellenüberwachungen mit dem Befehl `show vrrp track` an.

10.1.4.5 track links

Beschreibung

Mit diesem Befehl definieren Sie, wie viele der überwachten Schnittstellen in den Zustand "down" wechseln müssen, bevor die Priorität der zugeordneten VRRP-Schnittstelle geändert wird.

Voraussetzung

Sie befinden sich im VRRP Router Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-vrrp-v3)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
track <group-index> links <links-to-track(1-255)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`group-index`	ID der Schnittstellenüberwachung	-
`links-to-track`	Anzahl der Schnittstellen	1 ... 255

Ergebnis

Die Anzahl der überwachten Schnittstellen ist definiert.

Weitere Hinweise

Sie löschen die Konfiguration mit dem Befehl `no track links`.

Sie konfigurieren die Überwachung von Schnittstellen mit dem Befehl `track interface`.

Sie zeigen die konfigurierte Anzahl der überwachten Schnittstellen mit dem Befehl `show vrrp track`.

10.1.4.6 no track links

Beschreibung

Mit diesem Befehl löschen Sie die Anzahl der überwachten Schnittstellen.

Voraussetzung

Sie befinden sich im VRRP Router Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-vrrp-v3)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no track <group-index> links
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`group-index`	ID der Schnittstellenüberwachung	-

Ergebnis

Die Anzahl der überwachten Schnittstellen ist gelöscht.

Weitere Hinweise

Sie konfigurieren die Anzahl der überwachten Schnittstellen mit dem Befehl `track links`.

Sie zeigen die konfigurierte Anzahl der überwachten Schnittstellen mit dem Befehl `show vrrp track`.

10.1.4.7 vrrp vrid-track

Beschreibung

Mit diesem Befehl aktivieren Sie das VRID-Tracking.

Wenn aktiviert, werden alle VRRP-Instanzen überwacht. Wenn sich der Status einer VRRP-Instanz nach "Initialize" ändert, wird die Priorität aller VRRP-Instanzen auf den Wert "1" verringert.

Wenn sich der Status der VRRP-Instanz ändert, wird die ursprüngliche Priorität aller VRRP-Instanzen wiederhergestellt.

Voraussetzung

Sie befinden sich im VRRP Router Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-vrrp-v3)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
vrrp vrid-track
```

Ergebnis

VRID-Tracking ist aktiviert.

Weitere Hinweise

Sie deaktivieren VRID-Tracking mit dem Befehl `no vrrp vrid-track`.

Sie zeigen konfigurierte VRID-Trackings mit dem Befehl `show vrrp3` oder `show vrrp3 interface` mit dem Parameter `detail` an.

10.1.4.8 no vrrp vrid-track

Beschreibung

Mit diesem Befehl deaktivieren Sie das VRID-Tracking.

Voraussetzung

Sie befinden sich im VRRP Router Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-vrrp-v3)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no vrrp vrid-track
```

Ergebnis

VRID-Tracking ist deaktiviert.

Weitere Hinweise

Sie aktivieren VRID-Tracking mit dem Befehl `vrrp vrid-track`.

Sie zeigen konfigurierte VRID-Trackings mit dem Befehl `show vrrp3` oder `show vrrp3 interface` mit dem Parameter `detail` an.

10.1.5 Befehle im Interface Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die für das Arbeiten mit Routing über VRRPv3 relevant sind. Die Version 3 von VRRP basiert auf der Version 2.

Hinweis

- Aktivieren Sie Routing, um VRRPv3 zu nutzen.
- Die Befehle sind nur in Verbindung mit VLAN-Schnittstellen verwendbar.

VRRP und DHCP-Server

VRRP und DHCP-ServerWenn Sie auf den Geräten einer VRRP-Gruppe einen DHCP-Server betreiben wollen, muss der DHCP-Server auf dem Master-Router konfiguriert sein. Backup-Router reagieren nicht auf DHCP-Anfragen. Stellen Sie sicher, dass der Master-Router statisch konfiguriert ist und nach einem Ausfall wieder zum Master der VRRP-Gruppe wird.

10.1.5.1 vrrp associated-ip

Beschreibung

Mit diesem Befehl legen Sie fest, welche IP-Adressen der virtuelle Router überwacht.

Voraussetzung

Sie befinden sich im VRRP3 Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-vrrp-v3-if-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
vrrp <vrid(1-255)> associated-ip ipv4 <ip_addr>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vrid`	ID des virtuellen Routers	1 ... 255
`ipv4`	Schlüsselwort für IPv4-Adresse	-
`ip_addr`	IPv4-Adresse	Geben Sie eine gültige IPv4-Adresse an.

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die IP-Adressen sind festgelegt.

Weitere Hinweise

Sie konfigurieren eine VRRP3-Schnittstelle mit dem Befehl `interface`.

Sie entfernen eine IP-Adresse mit dem Befehl `no vrrp associated-ip`.

Sie zeigen die IP-Adressen mit dem Befehl `show vrrp3` an.

10.1.5.2 no vrrp associated-ip

Beschreibung

Mit diesem Befehl entfernen Sie eine IP-Adresse vom virtuellen Router.

Voraussetzung

Sie befinden sich im VRRP3 Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-vrrp-v3-if-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no vrrp <vrid(1-255)> associated-ip ipv4 <ip_addr>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vrid`	ID des virtuellen Routers	1 ... 255
`ipv4`	Schlüsselwort für IPv4-Adresse	-
`ip_addr`	IPv4-Adresse	Geben Sie eine gültige IPv4-Adresse an.

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die IP-Adresse ist vom virtuellen Router entfernt.

Weitere Hinweise

Sie konfigurieren eine VRRP3-Schnittstelle mit dem Befehl `interface`.

Sie zeigen die IP-Adressen mit dem Befehl `show vrrp` an.

10.1.5.3 vrrp primary-ip

Beschreibung

Mit diesem Befehl legen Sie die primäre IP-Adresse fest, die bei den VRRP3-Paketen als Quelladresse angegeben wird.

Voraussetzung

Sie befinden sich im VRRP3 Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-vrrp-v3-if-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
vrrp <vrid(1-255)> primary-ip ipv4 <ip_addr>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vrid`	ID des virtuellen Routers	1 ... 255
`ipv4`	Schlüsselwort für IPv4-Adresse	-
`ip_addr`	IPv4-Adresse	Geben Sie eine gültige IPv4-Adresse an.

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die primäre IP-Adresse ist festgelegt.

Weitere Hinweise

Sie konfigurieren eine VRRP3-Schnittstelle mit dem Befehl `interface`.

Sie entfernen die primäre IP-Adresse mit dem Befehl `no vrrp pirmary-ip`.

Sie zeigen die Konfiguration des virtuellen Routers mit dem Befehl `show vrrp3` an.

10.1.5.4 no vrrp primary-ip

Beschreibung

Mit diesem Befehl entfernen Sie eine primäre IP-Adresse vom virtuellen Router.

Voraussetzung

Sie befinden sich im VRRP3 Interface Konfigurationsmodus.
Die Eingabeaufforderung lautet:

```
cli(config-vrrp-v3-if-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no vrrp <vrid(1-255)> primary-ip ipv4 <ip_addr>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vrid`	ID des virtuellen Routers	1 ... 255
`ipv4`	Schlüsselwort für IPv4-Adresse	-
`ip_addr`	IPv4-Adresse	Geben Sie eine gültige IPv4-Adresse an.

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die primäre IP-Adresse ist vom virtuellen Router entfernt.

Weitere Hinweise

Sie konfigurieren eine VRRP3-Schnittstelle mit dem Befehl `interface`.

Sie ordnen eine primäreIP-Adresse einem virtuellen Router mit dem Befehl `vrrp primary-ip` zu.

Sie zeigen die IP-Adressen mit dem Befehl `show vrrp3` an.

10.1.5.5 vrrp priority

Beschreibung

Mit diesem Befehl legen Sie die Priorität des virtuellen Routers fest. Die 255 erhält automatisch der aktuelle Master-Router. Alle anderen Prioritäten können frei auf die VRRP-Router verteilt werden. Je größer eine Priorität ist, desto eher wird der VRRP-Router zum "Master".

Voraussetzung

- Dem virtuellen Router ist eine IP-Adresse zugeordnet.
- Sie befinden sich im VRRP3 Interface Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-vrrp-v3-if-$$$)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
vrrp <vrid(1-255)> priority <priority(1-254)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vrid`	ID des virtuellen Routers	1 ... 255
`priority`	Priorität des virtuellen Routers	1 ... 254 Default: 1

Ergebnis

Die Priorität des virtuellen Routers ist festgelegt.

Weitere Hinweise

Sie konfigurieren eine VRRP3-Schnittstelle mit dem Befehl `interface`.

Sie setzen die Priorität mit dem Befehl `no vrrp priority` auf den voreingestellten Wert zurück.

Sie ordnen IP-Adressen einem virtuellen Router mit dem Befehl `vrrp associated-ip` zu.

Sie zeigen die Priorität mit dem Befehl `show vrrp3` an.

10.1.5.6 no vrrp priority

Beschreibung

Mit diesem Befehl setzen Sie die Router-Priorität auf den voreingestellten Wert zurück.

Voraussetzung

- Dem virtuellen Router ist eine IP-Adresse zugeordnet.
- Sie befinden sich im VRRP3 Interface Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-vrrp-v3-if-$$$)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no vrrp <vrid(1-255)> priority
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vrid`	ID des virtuellen Routers	1 ... 255

Ergebnis

Das Priorität ist zurückgesetzt.

Weitere Hinweise

Sie konfigurieren eine VRRP3-Schnittstelle mit dem Befehl `interface`.

Sie legen die Priorität mit dem Befehl `vrrp priority` fest.

Sie ordnen IP-Adressen einem virtuellen Router mit dem Befehl `vrrp associated-ip` zu.

Sie zeigen die Priorität mit dem Befehl `show vrrp3` an.

10.1.5.7 vrrp timer

Beschreibung

Mit diesem Befehl legen Sie das Zeitintervall fest, nach dem ein virtueller Router im Zustand "Master" erneut ein Advertisement-Paket verschickt.

Voraussetzung

- Dem virtuellen Router ist eine IP-Adresse zugeordnet.
- Sie befinden sich im VRRP3 Interface Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-vrrp-v3-if-$$$)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
vrrp <vrid(1-255)> timer <interval(10-4095)centiseconds>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vrid`	ID des virtuellen Routers	1 ... 255
`interval`	Zeitintervall in Hundertstelsekunden	10 ... 4095 Default: 10

Ergebnis

Das Zeitintervall ist festgelegt.

Weitere Hinweise

Sie konfigurieren eine VRRP3-Schnittstelle mit dem Befehl `interface`.

Sie aktivieren das Routing über VRRP3 mit dem Befehl `router vrrp3`.

Sie setzen das Zeitintervall mit dem Befehl `no vrrp timer` auf den voreingestellten Wert zurück.

Sie ordnen IP-Adressen einem virtuellen Router mit dem Befehl `vrrp associated-ip` zu.

Sie zeigen das Intervall mit dem Befehl `show vrrp3` an.

10.1.5.8 no vrrp timer

Beschreibung

Mit diesem Befehl setzen Sie das Zeitintervall auf den voreingestellten Wert zurück

Voraussetzung

- Routing über VRRP3 ist aktiviert.
- Dem virtuellen Router ist eine IP-Adresse zugeordnet.
- Sie befinden sich im VRRP3 Interface Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-vrrp-v3-if-$$$)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no vrrp <vrid(1-255)> timer <interval(50-4095)centiseconds>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vrid`	ID des virtuellen Routers	1 ... 255
`interval`	Zeitintervall in Hundertstelsekunden	50 ... 4095

Ergebnis

Das Zeitintervall ist zurückgesetzt.

Weitere Hinweise

Sie konfigurieren eine VRRP3-Schnittstelle mit dem Befehl `interface`.

Sie aktivieren das Routing über VRRP3 mit dem Befehl `router vrrp3`.

Sie konfigurieren das Intervall mit dem Befehl `vrrp timer`.

Sie ordnen IP-Adressen einem virtuellen Router mit dem Befehl `vrrp associated-ip` zu.

Sie zeigen das Intervall mit dem Befehl `show vrrp3` an.

10.1.5.9 vrrp track decrement

Beschreibung

Mit diesem Befehl ordnen Sie einer Schnittstellenüberwachung eine VRRP-Schnittstelle zu und konfigurieren, um welchen Wert die Priorität verringert wird.

Voraussetzung

Sie befinden sich im VRRP Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-vrrp-v3-if-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
vrrp <vrid(1-255)> track <group-index> decrement <integer(1-254)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vrid`	ID des virtuellen Routers	1 ... 255
`group-index`	ID der Schnittstellenüberwachung	-
`integer`	Wert, um den die Priorität der VRRP-Schnittstelle verringert wird	1 ... 254

Ergebnis

Der Schnittstellenüberwachung ist eine VRRP-Schnittstelle zugeordnet. Der Wert, um den die Priorität verringert werden soll, ist definiert.

Weitere Hinweise

Sie löschen die Konfiguration mit dem Befehl `no vrrp track`.

Sie zeigen die Zuordnung und den Wert der Priorität mit dem Befehl `show vrrp3` oder `show vrrp3 interface` mit dem Parameter `detail` an.

Sie konfigurieren die Überwachung von Schnittstellen mit dem Befehl `track interface`.

10.1.5.10 no vrrp track

Beschreibung

Mit diesem Befehl löschen Sie die Zuordnung einer Schnittstellenüberwachung zu einer VRRP-Schnittstelle und den Wert, um den die Priorität verringert wird.

Voraussetzung

Sie befinden sich im VRRP Interface Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-vrrp-v3-if-$$$)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no vrrp <vrid(1-255)> track
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`vrid`	ID des virtuellen Routers	1 ... 255

Ergebnis

Der Zuordnung und der Wert, um den die Priorität verringert werden soll, sind gelöscht.

Weitere Hinweise

Sie ordnen einer Schnittstellenüberwachung eine VRRP-Schnittstelle zu und konfigurieren, um welchen Wert die Priorität verringt wird, mit dem Befehl `vrrp track decrement`.

Sie zeigen die Zuoprdnung und den Wert der Priorität mit dem Befehl `show vrrp3` oder `show vrrp3 interface` mit dem Parameter `detail` an.

10.2 NAT

In diesem Kapitel werden Befehle beschrieben, die für NAT / NAPT relevant sind.

10.2.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

10.2.1.1 show firewallnat masquerading

Beschreibung

Dieser Befehl zeigt die Schnittstellen an, an denen IP-Masquerading aktiviert ist.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show firewallnat masquerading
```

Ergebnis

Die Schnittstellen werden angezeigt.

10.2.1.2 show firewallnat napt

Beschreibung

Dieser Befehl zeigt die konfigurierten NAPT-Regeln an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show firewallnat napt
```

Ergebnis

Die konfigurierten NAPT-Regeln werden angezeigt.

10.2.1.3 show firewallnat netmap

Beschreibung

Dieser Befehl zeigt die konfigurierten NETMAP-Regeln an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show firewallnat netmap
```

Ergebnis

Die konfigurierten NETMAP-Regeln werden angezeigt.

10.2.1.4 show firewallnat src-nat

Beschreibung

Dieser Befehl zeigt die konfigurierten Source-NAT-Regeln an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show firewallnat src-nat
```

Ergebnis

Die konfigurierten Source-NAT-Regeln werden angezeigt.

10.2.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

10.2.2.1 firewallnat

Beschreibung

Mit diesem Befehl wechseln Sie in den FIREWALL NAT-Konfigurationsmodus.

Voraussetzung

Sie befinden sich jetzt im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
firewallnat
```

Ergebnis

Sie befinden sich jetzt im FIREWALL NAT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fwnat)#
```

Weitere Hinweise

Sie verlassen den FIREWALL NAT-Konfigurationsmodus mit dem Befehl `end` oder `exit`.

10.2.3 Befehle im FIREWALL NAT-Konfigurationsmodus

10.2.3.1 Einleitungssatz FirewallNAT Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im FIREWALL NAT-Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl `firewallnat` ein, um in diesen Modus zu wechseln.

- Wenn Sie den FIREWALL NAT-Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den FIREWALL NAT-Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

Verfügbare Schnittstellen

Als Quell- und Ziel-Schnittstellen sind folgende Schnittstellen verfügbar:

Schnittstelle		masquerading-nat napt	netmap src-nat	
VLAN	VLANs mit konfiguriertem Subnetz	x	x	`vlan num`
PPP	WAN-Schnittstelle	x	x	`ppp 2`
IPsec VPN	Alle IPsec VPN-Verbindungen	-	x	`ipsecall`
	Spezifische IPsec VPN-Verbindung	-	x	`ipsec num`
OpenVPN	Alle OpenVPN-Verbindungen	-	x	`openvpnall`
	Spezifische OpenVPN-Verbindung	-	x	`openvpn num`
SINEMA RC	Verbindung zum SINEMA RC-Server	-	x	`sinemarcall`

x: verfügbar

- : nicht verfügbar

10.2.3.2 ipsec connection show-idx

Beschreibung

Mit diesem Befehl zeigen Sie die Nummern der konfigurierten IPsec VPN-Verbindungen an.

Voraussetzung

Sie befinden sich im FIREWALL NAT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fwnat)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
ipsec connection show-idx
```

Ergebnis

Die Einträge werden aufgelistet.

10.2.3.3 masquerading show-idx

Beschreibung

Mit diesem Befehl zeigen Sie die Nummern der konfigurierten Regeln für Masquerading an.

Voraussetzung

Sie befinden sich im FIREWALL NAT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fwnat)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
masquerading show-idx
```

Ergebnis

Die Nummern werden aufgelistet.

Weitere Hinweise

Sie löschen eine Regel für Masquerading mit dem Befehl `no masquerading`.

Sie erstellen eine Regel für Masquerading mit dem Befehl `masquerading`.

10.2.3.4 masquerading

Beschreibung

Mit diesem Befehl aktivieren Sie an der Schnittstelle die Regeln für IP-Masquerading.

Voraussetzung

- VLAN-Schnittstelle mit Subnetzzuordnung
- Sie befinden sich im FIREWALL NAT-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fwnat)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
masquerading {vlan|ppp|usb} <num(0-4094)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`vlan`	VLAN-Schnittstelle	-
`ppp`	WAN-Schnittstelle	-
`usb`		-
`num`	Nummer des angesprochenen VLANs	Geben Sie einen gültigen Schnittstellenindex an. 0 ... 4094

Zur Bezeichnung von Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL NAT-Konfigurationsmodus (Seite 416)".

Ergebnis

An der angegebenen Schnittstelle sind die Regeln für IP-Masquerading aktiviert.

Weitere Hinweise

Sie deaktivieren IP-Masquerading mit dem Befehl `no masquerading`.

Sie zeigen die Einstellung mit dem Befehl `show masquerading` an.

10.2.3.5 no masquerading

Beschreibung

Mit diesem Befehl deaktivieren Sie an der Schnittstelle die Regeln für IP-Masquerading.

Voraussetzung

Sie befinden sich im FIREWALL NAT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fwnat)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no masquerading {{vlan|ppp|usb} <num(0-4094)>|all-int|show-int}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`vlan`	VLAN-Schnittstelle	-
`ppp`	WAN-Schnittstelle	-
`usb`		-

Parameter	Beschreibung	Wertebereich / Anmerkung
`num`	Nummer des angesprochenen VLANs	Geben Sie einen gültigen Schnittstellenindex an. 0 ... 4094
`all-int`	Deaktiviert an allen Schnittstellen die Regeln für IP-Masquerading.	-
`show-int`	Listet die verfügbaren Schnittstellen auf.	-

Zur Bezeichnung von Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL NAT-Konfigurationsmodus (Seite 416)".

Ergebnis

An der entsprechenden Schnittstelle sind die Regeln für IP-Masquerading deaktiviert.

Weitere Hinweise

Sie aktivieren IP-Masquerading mit dem Befehl `masquerading-nat`.

10.2.3.6 napt show-idx

Beschreibung

Mit diesem Befehl zeigen Sie die Nummern der konfigurierten NAPT-Regeln an.

Voraussetzung

Sie befinden sich im FIREWALL NAT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fwnat)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
napt show-idx
```

Ergebnis

Die Nummern werden aufgelistet.

Weitere Hinweise

Sie löschen eine NAPT-Regel mit dem Befehl `no napt`.

Sie erstellen eine NAPT-Regel mit dem Befehl `napt`.

10.2.3.7 napt type ipv4

Beschreibung

Mit diesem Befehl können Sie zusätzlich zur Adressumsetzung auch eine Port-Umsetzung konfigurieren.

Folgende Port-Umsetzungen sind möglich:

- Von einem einzigen Port zu dem gleichen Port:

  Wenn die Ports gleich sind, werden die Telegramme ohne Port-Umsetzung weitergeleitet.
- Von einem einzigen Port zu einem einzigen Port

  Die Telegramme werden auf den Port umgesetzt.
- Von einem Port-Bereich zu einem einzigen Port

  Die Telegramme aus dem Port-Bereich werden auf den gleichen Port umgesetzt (n:1).
- Von einem Port-Bereich zu dem gleichen Port-Bereich

  Wenn die Port-Bereiche gleich sind, werden die Telegramme ohne Port-Umsetzung weitergeleitet.

Voraussetzung

- VLAN-Schnittstelle mit Subnetzzuordnung
- Sie befinden sich im FIREWALL NAT-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fwnat)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
napt srcint <vlan> <num(0-4094)> proto {udp|tcp} dstport <num(1-65535)|range>
transport <num(1-65535)|range> type ipv4 transip <ip> [dstip <ip>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`srcint`	Schlüsselwort für die Quell-Schnittstelle	-
`vlan`	VLAN-Schnittstelle	-
`num`	Nummer des angesprochenen VLANs	0 ... 4094
`proto`	Schlüsselwort für Protokoll	-
`udp`	Adresszuordnung für UDP gültig.	-
`tcp`	Adresszuordnung für TCP gültig.	-
`dstport`	Schlüsselwort für Ziel-Port	
`num`	Ziel-Port	1 ... 65535

Parameter	Beschreibung	Wertebereich / Anmerkung
`range`	Portbereich	Geben Sie den Start-Port und End-Port an, z. B. 10 - 20.
`transport`	Schlüsselwort für neuen Ziel-Port	
`num`	Neuer Ziel-Port	1 ... 65535
`range`	Neuer Portbereich	Geben Sie den Start-Port und End-Port an, z. B. 10 - 20.
`transip`	Schlüsselwort für die IPv4-Adresse des Teilnehmers, an den dieses Telegramm weitergeleitet wird	-
`ip`	IPv4-Adresse	Geben Sie eine gültige IPv4-Adresse an.
`destip`	Schlüsselwort für die Ziel-IP-Adresse	-
`ip`	IPv4-Adresse	Geben Sie eine gültige IPv4-Adresse an.

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL NAT-Konfigurationsmodus (Seite 416)".

Hinweis

Wenn der Port bereits durch einen lokalen Dienst z. B. Telnet belegt ist, wird eine Warnmeldung ausgegeben. Vermeiden Sie auf jeden Fall die Nutzung von folgenden Ports: TCP-Port 23 (Telnet), Port 22 (SSH), die Ports 80/443 (http/https: Erreichbarkeit des Clients mit dem WBM), UDP-Port 161 (SNMP), Port 500 (ISAKMP), Port 4500 (IPsec Nat-T).

Ergebnis

Die NAPT-Regel ist erstellt. Beim Anlegen wird ein Eintrag mit einer eindeutigen Nummer (Index) angelegt.

Weitere Hinweise

Sie löschen eine NAPT-Regel mit dem Befehl `no napt`.

Sie löschen alle NAPT-Regeln mit dem Befehl `no napt all`.

Sie zeigen die Nummern der NAPT-Regeln mit dem Befehl `napt show-idx` an.

Sie zeigen die NAPT-Regel mit dem Befehl `show firewallnat napt` an.

10.2.3.8 no napt

Beschreibung

Mit diesem Befehl löschen Sie eine bestimmte NAPT-Regel.

Voraussetzung

- VLAN-Schnittstelle mit Subnetzzuordnung
- Sie befinden sich im FIREWALL NAT-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fwnat)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no napt srcint <vlan> <num(0-4094)> idx <num(1-200)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`srcint`	Schlüsselwort für die Quell-Schnittstelle	-
VLAN	VLAN-Schnittstelle	-
`num`	Nummer des angesprochenen VLANs	0 ... 4094
`idx`	Nummer, die einer bestimmten NAPT-Regel entspricht. Geben Sie eine gültige Nummer an.	0 ...200

Ergebnis

Die angegebene NAPT-Regel ist gelöscht.

Weitere Hinweise

Sie zeigen die Nummern der NAPT-Regeln mit dem Befehl `napt show-idx` an.

Sie löschen alle NAPT-Regeln mit dem Befehl `no napt all`.

Sie erstellen eine NAPT-Regel mit dem Befehl `napt type ipv4`.

10.2.3.9 no napt all

Beschreibung

Mit diesem Befehl löschen Sie alle NAPT-Regeln.

Voraussetzung

Sie befinden sich im FIREWALL NAT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fwnat)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no napt all
```

Ergebnis

Alle NAPT-Regeln sind gelöscht.

Weitere Hinweise

Sie erstellen eine NAPT-Regel mit dem Befehl `napt type ipv4`.

10.2.3.10 netmap destination srcint

Beschreibung

Mit diesem Befehl erstellen Sie die NETMAP-Regel für die Adressumsetzung der Ziel-IP-Adresse.

Voraussetzung

Sie befinden sich im FIREWALL NAT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fwnat)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
netmap destination srcint <vlan|ipsec|ipsecall|sinemarcall|openvpn|openvpnall>
[<num(0-4094)>] dstint <vlan|ipsec|ipsecall|sinemarcall|openvpn|openvpnall> [<num(0-
4094)>] type ipv4 srcip <*|subnet> dstip <subnet> transip <subnet> [auto-fwrules]
[auto-bidirectionalrule]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`srcint`	Schlüsselwort für die Quell-Schnittstelle	-
`vlan`	VLAN-Schnittstelle	-

`ipsec`
`ipsecall`
`sinemarcall`
`openvpn`
`openvpnall`
	Zugriff über VPN-Tunnelpartner, die über SINEMA RC, über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung <num> zu erreichen sind.	-

Parameter	Beschreibung	Wertebereich / Anmerkung
num	Nummer der VLAN-Schnittstelle oder der VPN-Verbindung	0 ... 4094
dstint	Schlüsselwort für die Ziel-Schnittstelle	-
vlan	VLAN-Schnittstelle	
ipsec ipsecall sinemarcall openvpn openvpnall	Zugriff auf die VPN-Tunnelpartner, die über SINEMA RC, über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung <num> zu erreichen sind.	-
num	Nummer der VLAN-Schnittstelle oder der VPN-Verbindung	0 ... 4094
srcip	Schlüsselwort für das Quell-Subnetz (Absender)	-
*	Alle iP-Adressen	-
subnet	Das Subnetz kann auch nur ein einzelner PC, oder eine andere Untermenge des Subnetzes sein.	Geben Sie das Subnetz in der CIDR-Notation an.
dstip	Schlüsselwort für das Ziel-Subnetz (Empfängers)	-
subnet	Das Subnetz kann auch nur ein einzelner PC, oder eine andere Untermenge des Subnetzes sein.	Geben Sie das Subnetz in der CIDR-Notation an.
transip	Schlüsselwort für das Subnetz, mit der das Ziel-Subnetz ersetzt wird.	-
subnet	Das Subnetz kann auch nur ein einzelner PC, oder eine andere Untermenge des Subnetzes sein.	Geben Sie das Subnetz in der CIDR-Notation an.
auto-fwrules	Automatisch wird die NETMAP-Regel für die Gegenrichtung erstellt.	-
auto-bidirectionalrule	Automatisch werden die IPv4-Firewallregeln erzeugt.	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL NAT-Konfigurationsmodus (Seite 416)".

Hinweis

Firewallregel bei Destination-NAT

Die Adressumsetzung mit NAT wurde bereits vor der Firewall durchgeführt, deshalb werden in der Firewall die umgesetzten Adressen verwendet.

`ipv4rule`

- `srcip <ip|subnet|range>`: Eingabe aus "`srcip <*|subnet>`"
- `dstip <ip|subnet|range>`: Eingabe aus "`transip <subnet>` "

Ergebnis

Die NETMAP-Regel für die Adressumsetzung der Ziel-IP-Adresse ist erstellt. Beim Erstellen wird ein Eintrag mit einer eindeutigen Nummer (Index) angelegt.

Weitere Hinweise

Sie löschen eine NETMAP-Regel mit dem Befehl `no netmap`.

Sie löschen alle NETMAP-Regeln mit dem Befehl `no netmap all`.

Sie zeigen die Nummern der NETMAP-Regeln mit dem Befehl `netmap show-idx` an.

Sie zeigen die NETMAP-Regel mit dem Befehl `show firewallnat netmap-nat` an.

Sie zeigen die IPv4-Firewallregeln mit dem Befehl `show firewall ip-rules ipv4` an.

10.2.3.11 netmap show-idx

Beschreibung

Mit diesem Befehl zeigen Sie die Nummern der konfigurierten NETMAP-Regeln an.

Voraussetzung

Sie befinden sich im FIREWALL NAT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fwnat)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
netmap show-idx
```

Ergebnis

Die Nummern werden aufgelistet.

Weitere Hinweise

Sie löschen eine NETMAP-Regel mit dem Befehl `no netmap`.

Sie löschen alle NETMAP-Regeln mit dem Befehl `no netmap all`.

Sie erstellen eine NETMAP-Regel mit den Befehlen `netmap source type ipv4` und `netmap destination type ipv4`.

10.2.3.12 netmap source type ipv4

Beschreibung

Mit diesem Befehl erstellen Sie die NETMAP-Regel für die Adressumsetzung der Quell-IP-Adresse.

Voraussetzung

Sie befinden sich im FIREWALL NAT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fwnat)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
netmap source srcint <vlan|ipsec|ipsecall|sinemarcall|openvpn|openvpnall> [<num(0-4094)>] dstint <vlan|ipsec|ipsecall|sinemarcall|openvpn|openvpnall> [<num(0-4094)>] type ipv4 srcip <subnet> transip <subnet> dstip <*|subnet>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`srcint`	Schlüsselwort für die Quell-Schnittstelle	-
`vlan`	VLAN-Schnittstelle	-

`ipsec`
`ipsecall`
`sinemarcall`
`openvpn`
`openvpnall`
	Zugriff über VPN-Tunnelpartner, die über SINEMA RC, über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung <num> zu erreichen sind.	-

`num`	Nummer der Schnittstelle oder der VPN-Verbindung	0 ... 4094

Parameter	Beschreibung	Wertebereich / Anmerkung
dstint	Schlüsselwort für die Ziel-Schnittstelle	-
vlan	VLAN-Schnittstelle	
ipsec ipsecall sinemarcipsec ipsecall sinemarcall openvpn openvpnall	Zugriff auf die VPN-Tunnelpartner, die über SINEMA RC, über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung <num> zu erreichen sind.	-
num	Nummer der Schnittstelle oder der VPN-Verbindung	0 ... 4094
srcip	Schlüsselwort für das Quell-Subnetz (Absenders)	-
subnet	Das Subnetz kann auch nur ein einzelner PC, oder eine andere Untermenge des Subnetzes sein.	Geben Sie das Subnetz in der CIDR-Notation an.
transip	Schlüsselwort für das Subnetz, mit der das Quell-Subnetz ersetzt wird.	-
subnet	Das Subnetz kann auch nur ein einzelner PC, oder eine andere Untermenge des Subnetzes sein.	Geben Sie das Subnetz in der CIDR-Notation an.
srcip	Schlüsselwort für das Quell-Subnetz (Absender)	-
*	Alle iP-Adressen	-
subnet	Das Subnetz kann auch nur ein einzelner PC, oder eine andere Untermenge des Subnetzes sein.	Geben Sie das Subnetz in der CIDR-Notation an.
auto-fwrules	Automatisch wird die NETMAP-Regel für die Gegenrichtung erstellt.	-
auto-bidirectionalrule	Automatisch werden die IPv4-Firewallregeln erzeugt.	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL NAT-Konfigurationsmodus (Seite 416)".

Hinweis

Firewallregel bei Source-NAT

Die Adressumsetzung mit Source-NAT wird erst nach der Firewall durchgeführt, deshalb werden die nicht umgesetzten Adressen verwendet.

`ipv4rule`

- `srcip <ip|subnet|range>`: Eingabe aus "`srcip <*|subnet>`"
- `dstip <ip|subnet|range>`: Eingabe aus " `dstip <*|subnet>`"

Ergebnis

Die NETMAP-Regel für die Adressumsetzung der Quell-IP-Adresse ist erstellt. Beim Erstellen wird ein Eintrag mit einer eindeutigen Nummer (Index) angelegt.

Weitere Hinweise

Sie löschen eine NETMAP-Regel mit dem Befehl `no netmap`.

Sie löschen alle NETMAP-Regeln mit dem Befehl `no netmap all`.

Sie zeigen die Nummern der NETMAP-Regeln mit dem Befehl `netmap show-idx` an.

Sie zeigen die NETMAP-Regel mit dem Befehl `show firewallnat netmap` an.

Sie zeigen die IPv4-Firewallregeln mit dem Befehl `show firewall ip-rules ipv4` an.

10.2.3.13 no netmap srcint

Beschreibung

Mit diesem Befehl löschen Sie eine bestimmte NETMAP-Regel.

Voraussetzung

Sie befinden sich im FIREWALL NAT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fwnat)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no netmap srcint <vlan|ipsec|ipsecall|sinemarcall|openvpn|openvpnall> [<num(0-4094)>]
dstint <vlan|ipsec|ipsecall|sinemarcall|openvpn|openvpnall> [<integer(0-4094)>] idx
<integer(1-200)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`srcint`	Schlüsselwort für die Quell-Schnittstelle	-
`vlan`	Typ bzw. Geschwindigkeit der Schnittstelle	-

`ipsec`
`ipsecall`
`sinemarcall`
`openvpn`
`openvpnall`
	Zugriff über VPN-Tunnelpartner, die über SINEMA RC, über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung <integer> zu erreichen sind.	-

`num`	Nummer der angesprochenen Schnittstelle	0 ... 4094
`dstint`	Schlüsselwort für die Ziel-Schnittstelle	-
`vlan`	Typ bzw. Geschwindigkeit der Schnittstelle	-

Parameter	Beschreibung	Wertebereich / Anmerkung

`ipsec`
`ipsecall`
`sinemarcall`
`openvpn`
`openvpnall`
	Zugriff über VPN-Tunnelpartner, die über SINEMA RC, über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung <integer> zu erreichen sind.	-

`integer`	Nummer der angesprochenen Schnittstelle	0 ... 4094
`idx`	Schlüsselwort für die Nummer der NETMAP-Regel	-
`integer`	Nummer, die einer bestimmten NETMAP-Regel entspricht.	Geben Sie eine gültige Nummer an. 0 ... 200

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL NAT-Konfigurationsmodus (Seite 416)".

Ergebnis

Die angegebene NETMAP-Regel ist gelöscht.

Weitere Hinweise

Sie zeigen die Nummern der NETMAP-Regeln mit dem Befehl `netmap show-idx` an.

Sie löschen alle NETMAP-Regeln mit dem Befehl `no netpmap all`.

Sie erstellen eine NETMAP-Regel mit den Befehlen `netmap source type ipv4` und `netmap destination type ipv4`.

10.2.3.14 no netmap all

Beschreibung

Mit diesem Befehl löschen Sie alle NETMAP-Regeln.

Voraussetzung

Sie befinden sich im FIREWALL NAT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fwnat)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no netmap all
```

Ergebnis

Alle NETMAP-Regeln sind gelöscht.

Weitere Hinweise

Sie erstellen eine NETMAP-Regel mit den Befehlen `netmap source type ipv4` und `netmap destination type ipv4`.

10.2.3.15 src-nat show-idx

Beschreibung

Mit diesem Befehl zeigen Sie die Nummern der konfigurierten Source-NAT-Regeln an.

Voraussetzung

Sie befinden sich im FIREWALL NAT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fwnat)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
src-nat show-idx
```

Ergebnis

Die Nummern werden aufgelistet.

Weitere Hinweise

Sie löschen eine Source-NAT-Regel mit dem Befehl `no src-nat`.

Sie löschen alle Source-NAT-Regeln mit dem Befehl `no src-nat all`.

Sie erstellen eine Source-NAT-Regel mit dem Befehl `src-nat type ipv4`.

10.2.3.16 src-nat type ipv4

Beschreibung

Mit diesem Befehl erstellen Sie eine Regel für Source-NAT.

Voraussetzung

Sie befinden sich im FIREWALL NAT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fwnat)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
src-nat srcint <vlan|ipsec|ipsecall|sinemarcall|openvpn|openvpnall> [<integer(0-
4094)>] dstint <vlan|ipsec|ipsecall|sinemarcall|openvpn|openvpnall> [<integer(0-
4094)>] type ipv4 srcip <ip|subnet> dstip <ip|subnet> [transip <ip>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
srcint	Schlüsselwort für die Quell-Schnittstelle	-
vlan	VLAN-Schnittstelle	-
ipsec ipsecall sinemarcall openvpn openvpnall	Zugriff über VPN-Tunnelpartner, die über SINEMA RC, über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung <integer> zu erreichen sind.	-
integer	Nummer der Schnittstelle oder der VPN-Verbindung	0 ... 4094
dstint	Schlüsselwort für die Ziel-Schnittstelle	-
vlan	VLAN-Schnittstelle	
ipsec ipsecall sinemarcall openvpn openvpnall	Zugriff auf die VPN-Tunnelpartner, die über SINEMA RC, über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung <integer> zu erreichen sind.	-
integer	Nummer der Schnittstelle oder der VPN-Verbindung	0 ... 4094
srcip	Schlüsselwort für die Quell-IP-Adresse	-
ip	IPv4-Adresse oder bestimmter IPv4-Adressbereich	Geben Sie eine gültige IPv4-Adresse oder einen IP-Adressbereich an.

Parameter	Beschreibung	Wertebereich / Anmerkung
`subnet`	Das Subnetz kann auch nur ein einzelner PC, oder eine andere Untermenge des Subnetzes sein.	Geben Sie das Subnetz in der CIDR-Notation an.
`dstip`	Schlüsselwort für die Ziel-IP-Adresse	-
`ip`	IPv4-Adresse oder bestimmter IPv4-Adressbereich	Geben Sie eine gültige IPv4-Adresse an.
`subnet`	Das Subnetz kann auch nur ein einzelner PC, oder eine andere Untermenge des Subnetzes sein.	Geben Sie das Subnetz in der CIDR-Notation an.
`transip`	Schlüsselwort für die IPv4-Adresse, mit der die IPv4-Adresse der Quelle ersetzt wird. **Hinweis** Wenn Sie den Parameter nicht verwenden, wird die IP-Adresse der ausgewählten Ziel-Schnittstelle verwendet.	-
`ip`	Wenn die Schnittstelle eine IPv4-Adresse besitzt, ist der Parameter optional. In diesem Fall wird die IPv4-Adresse der Schnittstelle verwendet.	Geben Sie eine gültige IPv4-Adresse an.

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL NAT-Konfigurationsmodus (Seite 416)".

Hinweis

Firewallregeln bei Source-NAT

Wenn Sie für eine Source-NAT-Regel eine entsprechende Firewall-Regel anlegen, verwenden Sie bei "IP-Regeln" für die "Quelle (Bereich)" die Eingabe aus "Quell-IP-Subnetz". Und für die "Ziel (Bereich)" verwenden Sie die Eingabe aus "Ziel-IP-Subnetz".

Ergebnis

Die Source-NAT-Regel ist erstellt. Beim Erstellen wird ein Eintrag mit einer eindeutigen Nummer (Index) angelegt.

Weitere Hinweise

Sie löschen eine Source-NAT-Regel mit dem Befehl `no src-nat`.

Sie löschen alle Source-NAT-Regeln mit dem Befehl `no src-nat all`.

Sie zeigen die Nummern der Source-NAT-Regeln mit dem Befehl `src-nat show-idx` an.

Sie zeigen die Source-NAT-Regel mit dem Befehl `show firewallnat src-nat` an.

10.2.3.17 no src-nat all

Beschreibung

Mit diesem Befehl löschen Sie alle Source-NAT-Regeln.

Voraussetzung

Sie befinden sich im FIREWALL NAT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fwnat)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
src-nat del all
```

Ergebnis

Alle Source-NAT-Regeln sind gelöscht.

Weitere Hinweise

Sie erstellen eine Source-NAT-Regel mit dem Befehl `src-nat type ipv4`.

10.2.3.18 no src-nat

Beschreibung

Mit diesem Befehl löschen Sie eine bestimmte Source-NAT-Regel.

Voraussetzung

Sie befinden sich im FIREWALL NAT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fwnat)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no src-nat srcint <vlan|ipsec|ipsecall|sinemarcall|openvpn|openvpnall> [<num(0-
4094)>] dstint <vlan|ipsec|ipsecall|sinemarcall|openvpn|openvpnall> [<num(0-4094)>]
idx <num(1-200)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`srcint`	Schlüsselwort für die Quell-Schnittstelle	-
`vlan`	VLAN-Schnittstelle	-

`ipsec`
`ipsecall`
`sinemarcall`
`openvpn`
`openvpnall`
	Zugriff über VPN-Tunnelpartner, die über SINEMA RC, über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung <num> zu erreichen sind.	-

`num`	Nummer der Schnittstelle oder der VPN-Verbindung	0 ... 4094
`dstint`	Schlüsselwort für die Ziel-Schnittstelle	-
`vlan`	VLAN-Schnittstelle	

`ipsec`
`ipsecall`
`sinemarcall`
`openvpn`
`openvpnall`
	Zugriff auf die VPN-Tunnelpartner, die über SINEMA RC, über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung <num> zu erreichen sind.	-

`num`	Nummer der Schnittstelle oder der VPN-Verbindung	0 ... 4094
`idx`	Schlüsselwort für die Nummer der Source-NAT-Regel	-
`num`	Nummer, die einer bestimmten Source-NAT-Regel entspricht.	Geben Sie eine gültige Nummer an. 0 ... 200

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL NAT-Konfigurationsmodus (Seite 416)".

Ergebnis

Die angegebene Source-NAT-Regel ist gelöscht.

Weitere Hinweise

Sie löschen alle Source-NAT-Regeln mit dem Befehl `no src-nat all`.

Sie erstellen eine Source-NAT-Regel mit dem Befehl `src-nat type ipv4`.

Sie zeigen die Nummern der Source-NAT-Regeln mit dem Befehl `src-nat show-idx` an.

Sicherheit und Authentifizierung 11

In diesem Abschnitt finden Sie die Kapitel, die Zugriffsrechte und Authentifizierungsverfahren beschreiben.

11.1 RADIUS-Client

RADIUS (Remote Authentication Dial-In User Service) ist ein Client-Server-Protokoll, das die zentrale Anmeldung von Benutzern ermöglicht, die sich in einem physikalischen oder virtuellen Netzwerk anmelden. Damit ist eine zentrale Verwaltung der Benutzerdaten möglich.

In diesem Kapitel werden Befehle beschrieben, die für die Konfiguration dieses Dienstes relevant sind.

11.1.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

11.1.1.1 show radius statistics

Beschreibung

Dieser Befehl zeigt die Verbindungsstatistik vom RADIUS-Client zum RADIUS-Server an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show radius statistics
```

Ergebnis

Die Verbindungsstatistik wird angezeigt.

11.1.1.2 show radius server

Beschreibung

Dieser Befehl zeigt die RADIUS Server Konfiguration an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show radius server [{<ucast_addr> | <ip6_addr>}]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ucast_addr`	Wert für eine IPv4-Unicast Adresse	Geben Sie eine gültige Unicast-Adresse an.
`ip6_addr`	Wert für eine IPv6-Adresse	Geben Sie eine gültige IPv6-Adresse an.

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Wenn Sie keinen Parameter angeben, werden alle konfigurierten RADIUS-Server angezeigt.

Ergebnis

Die RADIUS Server Konfiguration wird angezeigt.

11.1.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

11.1.2.1 login authentication

Beschreibung

Mit diesem Befehl ermöglichen Sie die Authentifizierung über einen RADIUS-Server.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
login authentication {radius | local-and-radius | radius-fallback-local}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`radius`	Die Anmeldung erfolgt über einen RADIUS-Server.	-
`local-and-radius`	Die Anmeldung kann sowohl über die in der Firmware vorhandenen Benutzer (Benutzername und Passwort) als auch über einen RADIUS-Server erfolgen.	Die lokalen Benutzer haben Vorrang. Es wird zuerst in der lokalen Datenbank nach dem Benutzer gesucht. Wenn der Benutzer dort nicht vorhanden ist, wird eine RADIUS-Anfrage verschickt.
`radius-fallback-local`	Die Authentifizierung muss über einen RADIUS-Server erfolgen.	Nur wenn der RADIUS-Server im Netz nicht erreichbar ist, wird eine lokale Authentifizierung durchgeführt.

Ergebnis

Die Authentifizierung erfolgt je nach gewähltem Parameter.

Weitere Hinweise

Sie deaktivieren die Authentifizierung über einen RADIUS-Server mit dem Befehl `no login authentication`.

Sie zeigen den Status dieser Funktion und weitere Informationen mit dem Befehl `show device information` an.

11.1.2.2 no login authentication

Beschreibung

Mit diesem Befehl deaktivieren Sie die Authentifizierung über einen RADIUS-Server.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no login authentication
```

Ergebnis

Die RADIUS-Authentifizierung ist deaktiviert.

Hinweis

Die Anmeldung ist nur mit lokalem Benutzernamen und Passwort möglich. Wenn die lokale Anmeldung fehlschlägt, findet keine Authentifizierung über einen RADIUS-Server statt.

Weitere Hinweise

Sie aktivieren die Authentifizierung über einen RADIUS-Server mit dem Befehl `login authentication`.

11.1.2.3 radius authorization-mode

Beschreibung

Mit diesem Befehl legen Sie bei der Login-Authentifizierung fest, wie bei einer erfolgreichen Authentifizierung die Rechtevergabe für die Benutzer erfolgt.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
radius authorization-mode { standard | vendor-specific }
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`standard`	In diesem Modus wird der Benutzer mit Administratorrechten angemeldet, wenn der Server für das Attribut "Service Type" den Wert "Administrative User" an das Gerät zurückgibt. In allen anderen Fällen wird der Benutzer mit Leserechten angemeldet.	Default
`vendor-specific`	In diesem Modus ist die Rechtevergabe davon abhängig, ob und welche Gruppe der Server für den Benutzer zurück gibt und ob es für den Benutzer einen Eintrag in der Tabelle "Externe Benutzeraccounts" gibt.	-

Ergebnis

Die Rechtevergabe bei der Login-Authentifizierung ist definiert.

Weitere Hinweise

Sie zeigen den Status dieser Funktion und weitere Informationen mit dem Befehl `show device information` an.

11.1.2.4 radius-server

Beschreibung

Mit diesem Befehl konfigurieren Sie einen RADIUS-Server-Eintrag auf dem RADIUS-Client.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
radius-server { ipv4 <ipv4-address> | fqdn-name <FQDN> } [auth-port <portno(1-65535)>] [retransmit <1-5>] [key <secret-key-string>] >] [primary] [test]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ipv4`	Schlüsselwort für eine IPv4-Adresse	-
`ipv4-address`	IPv4-Adresse des RADIUS-Servers	Geben Sie eine gültige IPv4-Adresse an.
`fqdn-name`	Schlüsselwort für einen Domainnamen	-
`FQDN`	Domainname (Fully Qualified Domain Name)	Maximal 100 Zeichen
`auth-port`	Schlüsselwort für die UDP-Portnummer für die Authentifizierung	
`portno`	Nummer des Ports	1 … 65535 Default:1812
`retransmit`	Schlüsselwort für die Anzahl der Wiederholungen eines Verbindungsversuchs	-
`-`	Geben Sie die maximale Anzahl der Wiederholungen eines Anfrageversuchs ein. Der initiale Verbindungsversuch wird um den hier angegebenen Wert wiederholt, bevor ein anderer konfigurierter RADIUS-Server angefragt wird oder die Anmeldung für gescheitert erklärt wird.	1 ... 5 Default: 3 (Wiederholungen, das bedeutet 4 Verbindungsversuche)
`key`	Schlüsselwort für den Schlüssel für die Kommunikation zwischen dem Authenticator und dem Server	-
`secret-key-string`	Wert für den Schlüssel	128 Zeichen Default: leere Zeichenkette
`primary`	Kennzeichnet den RADIUS-Server als primären Server	-
`test`	Testet, ob der angegebene RADIUS-Server verfügbar ist oder nicht. Sie können gleichzeitig einen neuen RADIUS-Server anlegen und den Test durchführen.	

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Adressen und Schnittstellenbezeichnungen (Seite 42)".

Wenn beim Konfigurieren optionale Parameter nicht angegeben werden, gelten die voreingestellten Werte.

Hinweis

Primärer Server

In einem Netzwerk kann nur ein RADIUS-Server als primärer Server gekennzeichnet sein.

Wenn Sie einen RADIUS-Server als primären Server kennzeichnen, ersetzt dieser den Server, der bisher als primärer Server gekennzeichnet war.

11.1.2.5 no radius-server

Beschreibung

Mit diesem Befehl löschen Sie einen RADIUS-Server-Eintrag auf dem Client.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no radius-server {ipv4 <ipv4-address> | fqdn-name <FQDN>} [primary]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ipv4`	Schlüsselwort für eine IPv4-Adresse	-
`ipv4-address`	IPv4-Adresse des RADIUS-Servers	geben Sie eine gültige IPv4-Adresse an
`fqdn-name`	Schlüsselwort für einen Domainnamen	-
`FQDN`	Domainname (Fully Qualified Domain Name)	Maximal 100 Zeichen
`primary`	kennzeichnet den RADIUS-Server als primären Server	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Adressen und Schnittstellenbezeichnungen" (Seite 42).

Ergebnis

Der Eintrag für eine Verbindung des RADIUS-Clients mit einem Server bzw. die Kennzeichnung als primärer Server ist gelöscht.

Weitere Hinweise

Sie konfigurieren die Verbindung eines RADIUS-Clients mit einem Server mit dem Befehl `radius-server`.

Sie zeigen die Konfiguration eines RADIUS-Servers auf dem Client mit dem Befehl `show radius server` an.

Sie zeigen statistische Informationen zu dieser Funktion mit dem Befehl `show radius statistics` an.

11.2 Benutzerverwaltung

In diesem Kapitel werden Befehle für den Zugang als Administrator und die Konfiguration der Authentifizierungsmethode beschrieben.

11.2.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

11.2.1.1 show password-policy

Beschreibung

Dieser Befehl zeigt an, welche Passwortrichtlinie aktuell verwendet wird.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show password-policy
```

Ergebnis

Die akutell gültige Passwortrichtlinie wird angezeigt.

Weitere Hinweise

Sie konfigurieren die Passwortrichtlinie mit dem Befehl `password-policy`.

11.2.1.2 show roles

Beschreibung

Dieser Befehl zeigt die angelegten Rollen an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show roles
```

Ergebnis

Die angelegten Rollen werden angezeigt.

Weitere Hinweise

Sie erstellen eine Rolle mit dem Befehl `role`.

Sie löschen eine Rolle mit dem Befehl `no role`.

11.2.1.3 show user-accounts

Beschreibung

Dieser Befehl zeigt die angelegten Benutzer an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show user-accounts [external]
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`external`	Schlüsselwort für die Tabelle "Externe Benutzerkonten"	-

Wenn Sie den optionalen Parameter nicht angeben, werden die lokalen Benutzer angezeigt.

Ergebnis

Die angelegten Benutzer werden angezeigt.

Weitere Hinweise

Sie legen einen neuen lokalen Benutzer an und erstellen einen Eintrag in der Tabelle "Externe Benutzerkonten" mit dem Befehl `user-account`.

Sie verknüpfen einen Benutzer, der auf einem externen Server angelegt ist, mit einer Rolle auf dem Gerät in der Tabelle "Externe Benutzerkonten" mit dem Befehl `user-account-ext`.

Sie löschen einen lokalen Benutzer und den entsprechenden Eintrag in der Tabelle "Externe Benutzerkonten" mit dem Befehl `no user-account`.

Sie löschen eine Verknüpfung in der Tabelle "Externe Benutzerkonten" mit dem Befehl `no user-account-ext`.

11.2.1.4 show user-groups

Beschreibung

Dieser Befehl zeigt die Verknüpfungen zwischen Gruppen und Rollen.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show user-groups
```

Ergebnis

Die Verknüpfungen werden angezeigt.

Weitere Hinweise

Sie verknüpfen eine Gruppe mit einer Rolle mit dem Befehl `user-group`.

Sie löschen eine Verknüpfung mit dem Befehl `no user-group`.

11.2.1.5 show users

Beschreibung

Dieser Befehl zeigt die angemeldeten CLI-Benutzer an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show users
```

Ergebnis

Die angemeldeten CLI-Benutzer werden angezeigt.

11.2.2 change password

Beschreibung

Mit diesem Befehl ändern Sie das Passwort des aktuell angemeldeten Benutzers.

Voraussetzung

- Sie sind mit einem lokalen Benutzerkonto auf dem Gerät angemeldet.
- Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

  Die Eingabeaufforderung lautet:

  `cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
change password <passwd>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`passwd`	Wert für das Passwort	Geben Sie das Passwort an. Die Eingabe ist von der Passwortrichtlinie abhängig. Der Befehl `show password-policy` zeigt an, welche Passwortrichtlinie aktuell verwendet wird.

Ergebnis

Das Passwort ist geändert.

Hinweis

Passwort ändern im Trial-Modus

Auch wenn Sie im Trial-Modus das Passwort ändern, wird diese Änderung sofort gespeichert.

Weitere Hinweise

Sie erstellen einen Benutzer mit dem Befehl `user-account`.

Sie löschen einen Benutzer mit dem Befehl `no user-account`.

Sie zeigen die angelegten Benutzer mit dem Befehl `show user-accounts` an.

Sie konfigurieren die Passwortrichtlinie mit dem Befehl `password-policy`.

11.2.3 whoami

Beschreibung

Dieser Befehl zeigt den Benutzernamen des angemeldeten Benutzers an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
whoami
```

Ergebnis

Der Benutzername des angemeldeten Benutzers wird angezeigt.

11.2.4 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

11.2.4.1 loginpage

Beschreibung

Mit diesem Befehl legen Sie fest, mit welcher Anmeldeseite das WBM standardmäßig startet.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
loginpage {configuration | firewall}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`configuration`	Anmelden am WBM	-
`firewall`	Anmelden an der WBM-Seite für benutzerspezifische Firewall.	-

Ergebnis

Die Standard-Anmeldeseite ist konfiguriert.

11.2.4.2 password-policy

Beschreibung

Mit diesem Befehl legen Sie fest, welche Passwortrichtlinie bei der Vergabe von neuen Passwörtern beachtet wird.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
password-policy < low | high >
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
low	Passwortrichtlinie: Niedrig	Passwortlänge: mindestens 6 Zeichen
high	Passwortrichtlinie: Hoch	Passwortlänge: mindestens 8 Zeichen: Mindestens 1 Großbuchstabe Mindestens 1 Sonderzeichen Mindestens 1 Zahl

Ergebnis

Die Passwortrichtlinie ist festgelegt.

Weitere Hinweise

Sie vergeben ein neues Passwort mit dem Befehl `user-account`.

Sie zeigen die Einstellung mit dem Befehl `show password-policy` an.

11.2.4.3 role

Beschreibung

Mit diesem Befehl erstellen Sie Rollen, die lokal auf dem Gerät gültig sind.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
role <role-name> function-rights <function-rights-value(1-15)> [description <role-description>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`role-name`	Rollenname	Geben Sie einen Namen für die Rolle ein. Der Name muss folgende Bedingungen erfüllen: • Er muss eindeutig sein. • Er muss zwischen 1 und 64 Zeichen lang sein.
`function-rights`	Schlüsselwort für die Funktionsrechte	-
`function-rights-value`	Wert der Funktionsrechte	Wählen Sie die Funktionsrechte der Rolle aus: • 1 Benutzer mit dieser Rolle können Geräteparameter lesen aber nicht verändern. • 15 Benutzer mit dieser Rolle können Geräteparameter sowohl lesen als auch verändern.
`description`	Schlüsselwort für die Beschreibung	-
`role-description`	Inhalt der Beschreibung	Geben Sie eine Beschreibung für die Rolle ein. Der Beschreibungstext kann bis zu 100 Zeichen lang sein.

Ergebnis

Die Rolle ist angelegt.

Hinweis

Rollenname nicht änderbar

Nach dem Anlegen einer Rolle kann der Rollenname nicht mehr geändert werden.

Wenn ein Rollenname geändert werden soll, dann muss die Rolle gelöscht und eine neue Rolle angelegt werden.

Hinweis

Funktionsrechte eingeschränkt änderbar

Sie können die Funktionsrechte einer Rolle nur ändern, wenn die Rolle nicht mit einem Benutzer verknüpft ist.

Weitere Hinweise

Sie löschen eine Rolle mit dem Befehl `no role`.

Sie zeigen die angelegten Rollen mit dem Befehl `show roles`.

11.2.4.4 no role

Beschreibung

Mit diesem Befehl löschen Sie eine Rolle.

Hinweis

Sie können eine Rolle nur löschen, wenn sie nicht mit einem Benutzer verknüpft ist.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no role <role-name>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
role-name	Rollenname	Geben Sie den Namen einer Rolle ein.

Ergebnis

Die Rolle ist gelöscht.

Weitere Hinweise

Sie erstellen eine Rolle mit dem Befehl `role`.

Sie zeigen die angelegten Rollen mit dem Befehl `show roles`.

11.2.4.5 user-account

Beschreibung

Mit diesem Befehl legen Sie einen neuen Benutzer an. Zudem können Sie das Passwort/die Rolle eines bereits angelegten Benutzers ändern.

Voraussetzung

- Der Benutzer ist mit der Rolle "admin" angemeldet.
- Sie befinden sich im globalen Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
user-account <user-name> password <user-password> role <user-role> [description
<user-description>][remote-access {none|additional|only}]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`user-name`	Benutzername	Geben Sie den Namen für den Benutzer ein. Der Name muss folgende Bedingungen erfüllen: • Er muss eindeutig sein. • Er muss zwischen 1 und 250 Zeichen lang sein. • Er darf folgende Zeichen nicht enthalten: § ? " ; : Die Zeichen für Space und Delete dürfen auch nicht enthalten sein.
`password`	Schlüsselwort für ein Passwort	-
`user-password`	Wert für das Passwort	Geben Sie das Passwort an. Es darf folgende Zeichen nicht enthalten: • § ? " ; : • Die Zeichen für Space und Delete dürfen auch nicht enthalten sein. Die Stärke des Passworts ist abhängig von der eingestellten Passwortrichtlinie: • `low`: Passwortlänge: mindestens 6 Zeichen • `high`: Das Passwort muss Folgendes erfüllen: – Passwortlänge: mindestens 8 Zeichen – Mindestens 1 Großbuchstabe – Mindestens 1 Sonderzeichen – Mindestens 1 Zahl
`role`	Schlüsselwort für eine Rolle	-
`user-role`	Rolle	Geben Sie eine Rolle ein. Sie können zwischen den voreingestellten und selbst definierten Rollen wählen.
`description`	Schlüsselwort für die Beschreibung	-

Parameter	Beschreibung	Wertebereich / Anmerkung
`user-description`	Inhalt der Beschreibung	Geben Sie eine Beschreibung für das Benutzerkonto ein. Der Beschreibungstext kann bis zu 100 Zeichen lang sein.
`remote-access`	Remote-Zugriff	• none Kein Remote-Zugriff. Der Benutzer wird mit den Rechten der verknüpften Rolle angemeldet. • additional Remote-Zugriff und Rechte, die dem Benutzer zugeordnet sind. • only Nur Remote-Zugriff, d. h. keine Rechte außer das Anmelden an der WBM-Seite für benutzerspezifische Firewall.

Hinweis

Benutzernamen: admin

Mit diesem Benutzernamen können Sie das Gerät konfigurieren.

Wenn Sie sich das erste Mal oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" anmelden, werden Sie aufgefordert das vordefinierte Passwort "admin" zu ändern. Zusätzlich können Sie einmalig den werksseitig voreingestellten Benutzer "admin" umbenennen. Danach ist ein Umbenennen von "admin" nicht mehr möglich.

Ergebnis

Der neue Benutzer ist angelegt oder das Passwort / Rolle ist geändert.

Hinweis

Änderungen im Modus "Trial"

Auch wenn sich das Gerät im Modus "Trial" befindet, werden diese Änderungen sofort gespeichert.

Hinweis

Die werksseitig voreingestellten Benutzer sowie angemeldete Benutzer können nicht gelöscht oder geändert werden.

Weitere Hinweise

Sie löschen einen Benutzer mit dem Befehl `no user-account`.

Sie zeigen die angelegten Benutzer mit dem Befehl `show user-accounts`.

Sie zeigen die aktuell gültige Passwortrichtlinie mit dem Befehl `show password-policy` an.

11.2.4.6 no user-account

Beschreibung

Mit diesem Befehl löschen Sie einen Benutzer.

Hinweis

Der voreingestellten Benutzer "admin" und angemeldete Benutzer können nicht gelöscht werden.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no user-account <user-name>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
user-name	Benutzername	Geben Sie einen gültigen Benutzernamen an.

Ergebnis

Der Benutzer ist gelöscht.

Weitere Hinweise

Sie erstellen einen Benutzer mit dem Befehl `user-account`.

Sie zeigen die angelegten Benutzer mit dem Befehl `show user-accounts`.

11.2.4.7 user-account-ext

Beschreibung

Mit diesem Befehl verknüpfen Sie einen Benutzer mit einer Rolle in der Tabelle "Externe Benutzerkonten". Der Benutzer ist auf einem RADIUS-Server definiert. Die Rolle ist lokal auf dem Gerät definiert.

Wenn ein RADIUS-Server einen Benutzer authentifiziert, die zugehörige Gruppe jedoch unbekannt oder nicht vorhanden ist, prüft das Gerät, ob es für den Benutzer einen Eintrag in der Tabelle "Externe Benutzerkonten" gibt. Wenn ein entsprechender Eintrag existiert, wird der Benutzer mit den Rechten der verknüpften Rolle angemeldet. Wenn die zugehörige Gruppe auf dem Gerät bekannt ist, werden beide Tabellen ausgewertet. Dem Benutzer wird die Rolle mit den größeren Rechten zugewiesen.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
user-account-ext <user-name-ext> role <user-role-ext> [description <user-ext-
description>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`user-account-ext`	Schlüsselwort für einen Benutzer für die Tabelle "Externe Benutzerkonten"	-
`user-name-ext`	Benutzername	Geben Sie den Namen für den Benutzer ein. Der Name muss folgende Bedingungen erfüllen: • Er muss eindeutig sein. • Er muss zwischen 1 und 250 Zeichen lang sein.
`role`	Schlüsselwort für den Rollennamen	-
`user-role-ext`	Rollenname	Geben Sie eine Rolle ein. Sie können zwischen den voreingestellten und selbst definierten Rollen wählen.

Parameter	Beschreibung	Wertebereich / Anmerkung
`description`	Schlüsselwort für die Beschreibung	-
`user-ext-description`	Inhalt der Beschreibung	Geben Sie eine Beschreibung für den Benutzer in der Tabelle "Externe Benutzerkonten" ein. Der Beschreibungstext kann bis zu 100 Zeichen lang sein.

Ergebnis

Die Verknüpfung in der Tabelle "Externe Benutzerkonten" ist angelegt.

Hinweis

Benutzername nicht änderbar

Nach dem Anlegen eines Benutzers kann der Benutzername nicht mehr geändert werden. Wenn ein Benutzername geändert werden soll, muss der Benutzer gelöscht und ein neuer Benutzer angelegt werden.

Weitere Hinweise

Sie löschen eine Verknüpfung mit dem Befehl `no user-account-ext`.

Sie zeigen die Verknüpfungen in der Tabelle "Externe Benutzerkonten" mit dem Befehl `show user-accounts external`.

11.2.4.8 no user-account-ext

Beschreibung

Mit diesem Befehl löschen Sie die Verknüpfung zwischen einem Benutzer und einer Rolle in der Tabelle "Externe Benutzerkonten".

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no user-account-ext <user-name-ext>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`user-name-ext`	Benutzername	Geben Sie den Namen eines Benutzers ein.

Ergebnis

Die Verknüpfung in der Tabelle "Externe Benutzerkonten" ist gelöscht.

Weitere Hinweise

Sie verknüpfen einen Benutzer mit einer Rolle in der Tabelle "Externe Benutzerkonten" mit dem Befehl `user-account-ext`.

Sie zeigen die Verknüpfungen in der Tabelle "Externe Benutzerkonten" mit dem Befehl `show user-accounts external`.

11.2.4.9 user-group

Beschreibung

Mit diesem Befehl verknüpfen Sie eine Gruppe mit einer Rolle.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
user-group <user-group-name> role <role-name> [description <user-group-description>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`user-group`	Schlüsselwort für einen Gruppennamen	-
`user-group-name`	Gruppenname	Geben Sie den Namen der Gruppe ein. Der Name muss der Gruppe auf dem RADIUS-Server entsprechen. Der Name muss folgende Bedingungen erfüllen: • Er muss eindeutig sein. • Er muss zwischen 1 und 64 Zeichen lang sein.
`role`	Schlüsselwort für den Rollennamen	-
`role-name`	Rollenname	Geben Sie einen Rollennamen ein. Benutzer, die über den RADIUS-Server mit der verknüpften Gruppe autorisiert werden, erhalten die Rechte dieser Rolle lokal auf dem Gerät. Sie können zwischen den voreingestellten und selbst definierten Rollen wählen.
`description`	Schlüsselwort für die Beschreibung	-
`user-group-description`	Inhalt der Beschreibung	Geben Sie eine Beschreibung für die Verknüpfung an. Der Beschreibungstext kann bis zu 100 Zeichen lang sein.

Ergebnis

Die Gruppe ist mit einer Rolle verknüpft.

Weitere Hinweise

Sie löschen eine Verknüpfung mit dem Befehl `no user-group`.

Sie zeigen die angelegten Verknüpfungen mit dem Befehl `show user-groups`.

11.2.4.10 no user-group

Beschreibung

Mit diesem Befehl löschen Sie die Verknüpfung zwischen einer Gruppe und einer Rolle.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no user-group <user-group-name>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`user-group-name`	Gruppenname	Geben Sie den Namen einer Gruppe ein.

Ergebnis

Die Verknüpfung ist gelöscht.

Weitere Hinweise

Sie verknüpfen eine Gruppe mit einer Rolle mit dem Befehl `user-group`.

Sie zeigen die angelegten Verknüpfungen mit dem Befehl `show user-groups`.

11.2.4.11 username

Beschreibung

Mit diesem Befehl ändern Sie das Passwort für Benutzer mit den Benutzernamen "`user`" oder "`admin`".

Voraussetzung

- Der Benutzer ist mit der Rolle "admin" angemeldet.
- Sie befinden sich im globalen Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
username {user|admin} password <passwd>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`user`	Benutzer mit dem Benutzernamen "`user`".	Wenn Sie einen Benutzer mit dem Benutzernamen "`user`" angelegt haben, können Sie mit diesem Befehl das Passwort für diesen Benutzer ändern.
`admin`	Benutzer mit dem Benutzernamen "`admin`".	Wenn Sie den werkseitig voreingestellten Benutzer "`admin`" nicht umbenannt haben, können Sie mit diesem Befehl das Passwort für diesen Benutzer ändern.
`password`	Schlüsselwort für ein Passwort	-
`passwd`	Wert für das Passwort	Geben Sie das Passwort an. Die Stärke des Passworts ist abhängig von der eingestellten Passwortrichtlinie: • `low`: Passwortlänge: mindestens 6 Zeichen • `high`: Das Passwort muss Folgendes erfüllen: – Passwortlänge: mindestens 8 Zeichen – Mindestens 1 Großbuchstabe – Mindestens 1 Sonderzeichen – Mindestens 1 Zahl

Ergebnis

Das Passwort ist geändert.

Hinweis

Passwort ändern im Trial-Modus

Auch wenn Sie im Trial-Modus das Passwort ändern, wird diese Änderung sofort gespeichert.

Weitere Hinweise

Sie zeigen die angelegten Benutzer mit dem Befehl `show user-accounts`.

Sie können die Passwörter auch mit dem Befehl `user-account` ändern.

Sie zeigen die aktuell gültige Passwortrichtlinie mit dem Befehl `show password-policy` an.

11.3 Firewall

11.3.1 Einleitung zum Kapitel Firewall

In diesem Kapitel werden Befehle beschrieben, die für Firewall relevant sind.

11.3.2 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

11.3.2.1 show firewall icmp-services ipv4

Beschreibung

Dieser Befehl zeigt die konfigurierten ICMPv4-Dienste an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show firewall icmp-services ipv4
```

Ergebnis

Die konfigurierten ICMPv4-Dienste werden angezeigt.

11.3.2.2 show firewall information

Beschreibung

Dieser Befehl zeigt die Konfiguration der Firewall an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show firewall information
```

Ergebnis

Die Konfiguration wird angezeigt.

11.3.2.3 show firewall ip-protocols

Beschreibung

Dieser Befehl zeigt die konfigurierten Protokolle an

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show firewall ip-protocols
```

Ergebnis

Die konfigurierten Protokolle werden angezeigt.

11.3.2.4 show firewall ip-rules ipv4

Beschreibung

Dieser Befehl zeigt eine Übersicht der IPv4-Firewallregeln an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show firewall ip-rules ipv4
```

Ergebnis

Die Übersicht der IPv4-Firewallregeln wird angezeigt.

11.3.2.5 show firewall ip-services

Beschreibung

Dieser Befehl zeigt die konfigurierten IP-Dienste an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

show firewall ip-services

Ergebnis

Die konfigurierten IP-Dienste werden angezeigt.

11.3.2.6 show firewall pre-rules ipv4

Beschreibung

Dieser Befehl zeigt die vordefinierten IPv4-Regeln an, die an der Schnittstelle verfügbar sind.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show firewall pre-rules ipv4
```

Ergebnis

Die vordefinierten IPv4-Regeln werden angezeigt.

11.3.2.7 show firewall ruleset

Beschreibung

Dieser Befehl zeigt die benutzerdefinierten Regelsätze an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show firewall ruleset
```

Ergebnis

Die die benutzerdefinierten Regelsätze werden angezeigt.

11.3.2.8 show firewall ruleset assignment

Beschreibung

Dieser Befehl zeigt die Zuordung der Regelsätze.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show firewall ruleset assignment
```

Ergebnis

Die Zuordnung wird angezeigt.

11.3.3 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

11.3.3.1 firewall

Beschreibung

Mit diesem Befehl wechseln Sie in den FIREWALL-Konfigurationsmodus.

Voraussetzung

Sie befinden sich jetzt im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
firewall
```

Ergebnis

Sie befinden sich jetzt im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Weitere Hinweise

Sie verlassen den FIREWALL-Konfigurationsmodus mit dem Befehl `end`.

11.3.4 Befehle im FIREWALL-Konfigurationsmodus

11.3.4.1 Einleitungssatz Firewall Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im FIREWALL-Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl `firewall` ein, um in diesen Modus zu wechseln.

- Wenn Sie den FIREWALL-Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den FIREWALL-Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

Verfügbare Schnittstellen

Als Quell- und Ziel-Schnittstellen sind folgende Schnittstellen verfügbar:

Schnittstelle		vordefi-nierte Firewall-Regeln	eigene Fire-wall-Regeln	
VLAN	VLANs mit konfiguriertem Subnetz	x	x	`vlan integer(0)`
PPP (vlan)	WAN-Schnittstelle	x	x	`ppp 2`
IPsecVPN	Alle IPsec VPN-Verbindungen	-	x	`IPsecall`
	Spezifische IPsec VPN-Verbindung	-	x	`IPsec ifnum`
Open VPN	Alle OpenVPN-Verbindungen			`OpenVPNall`
	Spezifische OpenVPN-Verbindung	-	x	`OpenVPN ifnum`
SINEMA RC	Verbindung zum Sinema RC-Server	-	x	`SinemaRC`
`Device`	Verbindung zum Gerät	-	x	`Device`

x: verfügbar

- : nicht verfügbar

Kommunikationsrichtungen

von	nach	Bedeutung
`vlan (1-x)`	`vlan (1-x)`	Zugriff vom IP-Subnetz vlan x auf das IP-Subnetz vlan x. Beispiel: vlan1 (INT) → vlan2 (EXT) Zugriff vom lokalen IP-Subnetz und dem Gerät auf das externe IP-Subnetz.
	`ppp 2`	Zugriff vom IP-Subnetz auf die WAN-Schnittstelle des Geräts.
	`Device`	Zugriff vom IP-Subnetz auf das Gerät.
	`SinemaRC`	Zugriff vom IP-Subnetz und dem Gerät auf den SINEMA RC-Server.

	`IPsecall`
	`IPsec ifnum`
	`OpenVPNall`
	`OpenVPN ifnum`
		Zugriff vom IP-Subnetz auf die VPN-Tunnelpartner, die über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung (`ifnum`) zu erreichen sind.

`Device`	`vlan (1-x)`	Zugriff vom Gerät auf das IP-Subnetz.
	`ppp 2`	Zugriff vom Gerät auf die WAN-Schnittstelle des Geräts.
	`SinemaRC`	Zugriff vom Gerät auf den SINEMA RC-Server

	`IPsecall`
	`IPsec ifnum`
	`OpenVPNall`
	`OpenVPN ifnum`
		Zugriff vom Gerät auf die VPN-Tunnelpartner, die über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung (`ifnum`) zu erreichen sind.

`SinemaRC`	`vlan (1-x)`	Zugriff vom SINEMA RC-Server auf das IP-Subnetz.
	`ppp 2`	Zugriff vom SINEMA RC-Server auf die WAN-Schnittstelle des Geräts.
	`Device`	Zugriff vom SINEMA RC-Server auf das Gerät.

von	nach	Bedeutung

	`IPsecall`
	`IPsec ifnum`
	`OpenVPNall`
	`OpenVPN ifnum`
		Zugriff vom SINEMA RC-Server auf die VPN-Tunnelpartner, die über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung (`ifnum`) zu erreichen sind.

`IPsecall`
`IPsec ifnum`
`OpenVPNall`
`OpenVPN ifnum`
	`vlan (1-x)`	Zugriff über VPN-Tunnelpartner auf das IP-Subnetz.

	`ppp 2`	Zugriff über VPN-Tunnelpartner auf die WAN-Schnittstelle des Geräts.
	`Device`	Zugriff über VPN-Tunnelpartner auf das Gerät.
	`SinemaRC`	Zugriff über VPN-Tunnelpartner auf den SINEMA RC-Server.
`ppp 2`	`vlan (1-x)`	Zugriff von der WAN-Schnittstelle auf das IP-Subnetz.
	`Device`	Zugriff von der WAN-Schnittstelle auf das Gerät.
	`SinemaRC`	Zugriff von der WAN-Schnittstelle auf den SINEMA RC-Server.

	`IPsecall`
	`IPsec ifnum`
	`OpenVPNall`
	`OpenVPN ifnum`
		Zugriff von der WAN-Schnittstelle auf die VPN-Tunnelpartner, die über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung (`ifnum`) zu erreichen sind.

11.3.4.2 di-input set address

Beschreibung

Mit diesem Befehl konfigurieren Sie die IP-Adresse oder einen IP-Bereich, die die IP-Pakete senden darf.

Voraussetzung

- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
di-input idx 1 set address <ipaddr>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`idx`	Nummer des digitalen Eingangs	1
`address`	Schlüsselwort für die Quelle.	-
`ipaddr`	Adresse, die IP-Pakete senden darf.	• Einzelne IP-Adresse: Geben Sie die IP-Adresse an. • IP-Bereich: Geben Sie den Bereich mit Startadresse "-" Endadresse an, z. B. 192.168.100.10 - 192.168.100.20 • Alle IP-Adressen: Geben Sie " 0.0.0.0/0" an.

Ergebnis

Die IP-Adresse oder der IP-Bereich ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `di-input show-idx` an.

11.3.4.3 di-input set ruleset

Beschreibung

Mit diesem Befehl legen Sie fest, welcher Regelsatz durch Ansteuern des digitalen Eingangs ausgeführt wird.

Voraussetzung

- Beim Ereignis "Firewall" ist digitaler Eingang konfiguriert.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
di-input idx 1 set ruleset {idx <integer> | name <string>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`idx`	Nummer des digitalen Eingangs	1
`ruleset`	Gibt an, welcher Regelsatz verwendet wird.	-
`idx`	Nummer, die einem bestimmten Regelsatz entspricht.	Geben Sie die gewünschte Nummer an. 1 ... 8
`name`	Namen des Regelsatzes	Geben Sie den gewünschten Namen an.

Ergebnis

Der Regelsatz ist dem digitalen Eingang zugeordnet.

Weitere Hinweise

Sie zeigen diese Zuordnung mit dem Befehl `di-input show-idx` an.

Sie konfigurieren einen Regelsatz mit dem Befehl `ruleset name`.

Sie listen die verfügbaren Regelsätze mit dem Befehl `ruleset show-idx` auf.

Sie konfigurieren die IP-Adresse, die IP-Pakete senden darf, mit dem Befehl `di-input set address`.

Sie konfigurieren das Ereignis mit dem Befehl `event config`.

11.3.4.4 di-input show-idx

Beschreibung

Mit diesem Befehl sehen Sie, ob dem digitalen Eingang ein Regelsatz zugeordnet ist.

Voraussetzung

- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
di-input show-idx
```

Ergebnis

Die Zuordung wird angezeigt.

Weitere Hinweise

Sie konfigurieren die Zuordnung zum Regelsatz mit dem Befehl `di-input set ruleset`.

11.3.4.5 icmp name

Beschreibung

Mit diesem Befehl erstellen Sie einen ICMP-Dienst. Zudem können Sie den ICMP-Pakettyp und den Code eines bereits angelegten ICMP-Diensts ändern.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
icmp name <string(32)> type <num(0-256)> code <num(0-256)> ver ipv4
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`string`	ICMP-Dienstname	Geben Sie einen eindeutigen ICMP-Dienstnamen an. Maximal 32 Zeichen
`type`	Schlüsselwort für den ICMP-Pakettyp	-
`num`	Nummer, die einem bestimmten ICMP-Pakettyp entspricht.	Geben Sie die gewünschte Nummer an. Default: 256 = any
`code`	Schlüsselwort für den Code des ICMP-Pakettyps	-
`num`	Nummer, die einem bestimmten Code entspricht.	Geben Sie die gewünschte Nummer an. Default: 256
`ver`	Schlüsselwort für die Version des ICMP-Protokolls	-
`ipv4`	IP Version4	-

Ergebnis

Der ICMP-Dienst ist konfiguriert.

Weitere Hinweise

Sie ändern Sie die Konfiguration mit dem Befehl icmp name set type.

Sie zeigen die verfügbaren Dienstnamen mit dem Befehl `icmp show-names` an.

Sie zeigen die verfügbaren ICMP-Pakettypen und Codes mit dem Befehl `icmp show-types-codes` an.

Sie löschen diesen Dienst mit dem Befehl `no icmp`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall icmp-services ipv4` an.

11.3.4.6 no icmp

Beschreibung

Mit diesem Befehl löschen Sie alle ICMP-Dienste oder einen bestimmten ICMP-Dienst.

Voraussetzung

- Der entsprechende ICMP-Dienst ist angelegt und wird nirgendwo verwendet.
- Sie befinden sich im Firewall Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no icmp {name <string(255)> | all}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`name`	Schlüsselwort für ICMP-Dienstname	-
`string`	ICMP-Dienstname	Geben Sie einen gültigen Dienstnamen an. Maximal 255 Zeichen
`all`	Löscht alle ICMP-Dienstnamen	-

Ergebnis

Der entsprechende ICMP-Dienst ist gelöscht.

Weitere Hinweise

Sie legen den ICMP-Dienst mit dem Befehl `icmp name` an.

Sie zeigen die verfügbaren Dienstnamen mit dem Befehl `icmp show-names` an.

Sie zeigen die verfügbaren ICMP-Pakettypen und Codes mit dem Befehl `icmp show-types-codes` an.

11.3.4.7 icmp name set type

Beschreibung

Mit diesem Befehl ändern Sie den ICMP-Pakettyp und den Code eines bereits angelegten ICMP-Diensts.

Voraussetzung

- Der entsprechende ICMP-Dienst ist angelegt.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
icmp name <string(32)> set type <num(0-256)> code <num(0-256)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`string`	ICMP-Dienstname	Geben Sie einen gültigen Dienstnamen an. Maximal 32 Zeichen
`type`	Schlüsselwort für den ICMP-Pakettyp	-
`integer`	Nummer, die einem bestimmten ICMP-Pakettyp entspricht.	Geben Sie die gewünschte Nummer an.
`code`	Schlüsselwort für den Code des ICMP-Pakettyps	-
`integer`	Nummer, die einem bestimmten Code entspricht.	Geben Sie die gewünschte Nummer an. Die Auswahl ist abhängig vom ICMP-Pakettyp.

Ergebnis

Der ICMP-Pakettyp und Code ist geändert.

Weitere Hinweise

Sie erstellen einen ICMP-Dienst mit dem Befehl icmp name `type`.

Sie zeigen die verfügbaren Dienstnamen mit dem Befehl `icmp show-names` an.

Sie zeigen die verfügbaren ICMP-Pakettypen und Codes mit dem Befehl `icmp show-types-codes` an.

Sie löschen diesen Dienst mit dem Befehl `no icmp`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall icmp-services ipv4` an.

11.3.4.8 icmp show-names

Beschreibung

Mit diesem Befehl zeigen Sie die verfügbaren ICMP-Dienstnamen an.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
icmp show-names
```

Ergebnis

Die Liste wird angezeigt.

Weitere Hinweise

Sie legen ein Protokoll mit dem Befehl `icmp name` an.

11.3.4.9 icmp show-types-codes

Beschreibung

Mit diesem Befehl zeigen Sie die verfügbaren ICMP-Pakettypen und Codes an.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
icmp show-types-codes
```

Ergebnis

Die Liste wird angezeigt.

Weitere Hinweise

Sie legen ein Protokoll mit dem Befehl `icmp name` an.

11.3.4.10 idle timeout icmp

Beschreibung

Mit diesem Befehl konfigurieren Sie die gewünschte Zeitspanne für ICMP. Wenn kein Datenaustausch stattfindet, wird nach Ablauf dieser Zeitspanne die ICMP-Verbindung automatisch getrennt.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
idle timeout icmp <second(1-21474836)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`second`	Intervall in Sekunden	1 ... 21474836

Ergebnis

Das Intervall ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall information` an.

11.3.4.11 idle timeout tcp

Beschreibung

Mit diesem Befehl konfigurieren Sie die gewünschte Zeitspanne für TCP. Wenn kein Datenaustausch stattfindet, wird nach Ablauf dieser Zeitspanne die TCP-Verbindung automatisch getrennt.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
idle timeout tcp <second(1-21474836)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`second`	Intervall in Sekunden	1 ... 21474836

Ergebnis

Das Intervall ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall information` an.

11.3.4.12 idle timeout udp

Beschreibung

Mit diesem Befehl konfigurieren Sie die gewünschte Zeitspanne für UDP. Wenn kein Datenaustausch stattfindet, wird nach Ablauf dieser Zeitspanne die UDP-Verbindung automatisch getrennt.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
idle timeout udp <second(1-21474836)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
second	Intervall in Sekunden	1 ... 21474836

Ergebnis

Das Intervall ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall information` an.

11.3.4.13 ipv4rule

Beschreibung

Mit diesem Befehl erstellen Sie eigene IPv4-Regeln für die Firewall. Diese IPv4-Firewallregeln haben eine höhere Priorität als die vordefinierten IPv4-Firewallregeln.

Voraussetzung

- Der Dienstname oder Protokollname ist angelegt.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ipv4rule from <iftype|OpenVPN|OpenVPNall|IPsec|IPsecall|SinemaRC|Device> [<ifnum(0-
4094)>] to <iftype|OpenVPN|OpenVPNall|IPsec|IPsecall|SinemaRC|Device> [<ifnum(0-
4094)>] srcip <ip|subnet|range> dstip <ip|subnet|range> action {drop|acc|rej}
[service <all|name(32)>] [log {no|info|war|cri}] [prior <number(0-127)>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`from`	Schlüsselwort für die eingehende Richtung (von)	-
`iftype`	Schnittstelle, die das IPv4-Paket sendet	Geben Sie eine gültige Schnittstelle an.

`OpenVPN`
`OpenVPNall`
`IPsec`
`IPsecall`
`SinemaRC`
	Zugriff über VPN-Tunnelpartner, die über SINEMA RC, über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung <integer> zu erreichen sind.	-

`Device`	Zugriff vom Gerät	-
`ifnum`	Nummer der Schnittstelle oder der VPN-Verbindung	0 ... 4094
`to`	Schlüsselwort für die ausgehende Richtung (nach)	
`iftype`	Schnittstelle, die das IPv4-Pakete empfängt	Geben Sie eine gültige Schnittstelle an vlan

`OpenVPN`
`OpenVPNall`
`IPsec`
`IPsecall`
`SinemaRC`
	Zugriff auf die VPN-Tunnelpartner, die über SINEMA RC, über alle VPN-Verbindungen (all) oder über eine bestimmte VPN-Verbindung <integer> zu erreichen sind.	-

`Device`	Zugriff auf das Gerät	-
`ifnum`	Nummer der Schnittstelle oder der VPN-Verbindung	0 ... 4094
`srcip`	Schlüsselwort für die Quelle	-
`ip`	IPv4-Adressse	Geben Sie die IP-Adresse an.
`subnet`	Subnetz	Geben Sie das Subnetz in der CIDR-Notation an. Alle IP-Adressen: Geben Sie " 0.0.0.0/0" an.
`range`	IPv4-Adressbereich	Geben Sie den IP-Adressbereich mit Startadresse "-" Endadresse an,z. B.. 192.168.100.10 - 192.168.100.20.
`dstip`	Schlüsselwort für das Ziel	-
`ip`	IPv4-Adressse	Geben Sie die IP-Adresse an.
`subnet`	Subnetz	Geben Sie das Subnetz in der CIDR-Notation an. Alle IP-Adressen: Geben Sie " 0.0.0.0/0" an.
`range`	IPv2-Adressbereich	Geben Sie den IP-Adressbereich mit Startadresse "-" Endadresse an, z. B.. 192.168.100.10 - 192.168.100.20.
`action`	Schlüsselwort für das Verfahren der eintreffenden IPv4-Pakete	-
`acc`	Die Datenpakete dürfen passieren.	-

Parameter	Beschreibung	Wertebereich / Anmerkung
drop	Die Datenpakete werden ohne Rückmeldung an den Absender verworfen.	-
rej	Die Datenpakete werden abgewiesen, der Absender erhält eine entsprechende Meldung.	-
service	Schlüsselwort für Dienst- oder Protokollname	-
all	Alle Dienst- oder Protokollnamen, für die diese Regel gültig ist.	-
name	Dienst- oder Protokollname, für den diese Regel gültig ist.	Geben Sie einen gültigen Namen an. Maximal 32 Zeichen
log	Schlüsselwort für das Eintragen in das Firewall-Logbuch	-
no	Das Zutreffen wird nicht protokolliert.	-
info	Meldungen ab der Ereignisschwere "information" werden protokolliert.	-
war	Meldungen ab der Ereignisschwere "warning" werden protokolliert.	-
cri	Meldungen ab der Ereignisschwere "critical" werden protokolliert.	-
prior	Schlüsselwort für die Priorität	-
number	Priorität	Geben Sie die Priorität für die IPv4-Regel an. 0 ... 127

Zur Bezeichnung von Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL-Konfigurationsmodus (Seite 469)".

Ergebnis

Die IPv4-Regel ist erstellt. Beim Erstellen erhält die IPv4-Regel automatisch eine eindeutige Nummer (Index).

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall ip-rules ipv4` an.

Sie erstellen einen Dienst mit folgenden Befehlen: `icmp name`, `service name`.

Sie erstellen ein Protokoll mit dem Befehl `proto name`.

Sie ändern die Einstellungen mit den Befehlen `ipv4rule set...`.

11.3.4.14 ipv4rule del ruleset

Beschreibung

Mit diesem Befehl entfernen Sie die Zuordnung des Regelsatzes.

Voraussetzung

- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ipv4rule idx <number(1-128)> del ruleset {idx <number(1-5)> | name <string>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`idx`	Schlüsselwort für Index	-
`number`	Nummer, die einer bestimmten IPv4-Regel entspricht.	Geben Sie die gewünschte Nummer an. 1 ... 128
`ruleset`	Gibt an, welcher Regelsatz verwendet wird.	-
`idx`	Nummer, die einem bestimmten Regelsatz entspricht.	Geben Sie die gewünschte Nummer an. 1 ... 5
`name`	Namen des Regelsatzes	Geben Sie den gewünschten Namen an.

Ergebnis

Die Zuordnung ist entfernt.

Weitere Hinweise

Sie zeigen die Zuordnung und weitere Informationen mit dem Befehl `show firewall ruleset assignment` an.

Sie konfigurieren die Zuordnung des Regelsatzes mit dem Befehl `ipv4rule set ruleset`.

11.3.4.15 no ipv4 rule

Beschreibung

Mit diesem Befehl löschen Sie alle IPv4-Firewallregeln oder eine bestimmte IPv4-Firewallregel.

Voraussetzung

- Die entsprechende IPv4-Firewallregel ist angelegt und wird nirgends verwendet.
- Sie befinden sich im Firewall FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no ipv4rule {all | idx <integer(1-128)>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`all`	Löscht alle IPv4-Regeln	-
`idx`	Schlüsselwort für Index	-
`integer`	Nummer, die einer bestimmten IPv4-Regel entspricht.	Geben Sie die gewünschte Nummer an. 1 ... 128

Ergebnis

Die entsprechende IPv4-Firewallregel ist gelöscht.

Weitere Hinweise

Sie legen die IPv4-Firewallregel mit dem Befehl `ipv4rule` an.

Sie erhalten die Nummern mit dem Befehl `ipv4rule show-rules`.

11.3.4.16 ipv4rule set action

Beschreibung

Mit diesem Befehl ändern Sie das Verfahren der eintreffenden IPv4-Pakete.

Voraussetzung

- Die IPv4-Firewallregel ist angelegt.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ipv4rule idx <number(1-128)> set action {drop|acc|rej}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`idx`	Schlüsselwort für Index	-
`number`	Nummer, die einer bestimmten IPv4-Regel entspricht.	Geben Sie die gewünschte Nummer an. 1 ... 128
`action`	Schlüsselwort für das Verfahren der eintreffenden IPv4-Pakete	-
`acc`	Die Datenpakete dürfen passieren.	-
`drop`	Die Datenpakete werden ohne Rückmeldung an den Absender verworfen.	-
`rej`	Die Datenpakete werden abgewiesen, der Absender erhält eine entsprechende Meldung.	-

Ergebnis

Das Verfahren der entsprechenden IPv4-Firewallregel ist geändert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall ip-rules ipv4` an.

Sie erhalten die Nummern mit dem Befehl `ipv4rule show-rules`.

11.3.4.17 ipv4rule set dstip

Beschreibung

Mit diesem Befehl ändern Sie das Ziel.

Voraussetzung

- Die IPv4-Firewallregel ist angelegt.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ipv4rule idx <number(1-128)> set dstip <ip_addr>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`idx`	Schlüsselwort für Index	-
`number`	Nummer, die einer bestimmten IPv4-Regel entspricht.	Geben Sie die gewünschte Nummer an. 1 ... 128
`dstip`	Schlüsselwort für das Ziel	-
`ip_addr`	Adresse, die IPv4-Pakete empfängt.	• Einzelne IP-Adresse: Geben Sie die IP-Adresse an, • IP-Bereich: Geben Sie den Bereich mit Startadresse "-" Endadresse an, z. B. 192.168.100.10 - 192.168.100.20. • Alle IP-Adressen: Geben Sie " 0.0.0.0/0" an.

Ergebnis

Das Ziel der entsprechenden IPv4-Firewallregel ist geändert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall ip-rules ipv4` an.

Sie erhalten die Nummern mit dem Befehl `ipv4rule show-rules`.

11.3.4.18 ipv4rule set from

Beschreibung

Mit diesem Befehl ändern Sie die ausgehende Richtung.

Voraussetzung

- Die IPv4-Firewallregel ist angelegt.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ipv4rule idx <number(1-128)> set from <ifname(50)> [<ifnum(0-4094)>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`idx`	Schlüsselwort für Index	-
`number`	Nummer, die einer bestimmten IPv4-Regel entspricht.	Geben Sie die gewünschte Nummer an. 1 ... 128
`from`	Schlüsselwort für die ausgehende Richtung (von)	-
`ifname`	Schnittstelle, die das IPv4-Paket sendet	Geben Sie eine gültige Schnittstelle an. Maximal 50 Zeichen
`ifnum`	Nummer der Schnittstelle	0 ... 4094

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL-Konfigurationsmodus (Seite 469)".

Ergebnis

Die ausgehende Richtung der entsprechenden IPv4-Firewallregel ist geändert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall ip-rules ipv4` an.

Sie erhalten die Nummern mit dem Befehl `ipv4rule show-rules`.

11.3.4.19 ipv4rule set log

Beschreibung

Mit diesem Befehl ändern Sie das Eintragen in das Firewall-Logbuch.

Voraussetzung

- Die IPv4-Firewallregel ist angelegt.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ipv4rule idx <number(1-128)> set log {no|info|war|cri}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`idx`	Schlüsselwort für Index	-
`number`	Nummer, die einer bestimmten IPv4-Regel entspricht.	Geben Sie die gewünschte Nummer an. 1 ... 128
`log`	Schlüsselwort für das Eintragen in das Firewall-Logbuch	-
`no`	Das Zutreffen wird nicht protokolliert.	-
`info`	Meldungen ab der Ereignisschwere "`information`" werden protokolliert.	-
`war`	Meldungen ab der Ereignisschwere "`warning`" werden protokolliert.	-
`cri`	Meldungen ab der Ereignisschwere "`critical`" werden protokolliert.	-

Ergebnis

Das Eintragen in das Firewall-Logbuch ist geändert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall ip-rules ipv4` an.

Sie erhalten die Nummern mit dem Befehl `ipv4rule show-rules`.

11.3.4.20 ipv4rule set prior

Beschreibung

Mit diesem Befehl ändern Sie die Priorität der IPv4-Firewallregel.

Voraussetzung

- Die IPv4-Firewallregel ist angelegt.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ipv4rule idx <number(1-128)> set prior <number(0-127)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`idx`	Schlüsselwort für Index	-
`number`	Nummer, die einer bestimmten IPv4-Regel entspricht.	Geben Sie die gewünschte Nummer an. 1 ... 128
`prior`	Schlüsselwort für die Priorität	-
`number`	Priorität	Geben Sie die Priorität für die IPv4-Regel an. 0 ... 127

Ergebnis

Die Priorität der entsprechenden IPv4-Firewallregel ist geändert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall ip-rules ipv4` an.

Sie erhalten die Nummern mit dem Befehl `ipv4rule show-rules`.

11.3.4.21 ipv4rule set ruleset

Beschreibung

Mit diesem Befehl ordnen Sie der IPv4-Firewallregel einen Regelsatz zu. Durch den Regelsatz können Sie mehrere IPv4-Firewallregeln zusammenfassen.

Voraussetzung

- Die IPv4-Firewallregel und Regelsatz ist angelegt.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ipv4rule idx <number(1-128)> set ruleset {idx <number(1-8)> | name <string>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`idx`	Schlüsselwort für Index	-
`number`	Nummer, die einer bestimmten IPv4-Regel entspricht.	Geben Sie die gewünschte Nummer an. 1 ... 128
`ruleset`	Gibt an, welcher Regelsatz verwendet wird.	-
`idx`	Nummer, die einem bestimmten Regelsatz entspricht.	Geben Sie die gewünschte Nummer an. 1 ... 8
`name`	Namen des Regelsatzes	Geben Sie den gewünschten Namen an.

Ergebnis

Die IPv4-Firewallregel ist einem Regelsatz zugeordnet.

Weitere Hinweise

Sie zeigen diese Zuordnung und weitere Informationen mit dem Befehl `show firewall ruleset assignment` an.

Sie konfigurieren einen Regelsatz mit dem Befehl `ruleset name`.

Sie listen die verfügbaren IPv4-Firewallregeln mit dem Befehl `ipv4rule show-rules` auf.

Sie listen die verfügbaren Regelsätze mit dem Befehl `ruleset show-idx` auf.

Sie entfernen die Zuordnung des Regelsatzes mit dem Befehl `ipv4rule del ruleset`.

11.3.4.22 ipv4rule set service

Beschreibung

Mit diesem Befehl ändern Sie den Dienst- oder Protokollnamen.

Voraussetzung

- Die IPv4-Firewallregel ist angelegt.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ipv4rule idx <number(1-128)> set service <name(32)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`idx`	Schlüsselwort für Index	-
`number`	Nummer, die einer bestimmten IPv4-Regel entspricht.	Geben Sie die gewünschte Nummer an. 1 ... 128
`service`	Schlüsselwort für Dienst- oder Protokoll-name	-
`name`	Dienst- oder Protokollname, für den diese Regel gültig ist.	Geben Sie einen gültigen Namen an. Maximal 32 Zeichen

Ergebnis

Der Dienst- oder Protokollnamen der entsprechenden IPv4-Firewallregel ist geändert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall ip-rules ipv4` an.

Sie erhalten die Nummern mit dem Befehl `ipv4rule show-rules`.

11.3.4.23 ipv4rule set srcip

Beschreibung

Mit diesem Befehl ändern Sie die Quelle.

Voraussetzung

- Die IPv4-Firewallregel ist angelegt.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ipv4rule idx <number(1-128)> set srcip <ip_addr>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`idx`	Schlüsselwort für Index	-
`number`	Nummer, die einer bestimmten IPv4-Regel entspricht.	Geben Sie die gewünschte Nummer an. 1 ... 128
`srcip`	Schlüsselwort für die Quelle	
`ip_addr`	Adresse, die IPv4-Pakete sendet.	• Einzelne IP-Adresse: Geben Sie die IP-Adresse an, • IP-Bereich: Geben Sie den Bereich mit Startadresse "-" Endadresse an, z. B. 192.168.100.10 - 192.168.100.20. • Alle IP-Adressen: Geben Sie " 0.0.0.0/0" an.

Ergebnis

Die Quelle der entsprechenden IPv4-Firewallregel ist geändert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall ip-rules ipv4` an.

Sie erhalten die Nummern mit dem Befehl `ipv4rule show-rules`.

11.3.4.24 ipv4rule set to

Beschreibung

Mit diesem Befehl ändern Sie die eingehende Richtung (nach).

Voraussetzung

- Die IPv4-Firewallregel ist angelegt.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ipv4rule idx <number(1-128)> set to <ifname(50)> [<ifnum(0-4094)>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`idx`	Schlüsselwort für Index	-
`number`	Nummer, die einer bestimmten IPv4-Regel entspricht.	Geben Sie die gewünschte Nummer an. 1 ... 64
`to`	Schlüsselwort für die eingehende Richtung (nach)	-
`ifname`	Schnittstelle, die das IPv4-Paket empfängt	Geben Sie eine gültige Schnittstelle an. Maximal 50 Zeichen
`ifnum`	Nummer der Schnittstelle	0 ... 4094

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL-Konfigurationsmodus (Seite 469)".

Ergebnis

Die eingehende Richtung der entsprechenden IPv4-Firewallregel ist geändert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall ip-rules ipv4` an.

Sie erhalten die Nummern mit dem Befehl `ipv4rule show-rules`.

11.3.4.25 ipv4rule ipsec connection

Beschreibung

Mit diesem Befehl listen Sie die Firewallregeln für die IPsec-Verbindungen auf.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
ipv4rule ipsec connection show-idx
```

Ergebnis

Die IPv4-Firewallregeln werden aufgelistet.

Weitere Hinweise

Sie legen die IPv4-Firewallregel mit dem Befehl `ipv4rule` an.

11.3.4.26 ipv4rule show interfaces

Beschreibung

Mit diesem Befehl listen Sie die verfügbaren Quell- und Ziel-Schnittstellen auf.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ipv4rule show {from|to} interfaces
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`from`	Listet die Quell-Schnittstellen auf.	-
`to`	Listet die Ziel-Schnittstellen auf.	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL-Konfigurationsmodus (Seite 469)".

Ergebnis

Die Schnittstellen werden aufgelistet.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall pre-rules ipv4` an.

Sie listen die verfügbaren Schnittstellen mit dem Befehl `prerule ipv4 show-int` auf.

11.3.4.27 ipv4rule show-rules

Beschreibung

Mit diesem Befehl zeigen Sie die verfügbaren IPv4-Firewallregeln an.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
ipv4rule show-rules
```

Ergebnis

Die IPv4-Firewallregeln werden aufgelistet.

Weitere Hinweise

Sie zeigen weitere Informationen mit dem Befehl `show firewall ip-rules ipv4` an.

Sie legen die IPv4-Firewallregel mit dem Befehl `ipv4rule` an.

11.3.4.28 prerule all ipv4

Beschreibung

Mit diesem Befehl aktivieren Sie an der gewählten Schnittstelle alle vordefinierte Firewallregeln.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
prerule all ipv4 {int <interface-type> <num(0-4094)> | all-int} {enabled|disabled}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`int`	Schlüsselwort für Schnittstelle	-
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`num`	Schnittstellenindex	Geben Sie einen gültigen Schnittstellenindex an. 0 ... 4094
`all-int`	Aktiviert alle vordefinierten Firewallregeln an allen Schnittstellen.	-
`enabled`	Aktiviert die vordefinierten Firewallregeln.	-
`disabled`	Deaktiviert die vordefinierten Firewallregeln.	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL-Konfigurationsmodus (Seite 469)".

Ergebnis

An der entsprechenden Schnittstelle sind alle vordefinierten Firewallregeln aktiviert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall pre-rules ipv4` an.

Sie listen die verfügbaren Schnittstellen mit dem Befehl `prerule ipv4 show-int` auf.

11.3.4.29 prerule cloudconnector ipv4

Beschreibung

Mit diesem Befehl aktivieren Sie an der gewählten Schnittstelle die vordefinierte Firewallregel Cloud Connector.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
prerule cloudconnector  ipv4 {int <interface-type> <num(0-4094)> | all-int}
{enabled|disabled}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`int`	Schlüsselwort für Schnittstelle	-
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`num`	Schnittstellenindex	Geben Sie einen gültigen Schnittstellenindex an. 0 ... 4094
`all-int`	Aktiviert die vordefinierte Firewallregel an allen Schnittstellen.	-
`enabled`	Aktiviert die vordefinierte Firewallregel.	-
`disabled`	Deaktiviert die vordefinierte Firewallregel.	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL-Konfigurationsmodus (Seite 469)".

Ergebnis

An der entsprechenden Schnittstelle ist die vordefinierte Firewallregel Cloud Connector aktiviert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall pre-rules ipv4` an.

Sie listen die verfügbaren Schnittstellen mit dem Befehl `prerule ipv4 show-int` auf.

11.3.4.30 prerule dhcp ipv4

Beschreibung

Mit diesem Befehl aktivieren Sie an der gewählten Schnittstelle die vordefinierte Firewallregel DHCP.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
prerule dhcp ipv4 {int <interface-type> <num(0-4094)> | all-int} {enabled|disabled}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`int`	Schlüsselwort für Schnittstelle	-
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`num`	Schnittstellenindex	Geben Sie einen gültigen Schnittstellenindex an. 0 ... 4094
`all-int`	Aktiviert die vordefinierte Firewallregel an allen Schnittstellen.	-
`enabled`	Aktiviert die vordefinierte Firewallregel.	-
`disabled`	Deaktiviert die vordefinierte Firewallregel.	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL-Konfigurationsmodus (Seite 469)".

Ergebnis

An der entsprechenden Schnittstelle ist die vordefinierte Firewallregel DHCP aktiviert. Über die Schnittstelle kann auf den DHCP-Server oder den DHCP-Client zugriffen werden.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall pre-rules ipv4` an.

Sie listen die verfügbaren Schnittstellen mit dem Befehl `prerule ipv4 show-int` auf.

11.3.4.31 prerule dns ipv4

Beschreibung

Mit diesem Befehl aktivieren Sie an der gewählten Schnittstelle die vordefinierte Firewallregel DNS.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
prerule dns ipv4 {int <interface-type> <num(0-4094)> | all-int} {enabled|disabled}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`int`	Schlüsselwort für Schnittstelle	-
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`num`	Schnittstellenindex	Geben Sie einen gültigen Schnittstellenindex an. 0 ... 4094
`all-int`	Aktiviert die vordefinierte Firewallregel an allen Schnittstellen.	-
`enabled`	Aktiviert die vordefinierte Firewallregel.	-
`disabled`	Deaktiviert die vordefinierte Firewallregel.	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL-Konfigurationsmodus (Seite 469)".

Ergebnis

An der entsprechenden Schnittstelle ist die vordefinierte Firewallregel DNS aktiviert. Über die Schnittstelle sind DNS-Anfragen an das Gerät möglich.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall prerules ipv4` an.

Sie listen die verfügbaren Schnittstellen mit dem Befehl `prerule ipv4 show-int` auf.

11.3.4.32 prerule http ipv4

Beschreibung

Mit diesem Befehl aktivieren Sie an der gewählten Schnittstelle die vordefinierte Firewallregel HTTP.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
prerule http ipv4 {int <interface-type> <num(0-4094)> | all-int} {enabled|disabled}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`int`	Schlüsselwort für Schnittstelle	-
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`num`	Schnittstellenindex	Geben Sie einen gültigen Schnittstellenindex an. 0 ... 4094
`all-int`	Aktiviert die vordefinierte Firewallregel an allen Schnittstellen.	-
`enabled`	Aktiviert die vordefinierte Firewallregel.	-
`disabled`	Deaktiviert die vordefinierte Firewallregel.	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL-Konfigurationsmodus (Seite 469)".

Ergebnis

An der entsprechenden Schnittstelle ist die vordefinierte Firewallregel HTTP aktiviert. Über HTTP kann auf das WBM zugriffen werden.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall pre-rules ipv4` an.

Sie listen die verfügbaren Schnittstellen mit dem Befehl `prerule ipv4 show-int` auf.

11.3.4.33 prerule https ipv4

Beschreibung

Mit diesem Befehl aktivieren Sie an der gewählten Schnittstelle die vordefinierte Firewallregel für HTTPS.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
prerule https ipv4 {int <interface-type> <num(0-4094)> | all-int} {enabled|disabled}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`int`	Schlüsselwort für Schnittstelle	-
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`num`	Schnittstellenindex	Geben Sie einen gültigen Schnittstellenindex an. 0 ... 4049
`all-int`	Aktiviert die vordefinierte Firewallregel an allen Schnittstellen.	-
`enabled`	Aktiviert die vordefinierte Firewallregel.	-
`disabled`	Deaktiviert die vordefinierte Firewallregel.	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL-Konfigurationsmodus (Seite 469)".

Ergebnis

An der entsprechenden Schnittstelle ist die vordefiniert Firewallregel HTTPS aktiviert. Über HTTPS kann auf das WBM zugriffen werden.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall prerules ipv4` an.

Sie listen die verfügbaren Schnittstellen mit dem Befehl `prerule ipv4 show-int` auf.

11.3.4.34 prerule ipsec ipv4

Beschreibung

Mit diesem Befehl aktivieren Sie an der gewählten Schnittstelle die vordefinierte Firewallregel IPsec.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
prerule ipsec ipv4 {int <interface-type> <num(0-4094)> | all-int} {enabled|disabled}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`int`	Schlüsselwort für Schnittstelle	-
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`num`	Schnittstellenindex	Geben Sie einen gültigen Schnittstellenindex an. 0 ... 4094
`all-int`	Aktiviert die vordefinierte Firewallregel an allen Schnittstellen.	-
`enabled`	Aktiviert die vordefinierte Firewallregel.	-
`disabled`	Deaktiviert die vordefinierte Firewallregel.	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL-Konfigurationsmodus (Seite 469)".

Ergebnis

An der entsprechenden Schnittstelle ist die vordefiniert Firewallregel IPsec aktiviert. Der IKE (Internet Key Exchange) Datenverkehr vom externen Netz zum Gerät ist erlaubt.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall pre-rules ipv4` an.

Sie listen die verfügbaren Schnittstellen mit dem Befehl `prerule ipv4 show-int` auf.

11.3.4.35 prerule ipv4 show-int

Beschreibung

Mit diesem Befehl listen Sie die verfügbaren Schnittstellen auf.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
prerule ipv4 show-int
```

Ergebnis

Die Schnittstellen werden aufgelistet.

11.3.4.36 prerule ping ipv4

Beschreibung

Mit diesem Befehl aktivieren Sie an der gewählten Schnittstelle die vordefinierte Firewallregel Ping.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
prerule ping ipv4 {int <interface-type> <num(0-4094)> | all-int} {enabled|disabled}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`int`	Schlüsselwort für Schnittstelle	-
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`num`	Schnittstellenindex	Geben Sie einen gültigen Schnittstellenindex an. 0 ... 4094
`all-int`	Aktiviert die vordefinierte Firewallregel an allen Schnittstellen.	-
`enabled`	Aktiviert die vordefinierte Firewallregel.	-
`disabled`	Deaktiviert die vordefinierte Firewallregel.	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL-Konfigurationsmodus (Seite 469)".

Ergebnis

An der entsprechenden Schnittstelle ist die vordefinierte Firewallregel Ping aktiviert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall pre-rules ipv4` an.

Sie listen die verfügbaren Schnittstellen mit dem Befehl `prerule ipv4 show-int` auf.

11.3.4.37 prerule snmp ipv4

Beschreibung

Mit diesem Befehl aktivieren Sie an der gewählten Schnittstelle die vordefinierte Firewallregel SNMP.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
prerule snmp ipv4 {int <interface-type> <num(0-4094)> | all-int} {enabled|disabled}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`int`	Schlüsselwort für Schnittstelle	-
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`num`	Schnittstellenindex	Geben Sie einen gültigen Schnittstellenindex an. 0 ... 4094
`all-int`	Aktiviert die vordefinierte Firewallregel an allen Schnittstellen.	-
`enabled`	Aktiviert die vordefinierte Firewallregel.	-
`disabled`	Deaktiviert die vordefinierte Firewallregel.	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL-Konfigurationsmodus (Seite 469)".

Ergebnis

An der entsprechenden Schnittstelle ist die vordefinierte Firewallregel SNMP aktiviert. Über die Schnittstelle sind eingehende SNMP-Verbindungen möglich.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall pre-rules ipv4` an.

Sie listen die verfügbaren Schnittstellen mit dem Befehl `prerule ipv4 show-int` auf.

11.3.4.38 prerule ssh ipv4

Beschreibung

Mit diesem Befehl aktivieren Sie an der gewählten Schnittstelle die vordefinierte Firewallregel SSH.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
prerule ssh ipv4 {int <interface-type> <num(0-4094)> | all-int} {enabled|disabled}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`int`	Schlüsselwort für Schnittstelle	-
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`num`	Schnittstellenindex	Geben Sie einen gültigen Schnittstellenindex an. 0 ... 4094
`all-int`	Aktiviert die vordefinierte Firewallregel an allen Schnittstellen.	-
`enabled`	Aktiviert die vordefinierte Firewallregel.	-
`disabled`	Deaktiviert die vordefinierte Firewallregel.	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL-Konfigurationsmodus (Seite 469)".

Ergebnis

An der entsprechenden Schnittstelle ist die vordefinierte Firewallregel SSH aktiviert. Auf das CLI kann verschlüsselt zugegriffen werden.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall pre-rules ipv4` an.

Sie listen die verfügbaren Schnittstellen mit dem Befehl `prerule ipv4 show-int` auf.

11.3.4.39 prerule systime ipv4

Beschreibung

Mit diesem Befehl aktivieren Sie an der gewählten Schnittstelle die vordefinierte Firewallregel Systemzeit.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
prerule systime ipv4 {int <interface-type> <num(0-4094)> | all-int}
{enabled|disabled}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`int`	Schlüsselwort für Schnittstelle	-
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`num`	Schnittstellenindex	Geben Sie einen gültigen Schnittstellenindex an. 0 ... 4094
`all-int`	Aktiviert die vordefinierte Firewallregel an allen Schnittstellen.	-
`enabled`	Aktiviert die vordefinierte Firewallregel.	-
`disabled`	Deaktiviert die vordefinierte Firewallregel.	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL-Konfigurationsmodus (Seite 469)".

Ergebnis

An der entsprechenden Schnittstelle ist die vordefinierte Firewallregel Systemzeit aktiviert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall pre-rules ipv4` an.

Sie listen die verfügbaren Schnittstellen mit dem Befehl `prerule ipv4 show-int` auf.

11.3.4.40 prerule telnet ipv4

Beschreibung

Mit diesem Befehl aktivieren Sie an der gewählten Schnittstelle die vordefinierte Firewallregel Telnet.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
prerule telnet ipv4 {int <interface-type> <num(0-4094)> | all-int} {enabled|disabled}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`int`	Schlüsselwort für Schnittstelle	-
`interface-type`	Typ bzw. Geschwindigkeit der Schnittstelle	Geben Sie eine gültige Schnittstelle an.
`num`	Schnittstellenindex	Geben Sie einen gültigen Schnittstellenindex an. 0 ... 4094
`all-int`	Aktiviert die vordefinierte Firewallregel an allen Schnittstellen.	-
`enabled`	Aktiviert die vordefinierte Firewallregel.	-
`disabled`	Deaktiviert die vordefinierte Firewallregel.	-

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Befehle im FIREWALL-Konfigurationsmodus (Seite 469)".

Ergebnis

An der entsprechenden Schnittstelle ist die vordefinierte Firewallregel Telnet aktiviert. Auf das CLI kann unverschlüsselt zugegriffen werden.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall pre-rules ipv4` an.

Sie listen die verfügbaren Schnittstellen mit dem Befehl `prerule ipv4 show-int` auf.

11.3.4.41 proto name

Beschreibung

Mit diesem Befehl konfigurieren Sie benutzerdefinierte Protokolle. Sie vergeben einen Protokollnamen und ordnen eine Protokollnummer zu.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
proto name <name(32)> num <number(1-255)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`name`	Protokollnamen	Geben Sie einen eindeutigen Protokollnamen an. Max. 32 Zeichen
`num`	Protokollnummer	1 ... 255 Default: 255 Geben Sie die Protokollnummer an, z. B. 2. Eine Liste der Protokollnummern finden Sie auf den Internetseiten von Internet Assigned Numbers Authority (IANA) (https://www.iana.org/).

Ergebnis

Das Protokoll ist konfiguriert. Wenn die optionalen Parameter nicht angegeben werden, wird ein Protokoll mit diesem Namen erstellt und der voreingestellte Wert verwendet. Den Parameter können Sie später anpassen.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall ip-protocols` an.

Sie löschen das Protokoll mit dem Befehl `no proto`.

11.3.4.42 no proto

Beschreibung

Mit diesem Befehl löschen Sie alle Protokolle oder ein bestimmtes Protokoll.

Voraussetzung

- Das entsprechende Protokoll ist angelegt und wird nirgendwo verwendet.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no proto {name <string(32)> | all}}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`name`	Schlüsselwort für Protokollname	-
`string`	Protokollname	Geben Sie einen gültigen Protokollnamen an. Maximal 32 Zeichen
`all`	Löscht alle Protokollnamen	-

Ergebnis

Das entsprechende Protokoll ist gelöscht.

Weitere Hinweise

Sie erstellen ein Protokoll mit dem Befehl `proto name`.

Sie zeigen die verfügbaren Protokollnamen mit dem Befehl `proto show-names` an.

11.3.4.43 proto show-names

Beschreibung

Mit diesem Befehl zeigen Sie die verfügbaren Protokollnamen an.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
proto show-names
```

Ergebnis

Die Protokollnamen werden aufgelistet.

Weitere Hinweise

Sie legen ein Protokoll mit dem Befehl `proto name` an.

11.3.4.44 ruleset idx

Beschreibung

Mit diesem Befehl können Sie die Konfiguation eines Regelsatzes ändern.

Voraussetzung

- Der Regelsatz ist angelegt.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ruleset idx <number(0-5)> [name <text(128)>] [comment <text(128)>] [timeout <5-480>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`idx`	Schlüsselwort für Index	-
`number`	Nummer, die einem bestimmten Regelsatz entspricht.	Geben Sie die gewünschte Nummer an. 0 ... 5
`name`	Schlüsselwort für Name	-
`text`	Name des Regelsatzes	Geben Sie den gewünschten Namen an. Maximal 128 Zeichen
`comment`	Schlüsselwort für Kommentar	-
`text`	Kommentar	Geben Sie eine Beschreibung für den Regelsatz ein. Maximal 128 Zeichen
`timeout`	Dauer des Zugriffs	Geben Sie die Dauer des Zugriffs an. 5 ... 480 Minuten

Ergebnis

Die Konfiguration ist geändert.

Weitere Hinweise

Sie zeigen diese Zuordnung und weitere Informationen mit dem Befehl `show firewall ruleset assignment` an.

Sie konfigurieren einen Regelsatz mit dem Befehl `ruleset name`.

11.3.4.45 ruleset name

Beschreibung

Mit diesem Befehl erstellen Sie einen Regelsatz.

Voraussetzung

- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ruleset name <text(128)> [timeout <5-480>] [comment <text(128)>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`name`	Namen des Regelsatzes	Geben Sie einen eindeutigen Namen an. Maximal 128 Zeichen
`comment`	Kommentar	Geben Sie eine Beschreibung für den Regelsatz ein. Maximal 128 Zeichen
`timeout`	Dauer des Zugriffs	Geben Sie die Dauer des Zugriffs an. 5 ... 480 Minuten

Ergebnis

Der Regelsatz ist erstellt.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall ip-rules ipv4` an.

Sie erhalten die Nummern mit dem Befehl `ipv4rule show-rules`.

11.3.4.46 ruleset show-idx

Beschreibung

Mit diesem Befehl listen Sie die verfügbaren Regelsätze auf.

Voraussetzung

- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
ruleset show-idx
```

Ergebnis

Die Regelsätze werden aufgelistet.

Weitere Hinweise

Sie konfigurieren einen Regelsatz mit dem Befehl `ruleset name`.

11.3.4.47 no ruleset

Beschreibung

Mit diesem Befehl deaktivieren Sie einen bestimmten Regelsatz oder alle bestehenden Regelsätze.

Voraussetzung

- Der entsprechende Regelsatz ist angelegt und wird nirgends verwendet.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no ruleset {show-idx | idx <number> | name <text(128)> | all}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`show-idx`	Listet die verfügbaren Regelsätze auf.	-
`idx`	Schlüsselwort für Index	-
`number`	Nummer des Regelsatzes	Geben Sie die Nummer des zu löschenden Regelsatzes an. 0 ... 5
`name`	Schlüsselwort für Name	-
`text`	Name des Regelsatzes	Geben Sie den Namen des zu löschenden Regelsatzes an. Maximal 128 Zeichen
`all`	Deaktiviert alle Regelsätze.	-

Ergebnis

Der betreffende Regelsatz ist gelöscht.

Weitere Hinweise

Sie konfigurieren einen Regelsatz mit dem Befehl `ruleset name`.

11.3.4.48 service name

Beschreibung

Mit diesem Befehl konfigurieren Sie einen Dienst. Sie vergeben einen Dienstnamen und ordnen die Dienstparameter zu.

Voraussetzung

Sie befinden sich im Firewall Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
service name <string(32)> proto {udp|tcp} src {all|port <number(0-65535)|range>} dst
{all|port <number(0-65535)|range>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`string`	Dienstname	Geben Sie einen eindeutigen Dienstnamen an. Maximal 32 Zeichen
`proto`	Schlüsselwort für ein Protokoll	-
`udp`	Der Dienst ist nur für UDP-Telegramme gültig.	-
`tcp`	Der Dienst ist nur für TCP-Telegramme gültig.	Default
`src`	Schlüsselwort für die Quelle	-
`all`	Gilt für alle Ports.	-
`port`	Schlüsselwort für einen Port	-
`number`	Portnummer	0 ... 65535 Geben Sie den gewünschten Port an.
`range`	Schlüsselwort für Portbereich	0 ... 65535 Geben Sie den Start-Port und End-Port an, z. B. `10 - 20`.
`dst`	Schlüsselwort für das Ziel	-
`all`	Gilt für alle Ports.	-
`port`	Schlüsselwort für einen Port	-
`number`	Portnummer	0 ... 65535 Geben Sie den gewünschten Port an.
`range`	Schlüsselwort für Portbereich	0 ... 65535 Geben Sie den Start-Port und End-Port an, z. B. `10 - 20`.

Ergebnis

Der Dienst ist konfiguriert.

Weitere Hinweise

Sie löschen diesen Dienst mit dem Befehl `no service`.

Sie zeigen den Dienst mit dem Befehl `show firewall ip-services` an.

11.3.4.49 no service

Beschreibung

Mit diesem Befehl löschen Sie alle Dienste oder einen bestimmten Dienst.

Voraussetzung

- Der entsprechende Dienst ist angelegt und wird nirgendwo verwendet.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no service {name <string(32)> | all}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`name`	Schlüsselwort für Dienstname	-
`string`	Dienstname	Geben Sie einen gültigen Dienstnamen an. Maximal 32 Zeichen
`all`	Löscht alle Dienstnamen	-

Ergebnis

Der entsprechende Dienst ist gelöscht.

Weitere Hinweise

Sie zeigen die verfügbaren Dienstnamen mit dem Befehl `service show-names` an

Sie erstellen einen Dienst mit dem Befehl `service name` an.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall ip-services` an.

11.3.4.50 service name set dst

Beschreibung

Mit diesem Befehl ändern Sie den Ziel-Port.

Voraussetzung

- Der Dienstname ist angelegt.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
service name <string(32)> set dst {all|port <number(0-65535)|range>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`string`	Dienstname	Geben Sie einen gültigen Dienstnamen an. Maximal 32 Zeichen
`all`	Für alle Ports gültig.	-
`port`	Schlüsselwort für einen Port	-
`number`	Neuer Ziel-Port	0 ... 65535 Geben Sie den gewünschten Port an.
`range`	Neuer Portbereich	0 ... 65535 Geben Sie den Start-Port und End-Port an, z. B. `10 - 20`.

Ergebnis

Der Ziel-Port des entsprechenden Diensts ist geändert.

Weitere Hinweise

Sie zeigen die verfügbaren Dienstnamen mit dem Befehl `service show-names` an

Sie legen den Dienst mit dem Befehl `service name` an.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall ip-services` an.

11.3.4.51 service name set prot

Beschreibung

Mit diesem Befehl ändern Sie das Protokoll.

Voraussetzung

- Der Dienstname ist angelegt.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
service name <string(32)> set proto {udp|tcp}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`string`	Dienstname	Geben Sie einen gültigen Dienstnamen an. Maximal 32 Zeichen
`udp`	Der Dienst ist nur für UDP-Telegramme gültig.	-
`tcp`	Der Dienst ist nur für TCP-Telegramme gültig.	-

Ergebnis

Das Protokoll des entsprechenden Diensts ist geändert.

Weitere Hinweise

Sie zeigen die verfügbaren Dienstnamen mit dem Befehl `service show-names` an

Sie legen den Dienst mit dem Befehl `service name` an.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall ip-services` an.

11.3.4.52 service name set src

Beschreibung

Mit diesem Befehl ändern Sie den Quell-Port.

Voraussetzung

- Der Dienstname ist angelegt.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
service name <string(32)> set src {all|port <number(0-65535)|range>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`string`	Dienstname	Geben Sie einen gültigen Dienstnamen an. Maximal 32 Zeichen
`all`	Gilt für alle Ports.	-
`port`	Schlüsselwort für einen Port	-
`number`	Portnummer	0 ... 65535 Geben Sie den gewünschten Port an.
`range`	Schlüsselwort für Portbereich	0 ... 65535 Geben Sie den Start-Port und End-Port an, z. B. `10 - 20`.

Ergebnis

Der Quell-Port des entsprechenden Diensts ist geändert.

Weitere Hinweise

Sie zeigen die verfügbaren Dienstnamen mit dem Befehl `service show-names` an

Sie legen den Dienst mit dem Befehl `service cr name` an.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show firewall ip-services` an.

11.3.4.53 service show-names

Beschreibung

Mit diesem Befehl zeigen Sie die verfügbaren Dienstnamen an.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
service show-names
```

Ergebnis

Die Dienstnamen werden aufgelistet.

Weitere Hinweise

Sie legen ein Protokoll mit dem Befehl `service cr name` an.

11.3.4.54 shutdown

Beschreibung

Mit diesem Befehl deaktivieren Sie die Firewall.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
shutdown
```

Ergebnis

Die Firewall ist deaktiviert

Weitere Hinweise

Sie aktivieren die Firewall mit dem Befehl `no shutdown`.

11.3.4.55 no shutdown

Beschreibung

Mit diesem Befehl aktivieren Sie die Firewall.

Voraussetzung

Sie befinden sich im FIREWALL-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-fw)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no shutdown
```

Ergebnis

Die Firewall ist aktiviert.

Weitere Hinweise

Sie deaktivieren die Firewall mit dem Befehl `shutdown`.

11.3.4.56 useraccount show-idx

Beschreibung

Mit diesem Befehl zeigen Sie die Nummern der konfigurierten Benutzer mit Remote-Zugriff an.

Voraussetzung

- Der Benutzer hat Remote-Zugriff.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
useraccount show-idx
```

Ergebnis

Die Benutzer werden aufgelistet.

Weitere Hinweise

Sie konfigurieren den Remote-Zugriff mit dem Befehl `user-account`.

11.3.4.57 useraccount ruleset

Beschreibung

Mit diesem Befehl ordnen Sie einem Benutzer einen Regelsatz zu.

Voraussetzung

- Der Benutzer hat Remote-Zugriff.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
useraccount {idx <integer> | name <string(128)>} ruleset {idx <integer> | name
<string>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`idx`	Schlüsselwort für Index	-
`integer`	Nummer, die einem bestimmten Benutzer entspricht.	Geben Sie die gewünschte Nummer an.
`name`	Schlüsselwort für Benutzernamen	-
`string`	Benutzernamen	Geben Sie den gewünschten Namen an.
`ruleset`	Gibt an, welcher Regelsatz verwendet wird.	-
`idx`	Nummer, die einem bestimmten Regelsatz entspricht.	Geben Sie die gewünschte Nummer an. 1 ... 8
`name`	Namen des Regelsatzes	Geben Sie den gewünschten Namen an.

Ergebnis

Dem Benutzer ist ein Regelsatz zugewiesen.

Weitere Hinweise

Sie konfigurieren den Remote-Zugriff mit dem Befehl `user-account`.

Sie konfigurieren einen Regelsatz mit dem Befehl `ruleset name`.

Sie listen die verfügbaren Benutzer mit Remote-Zugriff mit dem Befehl `useraccount show-idx` auf.

Sie listen die verfügbaren Regelsätze mit dem Befehl `ruleset show-idx` auf.

11.3.4.58 no useraccount ruleset

Beschreibung

Mit diesem Befehl löschen Sie für einen bestimmten Benutzer die ihm zugeordneten Regelsätze.

Voraussetzung

- Der entsprechende Regelsatz ist angelegt und wird nirgends verwendet.
- Sie befinden sich im FIREWALL-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-fw)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no useraccount {idx <number> | name <text(128)>} ruleset
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`idx`	Schlüsselwort für Index	-
`number`	Nummer, die einem bestimmten Benutzer entspricht.	Geben Sie die gewünschte Nummer an. 1 ... 64
`name`	Schlüsselwort für Benutzernamen	
`text`	Benutzernamen	Geben den gewünschten Namen an. Maximal 128 Zeichen

Ergebnis

Der Regelsatz für den gewählten Benutzer ist gelöscht.

Weitere Hinweise

Sie ordnen einem Benutzer einen Regelsatz mit dem Befehl `useraccount ruleset` zu.

11.4 IPsec VPN

In diesem Kapitel werden Befehle beschrieben, die für IPsec relevant sind.

11.4.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

11.4.1.1 show ipsec conn-authentication

Beschreibung

Dieser Befehl zeigt die Sicherheitseinstellungen der IPsec VPN-Verbindungen an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show ipsec conn-authentication
```

Ergebnis

Die Einstellungen werden angezeigt.

11.4.1.2 show ipsec connections

Beschreibung

Dieser Befehl zeigt die Konfiguration der IPsec VPN-Verbindungen an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show ipsec connections
```

Ergebnis

Die Konfigurationen werden angezeigt.

11.4.1.3 show ipsec conn-phase1

Beschreibung

Dieser Befehl zeigt die Konfiguration der Phase 1 der IPsec VPN-Verbindungen an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show ipsec conn-phase1
```

Ergebnis

Die Konfigurationen werden angezeigt.

11.4.1.4 show ipsec conn-phase2

Beschreibung

Dieser Befehl zeigt die Konfiguration der Phase 2 der IPsec VPN-Verbindungen an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show ipsec conn-phase2
```

Ergebnis

Die Konfigurationen werden angezeigt.

11.4.1.5 show ipsec information

Beschreibung

Der Befehl zeigt die Grundeinstellung von IPsec VPN an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show ipsec information
```

Ergebnis

Die Einstellungen werden angezeigt.

11.4.1.6 show ipsec remoteend

Beschreibung

Dieser Befehl zeigt die Konfiguration der Gegenstellen (VPN-Endpunkt) an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show ipsec remoteend
```

Ergebnis

Die Konfigurationen werden angezeigt.

11.4.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

11.4.2.1 ipsec

Beschreibung

Mit diesem Befehl wechseln Sie in den IPSEC-Konfigurationsmodus.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
ipsec
```

Ergebnis

Sie befinden sich jetzt im IPSEC-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ipsec)#
```

Weitere Hinweise

Sie verlassen den IPSEC-Konfigurationsmodus mit dem Befehl `end` oder `exit`.

11.4.3 Befehle im IPSEC-Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im IPSEC-Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl `ipsec` ein, um in diesen Modus zu wechseln.

- Wenn Sie den IPSEC-Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den IPSEC-Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

11.4.3.1 crl-policy

Beschreibung

Mit diesem Befehl legen Sie fest, ob die Gültigkeit der Zertifikate anhand der Zertifikatssperrliste (CRL Certificate Revocation List) überprüft wird.

Voraussetzung

Sie befinden sich im IPSEC-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ipsec)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
CRL-policy {yes|no|ifuri}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`yes`	CRL wird verwendet	-
no	CRL wird nicht verwendet	-
`ifuri`	Wird nur verwendet, wenn eine CRLURL definiert ist.	-

Ergebnis

Der Einstellung ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl show ipsecvpn information an.

11.4.3.2 connection name

Beschreibung

Mit diesem Befehl wechseln Sie in den IPSEC CONNECTION-Konfigurationsmodus. Falls die passende VPN-Verbindung nicht vorhanden ist, wird zuerst eine VPN-Verbindung angelegt.

Voraussetzung

Sie befinden sich im IPSEC-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ipsec)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
connection name <name(122)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`name`	Name der VPN-Verbindung	Geben Sie den Namen für die VPN-Verbindung an. Maximal 122 Zeichen

Ergebnis

Sie befinden sich jetzt im IPSEC CONNECTION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-X)#
```

Weitere Hinweise

Sie verlassen den IPSEC CONNECTION-Konfigurationsmodus mit dem Befehl `end` oder `exit`.

Sie löschen eine VPN-Verbindung mit dem Befehl `no connection name`.

Sie löschen alle VPN-Verbindungen mit dem Befehl `no connection all`.

11.4.3.3 no connection name

Beschreibung

Mit diesem Befehl löschen Sie eine bestimmte VPN-Verbindung.

Voraussetzung

- Die entsprechende VPN-Verbindung ist angelegt und wird nirgendwo verwendet.
- Sie befinden sich im IPSEC CONNECTION-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-ipsec)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no connection name <name(122)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`name`	Name der VPN-Verbindung	Geben Sie den Namen der VPN-Verbindung an.

Ergebnis

Die entsprechende VPN-Verbindung ist gelöscht.

Weitere Hinweise

Sie legen die VPN-Verbindung mit dem Befehl `connection name` an.

11.4.3.4 no connection all

Beschreibung

Mit diesem Befehl löschen Sie alle VPN-Verbindungen.

Voraussetzung

- Die VPN-Verbindungen sind angelegt und werden nirgendwo verwendet.
- Sie befinden sich im IPSEC CONNECTION-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-ipsec)#
  ```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no connection all
```

Ergebnis

Alle VPN-Verbindungen sind gelöscht.

Weitere Hinweise

Sie legen die VPN-Verbindung mit dem Befehl `connection name` an.

11.4.3.5 nat-keep-alive

Beschreibung

Mit diesem Befehl legen Sie fest, in welchen Zeitabständen Lebenszeichentelegramme (Keep Alive) gesendet werden.

Voraussetzung

Sie befinden sich im IPSEC-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ipsec)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
nat-keep-alive <sec(1-10000)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
sec	Zeitintervall	Geben Sie das gewünschte Intervall an. 1 ... 10000 Sekunden

Ergebnis

Das Zeitintervall ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl show ipsecvpn information an.

11.4.3.6 remote-end name

Beschreibung

Mit diesem Befehl wechseln Sie in den IPSEC REMOTE END-Konfigurationsmodus. In diesem Modus konfigurieren Sie die weiteren Einstellungen.

Falls die passende VPN-Gegenstelle nicht vorhanden ist, wird zuerst die VPN-Gegenstelle angelegt.

Voraussetzung

Sie befinden sich im IPSEC-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ipsec)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
remote-end name <name(128)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`name`	Name der VPN-Gegenstelle	Geben Sie den Namen für die VPN-Gegenstelle an. Maximal 128 Zeichen

Ergebnis

Sie befinden sich jetzt im IPSEC REMOTE END-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ipsec-rmend-X)#
```

X ist ein Platzhalter für den Namen

Weitere Hinweise

Sie verlassen den IPSEC REMOTE END-Konfigurationsmodus mit dem Befehl `end` oder `exit`.

Sie löschen eine VPN-Gegenstelle mit dem Befehl `no remote-end name`.

Sie löschen alle VPN-Gegenstellen mit dem Befehl `no remote-end all`.

11.4.3.7 no remote-end name

Beschreibung

Mit diesem Befehl löschen Sie eine bestimmte VPN-Gegenstelle.

Voraussetzung

- Die entsprechende VPN-Gegenstelle ist angelegt und wird nirgendwo verwendet.
- Sie befinden sich im IPSEC REMOTE END-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-ipsec)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no remote-end name <name(128)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`name`	Name der VPN-Gegenstelle	Geben Sie den Namen der VPN-Gegenstelle an. Maximal 128 Zeichen

Ergebnis

Die entsprechende VPN-Gegenstelle ist gelöscht.

Weitere Hinweise

Sie legen die VPN-Gegenstelle mit dem Befehl `remote-end name` an.

11.4.3.8 no remote-end all

Beschreibung

Mit diesem Befehl löschen Sie alle VPN-Gegenstellen.

Voraussetzung

- Die VPN-Gegenstellen sind angelegt und werden nirgendwo verwendet.
- Sie befinden sich im IPSEC REMOTE END-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-ipsec)#
  ```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no remote-end all
```

Ergebnis

Alle VPN-Gegenstellen sind gelöscht.

Weitere Hinweise

Sie legen die VPN-Gegenstelle mit dem Befehl `remote-end name` an.

11.4.3.9 shutdown

Beschreibung

Mit diesem Befehl deaktivieren Sie das IPsec-Verfahren für VPN.

Voraussetzung

Sie befinden sich im IPSEC-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ipsec)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
shutdown
```

Ergebnis

Das IPsec-Verfahren ist deaktiviert.

Weitere Hinweise

Sie aktivieren das IPsec-Verfahren mit dem Befehl `no shutdown`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl show ipsecvpn information an.

11.4.3.10 no shutdown

Beschreibung

Mit diesem Befehl aktivieren Sie das IPsec-Verfahren für VPN.

Voraussetzung

Sie befinden sich im IPSEC-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ipsec)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no shutdown
```

Ergebnis

Das IPsec-Verfahren ist aktiviert.

Weitere Hinweise

Sie deaktivieren das IPsec-Verfahren mit dem Befehl shutdown.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl show ipsecvpn information an.

11.4.4 Befehle im IPSEC REMOTE END-Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im IPSEC REMOTE END-Konfigurationsmodus aufrufen können.

Geben Sie im IPSEC-Konfigurationsmodus den Befehl `remote end name` ein, um in diesen Modus zu wechseln.

- Wenn Sie den IPSEC REMOTE END-Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im IPSEC-Konfigurationsmodus.
- Wenn Sie den IPSEC REMOTE END-Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

11.4.4.1 addr

Beschreibung

Mit diesem Befehl konfigurieren Sie die Adresse der VPN-Gegenstelle.

Voraussetzung

Sie befinden sich im IPSEC REMOTE END-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ipsec-rmend-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
addr <subnet|dns>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`subnet`	IP-Subnetz	• Beim Roadwarrior-Modus Geben Sie die WAN-IP-Adresse an. • Beim Standard-Modus Geben Sie einen IP-Bereich an, aus dem Verbindungen entgegengenommen werden. 0.0.0.0/0 bedeutet alle IP-Adressen werden akzeptiert.
`dns`	DNS-Hostname	Nur beim Standard-Modus Geben Sie den DNS-Hostnamen an.

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Adresse ist festgelegt.

Weitere Hinweise

Sie konfigurieren den Modus mit dem Befehl `conn-mode`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec remoteend` an

11.4.4.2 addr-mode

Beschreibung

Mit diesem Befehl legen Sie die Art der Gegenstellen-Adresse fest.

Voraussetzung

Sie befinden sich im IPSEC REMOTE END-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ipsec-rmend-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
addr-mode <manual|any>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
manual	Nimmt die Verbindung von Gegenstellen mit bestimmter Adresse an.	• Beim Roadwarrior-Modus Nimmt ausschließlich Verbindungen von Gegenstellen mit fester IP-Adresse (/32), festem IP-Subnetz (CIDR Notation), oder (D)DNS-Hostnamen an. • Beim Standard-Modus Baut ausschließlich Verbindung zu einer bestimmten Gegenstelle mit fester IP-Adresse oder mit (D)DNS-Hostnamen auf. Oder nimmt ausschließlich Verbindung von einer bestimmten Gegenstelle mit fester IP-Adresse oder mit (D)DNS-Hostnamen an
any	Nimmt die Verbindung von Gegenstellen mit beliebiger IPv4-Adresse an.	Nur beim Roadwarrior-Modus

Ergebnis

Die Einstellung ist festgelegt.

Weitere Hinweise

Sie konfigurieren den Modus mit dem Befehl `conn-mode`.

Sie konfigurieren die IP-Adresse mit dem Befehl `addr`.

Sie konfigurieren das Remote-Subnetz mit dem Befehl `subnet`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec remoteend` an

11.4.4.3 conn-mode

Beschreibung

Mit diesem Befehl legen Sie fest, welche Rolle die Gegenstellen einnimmt.

Voraussetzung

Sie befinden sich im IPSEC REMOTE END-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ipsec-rmend-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
conn-mode {roadwarrior|standard}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`roadwarrior`	Roadwarrior-Modus Das Gerät nimmt VPN-Verbindungen von Gegenstellen mit unbekannter Adresse an.	-
`standard`	Standard-Modus Das Gerät baut eine Verbindung zu oder von einer bekannten Gegenstelle auf. Die Gegenstelle wird über die IPv4-Adresse oder den DDNS-Hostnamen identifiziert	-

Ergebnis

Die Rolle ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec remoteend` an.

11.4.4.4 subnet

Beschreibung

Mit diesem Befehl konfigurieren Sie das entfernte Subnetz der VPN-Gegenstelle.

Voraussetzung

Sie befinden sich im IPSEC REMOTE END-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ipsec-rmend-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
subnet <subnet|dns>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`subnet`	IP-Subnetz	Geben Sie das Subnetz an.
`dns`	DNS-Name	Geben Sie den DNS-Hostnamen an.

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Das entfernte Subnetz ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec remoteend` an.

11.4.4.5 vir-ip

Beschreibung

Mit diesem Befehl legen Sie das Subnetz fest, aus dem die Gegenstelle eine virtuelle IP-Adresse angeboten bekommt.

Voraussetzung

Sie befinden sich im IPSEC REMOTE END-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ipsec-rmend-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
vir-ip ipv4 [<subnet>]
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`subnet`	Subnetz, aus dem der Gegenstelle eine virtuelle IPv4-Adresse angeboten wird	Geben Sie das Subnetz in CIDR-Schreibweise ein.

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Ds Subnetz ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec remoteend` an.

Sie deaktivieren die Einstellung mit dem Befehl `no vir-ip`.

11.4.4.6 no vir-ip

Beschreibung

Mit diesem Befehl legen Sie fest, dass der Gegenstelle keine virtuelle IPv4-Adresse angeboten wird.

Voraussetzung

Sie befinden sich im IPSEC REMOTE END-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ipsec-rmend-X)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no vir-ip
```

Ergebnis

Die Einstellung ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec remoteend` an.

Sie aktivieren diese Einstellung mit dem Befehl vir-ip.

11.4.5 Befehle im IPSEC CONNECTION-Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im IPSEC CONNECTION-Konfigurationsmodus aufrufen können.

Geben Sie im IPSEC-Konfigurationsmodus den Befehl `connection name` ein, um in diesen Modus zu wechseln.

- Wenn Sie den IPSEC CONNECTION-Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im IPSEC-Konfigurationsmodus.
- Wenn Sie den IPSEC CONNECTION-Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

11.4.5.1 authentication

Beschreibung

Mi diesem Befehl wechseln Sie in den IPSEC AUTHENTICATION-Konfigurationsmodus.

Voraussetzung

Sie befinden sich im IPSEC CONNECTION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-X)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
authentication
```

Ergebnis

Sie befinden sich jetzt im IPSEC AUTHENTICATION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-auth)#
```

Weitere Hinweise

Sie verlassen den IPSEC AUTHENTICATION-Konfigurationsmodus mit dem Befehl `end` oder `exit`.

11.4.5.2 k-proto

Beschreibung

Mit diesem Befehl legen Sie fest, ob IKEv2 oder IKEv1 verwendet wird.

Voraussetzung

Sie befinden sich im IPSEC CONNECTION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
k-proto {ikev1|ikev2}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
IKEv1	Verwendet IKEv1	-
IKEv2	Verwendet IKEv2	-

Ergebnis

Die Einstellung ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec connections` an.

11.4.5.3 loc-subnet

Beschreibung

Mit diesem Befehl konfigurieren Sie das lokale Subnetz.

Voraussetzung

Sie befinden sich im IPSEC CONNECTION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
loc-subnet <subnet|dns>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
subnet	Lokale Subnetzadresse	Geben Sie das lokale Subnetz in der CIDR-Schreibweise an. Das lokale Netz kann ein einzelner PC, oder eine andere Untermenge des lokalen Netzes sein.

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel Schnittstellenbezeichnungen und Adressen (Seite 42).

Ergebnis

Das lokale Subnetz ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsecvpn connections` an.

11.4.5.4 operation

Beschreibung

Mit diesem Befehl legen Sie fest, wie die Verbindung aufgebaut wird.

Voraussetzung

Sie befinden sich im IPSEC CONNECTION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
operation {disabled|start|wait|on-demand|start-di|wait-di}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`disabled`	Die VPN-Verbindung ist deaktiviert	-
`start`	Das Gerät versucht, zu der Gegenstelle eine VPN-Verbindung aufzubauen.	-
`wait`	Das Gerät wartet, bis der Verbindungsaufbau von der Gegenstelle initiiert wird.	-
`on-demand`	Die VPN-Verbindung wird bei Bedarf aufgebaut.	-
`start-di`	Beim Eintreten des Ereignisses "Digital In" versucht das Gerät, zu der Gegenstelle eine VPN-Verbindung aufzubauen. Vorausgesetzt, dass das Ereignis "Digital In" an die VPN-Verbindung weitergegeben wird.	-
`wait-di`	Beim Eintreten des Ereignisses "Digital In" wartet das Gerät, bis der Verbindungsaufbau von der Gegenstelle initiiert wird. Vorausgesetzt, dass das Ereignis "Digital In" an die VPN-Verbindung weitergegeben wird.	-

Ergebnis

Die Einstellung ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec connections` an.

11.4.5.5 phase

Beschreibung

Mit diesem Befehl wechseln Sie in den IPSEC PHASE-Konfigurationsmodus.

Voraussetzung

Sie befinden sich im IPSEC CONNECTION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
phase <num(1-2)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`num`	Phase der VPN-Verbindung	• 1: Phase 1 • 2: Phase 2

Ergebnis

Sie befinden sich jetzt im IPSEC PHASE-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-phsX)#
```

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec connections` an.

11.4.5.6 rmend name

Beschreibung

Mit diesem Befehl legen Sie die VPN-Gegenstelle für die IPsec-Verbindung fest.

Voraussetzung

- Die VPN-Gegenstelle ist angelegt.
- Sie befinden sich im IPSEC CONNECTION-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-conn-X)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
rmend name <name(128)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`name`	Namen der VPN-Gegenstelle	Geben Sie einen gültigen Namen an. Maximal 128 Zeichen

Ergebnis

Die VPN-Gegenstelle ist konfiguriert

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec connections` an.

Sie erstellen die VPN-Gegenstelle mit dem Befehl `remote-end name`.

11.4.5.7 timeout

Beschreibung

Mit diesem Befehl konfigurieren Sie die Zeitspanne ein, nach der die VPN-Verbindung getrennt wird. Wenn innerhalb dieser Zeit keine Pakete gesendet werden, wird der VPN-Verbindung automatisch getrennt.

Voraussetzung

- Die VPN-Verbindung wird bei Bedarf aufgebaut (on demand)
- Sie befinden sich im IPSEC CONNECTION-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-conn-X)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
timeout <sec(0-1000)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`sec`	Zeitspanne	Geben Sie die Zeitspanne in Sekunden an.

Ergebnis

Die Zeitspanne ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec connections` an.

Sie konfigurieren die Einstellung `on demand` mit dem Befehl `operation`.

11.4.5.8 vir-ip

Beschreibung

Mit diesem Befehl legen Sie fest, dass beim Verbindungsaufbau eine virtuelle IPv4-Adresse von der VPN-Gegenstelle anfordert.

Voraussetzung

Sie befinden sich im IPSEC CONNECTION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-X)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
vir-ip
```

Ergebnis

Die Einstellung ist aktiviert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec connections` an.

Sie deaktivieren das Anfordern einer virtuellen IPv4-Adresse mit dem Befehl `no vir-ip`.

11.4.5.9 no vir-ip

Beschreibung

Mit diesem Befehl deaktivieren Sie das Anfordern einer virtuellen IPv4-Adresse.

Voraussetzung

Sie befinden sich im IPSEC CONNECTION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-X)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no vir-ip
```

Ergebnis

Die Einstellung ist deaktiviert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec connections` an.

Sie aktivieren das Anfordern einer virtuellen IPv4-Adresse mit dem befehl `vir-ip`.

11.4.6 Befehle im IPSEC AUTHENTICATION-Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im IPSEC AUTHENTICATION-Konfigurationsmodus aufrufen können.

Geben Sie im IPSEC CONNECTION-Konfigurationsmodus den Befehl `authentication` ein, um in diesen Modus zu wechseln.

- Wenn Sie den IPSEC AUTHENTICATION-Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im IPSEC CONNECTION-Konfigurationsmodus.
- Wenn Sie den IPSEC AUTHENTICATION-Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

11.4.6.1 auth cacert

Beschreibung

Mit diesem Befehl legen Sie fest, dass für die Authentifizierung ein CA-Zertifikat verwendet wird.

Voraussetzung

- Die Zertifikate sind geladen.
- Sie befinden sich im IPSEC AUTHENTICATION-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

```
cli(config-conn-auth)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
auth cacert <string(255)> localcert <string(255)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`cacert`	Schlüsselwort für CA-Zertifikat	
`string`	Name des CA-Zertifikats	Geben Sie ein gültiges CA-Zertifikat an.
`localcert`	Schlüsselwort für Gerätezertifikat	
`string`	Name des Gerätezertifikats	Geben Sie ein gültiges Gerätezertifikat an.

Ergebnis

Die Einstellung ist konfiguriert.

Weitere Hinweise

Sie zeigen die geladenen Zertifikate mit dem Befehl `show-idx` an.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-authentication` an.

Sie zeigen die verfügbaren Zertifikate mit dem Befehl `show-idx`.

Sie zeigen die Konfiguration der IPsec-Verbindung mit dem Befehl `show ipsec connections` an.

Sie entfernen die Authentifizierung mit dem Befehl `no auth`.

11.4.6.2 auth psk

Beschreibung

Mit diesem Befehl legen Sie fest, dass für die Authentifizierung ein Schlüssel verwendet wird.

Voraussetzung

Sie befinden sich im IPSEC AUTHENTICATION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-auth)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
auth psk <string(255)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`string`	Wert für den Schlüssel	Geben Sie einen gültigen Schlüssel an.

Ergebnis

Der Schlüssel ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-authentication` an.

Sie entfernen die Authentifizierung mit dem Befehl `no auth`.

11.4.6.3 auth remcert

Beschreibung

Mit diesem Befehl legen Sie fest, dass für die Authentifizierung das Gegenstellenzertifikat verwendet wird.

Voraussetzung

- Die Zertifikate sind geladen.
- Sie befinden sich im IPSEC AUTHENTICATION-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-conn-auth)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
auth remcert <string(255)> localcert <string(255)>
```

Dabei haben die Parameter folgende Bedeutung:

`remcert`	Schlüsselwort für Gegenstellenzertifikat	-
`string`	Name des Gegenstellenzertifikats	Geben Sie ein gültiges Gegenstellenzertifikat an. Maximal 255 Zeichen
`localcert`	Schlüsselwort für Gerätezertifikat	-
`string`	Name des Gerätezertifikats	Geben Sie ein gültiges Gerätezertifikat an. Maximal 255 Zeichen

Ergebnis

Die Einstellung ist konfiguriert.

Weitere Hinweise

Sie zeigen die geladenen Zertifikate mit dem Befehl `show-idx` an.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-authentication` an.

Sie entfernen die Authentifizierung mit dem Befehl `no auth`.

11.4.6.4 no auth

Beschreibung

Mit diesem Befehl löschen Sie das Authentifizierungsverfahren.

Voraussetzung

Sie befinden sich im IPSEC AUTHENTICATION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-auth)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no auth
```

Ergebnis

Das Authentifizierungsverfahren ist gelöscht.

11.4.6.5 local-id

Beschreibung

Mit diesem Befehl konfigurieren Sie die lokale ID.

Voraussetzung

Sie befinden sich im IPSEC AUTHENTICATION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-auth)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
local-id <string(255)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`string`	lokale ID	Geben Sie die lokale ID an. Wenn Sie die lokale ID nicht festlegen, wird die lokale ID aus dem Gerätezertifikat gelesen. Wenn Sie als Authentifizierung PSK verwenden, wird die WAN-IP-Adresse als lokale ID verwendet.

Ergebnis

Die lokale ID ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-authentication` an.

Sie entfernen die lokale ID mit dem Befehl `no local-id`.

11.4.6.6 no local-id

Beschreibung

Mit diesem Befehl entfernen Sie die lokale ID.

Voraussetzung

Sie befinden sich im IPSEC AUTHENTICATION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-auth)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no local-id
```

Ergebnis

Die lokale ID ist entfernt.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-authentication` an.

Sie konfigurieren die lokale ID mit dem Befehl `local-id`.

11.4.6.7 rem-id

Beschreibung

Mit diesem Befehl konfigurieren Sie die Remote-ID

Voraussetzung

Sie befinden sich im IPSEC AUTHENTICATION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-auth)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
rem-id <string(255)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`string`	Remote-ID	Geben Sie die Remote-ID an. Wenn Sie die Remote-ID nicht festlegen, wird die Remote-ID aus dem Gerätezertifikat gelesen. Wenn Sie als Authentifizierung PSK verwenden, wird die WAN-IP-Adresse als Remote-ID verwendet.

Ergebnis

Die Remote-ID ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-authentication` an.

Sie entfernen die Remote-ID mit dem Befehl `no rem-id`.

11.4.6.8 no rem-id

Beschreibung

Mit diesem Befehl entfernen Sie die Remote-ID

Voraussetzung

Sie befinden sich im IPSEC AUTHENTICATION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-auth)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no rem-id
```

Ergebnis

Die Remote-ID ist entfernt.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-authentication` an.

Sie konfigurieren die Remote-ID mit dem Befehl `rem-id`.

11.4.7 Befehle im IPSEC PHASE1-Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im IPSEC PHASE-Konfigurationsmodus aufrufen können.

Geben Sie im IPSEC CONNECTION-Konfigurationsmodus den Befehl `phase` mit dem Parameter `1` ein, um in diesen Modus zu wechseln.

- Wenn Sie den IPSEC PHASE1-Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im IPSEC CONNECTION-Konfigurationsmodus.
- Wenn Sie den IPSEC PHASE1-Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

11.4.7.1 aggressive

Beschreibung

Mit diesem Befehl legen Sie fest, dass der Aggressive Mode verwendet wird.

Voraussetzung

Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-phs1)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
aggressive
```

Ergebnis

Die Einstellung ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase1` an.

Sie deaktivieren den Aggressive Mode mit dem Befehl `no aggressive`.

11.4.7.2 no aggressive

Beschreibung

Mit diesem Befehl deaktivieren Sie den Aggressive Mode.

Voraussetzung

Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-phs1)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no aggressive
```

Ergebnis

Die Einstellung ist deaktiviert. Der Main Mode wird verwendet.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase1` an.

Sie aktivieren den Aggressive Mode mit dem Befehl `aggressive`.

11.4.7.3 default-ciphers

Beschreibung

Mit diesem Befehl legen Sie fest, das beim Verbindungsaufbau eine vorgegebene Liste (Default-Liste) an den VPN-Verbindungspartner übermittelt wird. In der Liste sind Kombinationen aus den drei Algorithmen (Encryption, Authentication, Key Derivation) enthalten.
Um eine VPN-Verbindung aufzubauen, muss der VPN-Verbindungspartner mindestens eine dieser Kombinationen unterstützen. Die Kombinationen sind abhängig von der Phase und vom Schlüsselaustauschverfahren (IKE).

Kombination			Phase 1		Phase 2	
Encryption	Authentication	Key Derivation	IKEv1	IKEv2	IKEv1	IKEv2
AES128	SHA1	DH Group 14	x	x	x	x
AES256	SHA512	DH Group 16	x	x	x	x
AES128 CCM 16	SHA256	DH Group 14	-	x	x	x
AES256 CCM 16	SHA512	DH Group 16	-	x	x	x
AES128	SHA1	none	-	-	x	x
AES256	SHA512	none	-	-	x	x
AES128 CCM 16	SHA256	none	-	-	x	x
AES256 CCM 16	SHA512	none	-	-	x	x

x: wird unterstützt

-: wird nicht unterstützt

none: Für die Phase 2 werden keine separaten Schlüssel ausgetauscht. Damit ist Perfect Forward Secrecy (PFS) deaktiviert.

Voraussetzung

Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-phsX)#

X: 1 (Phase 1)

   2 (Phase 2)
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
default-ciphers
```

Ergebnis

Die Default-Liste wird verwendet..

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phaseX` an.

Sie deaktivieren die Verwendung der Default-Liste mit dem Befehl `no default-ciphers`.

11.4.7.4 no default-ciphers

Beschreibung

Mit diesem Befehl deaktivieren Sie die Verwendung der Default-Liste

Voraussetzung

Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-phsX)#
X: 1 (Phase 1)
   2 (Phase 2)
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no default-ciphers
```

Ergebnis

Die Verwendung der Default-List ist deaktiviert. Für die Phase werden die festeingestellten Werte verwendet.

Weitere Hinweise

Sie konfigurieren die festgelegten Werte für die Phase 1 mit den Befehlen `ike-encryption`, `ike-auth` und `ike-keyderivation`.

Sie konfigurieren die festgelegten Werte für die Phase 2 mit den Befehlen `esp-encryption`, `esp-auth` und `esp-keyderivation`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase1` oder `show ipsec conn-phase2` an.

Sie aktivieren die Verwendung der Default-Liste mit dem Befehl `default-ciphers`.

11.4.7.5 dpd

Beschreibung

Mit diesem Befehl aktivieren Sie Dead Peer Detection (DPD).

Voraussetzung

Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-phs1)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

dpd

Ergebnis

DPD ist aktiviert. Mit DPD lässt sich feststellen, ob die VPN-Verbindung noch besteht oder ob sie abgebrochen ist.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase1` an.

Sie deaktivieren DPD mit dem Befehl `no dpd`.

11.4.7.6 no dpd

Beschreibung

Mit diesem Befehl deaktivieren Sie DPD.

Voraussetzung

Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-phs1)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

`no` dpd

Ergebnis

DPD ist deaktiviert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase1` an.

Sie aktivieren DPD mit dem Befehl `dpd`.

11.4.7.7 dpd-period

Beschreibung

Mit diesem Befehl konfigurieren Sie eine Zeitspanne, nach der DPD-Anfragen gesendet werden.

Voraussetzung

- DPD ist aktiviert
- Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-conn-phs1)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
dpd-period <sec(10-120)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`sec`	Zeitspanne der DPD-Anfragen	Geben Sie die Zeitspanne in Sekunden an.

Ergebnis

Die Zeitspanne ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase1` an.

Sie aktivieren DPD mit dem Befehl `dpd`.

11.4.7.8 dpd-timeout

Beschreibung

Mit diesem Befehl konfigurieren Sie die Timeout-Einstellung für die VPN-Verbindung. Wenn auf die DPD-Anfragen keine Antwort erfolgt, dann wird nach Ablauf dieser Zeit die Verbindung zur Gegenstelle für ungültig erklärt.

Voraussetzung

- DPD ist aktiviert
- Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-conn-phs1)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
dpd-timeout <sec(10-1000)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`sec`	Zeitspanne der DPD-Anfragen	Geben Sie die Zeitspanne in Sekunden an. **Hinweis:** Um ungewollte Verbindungsabbrüche zu vermeiden, stellen Sie den DPD-Timeout wesentlich länger als den DPD-Zeitraum ein. Wir empfehlen bei DPD-Timeout mindestens das Dreifache des DPD-Zeitraums einzustellen.

Ergebnis

Die Zeitspanne ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase1` an.

Sie aktivieren DPD mit dem Befehl `dpd`.

11.4.7.9 ike-auth

Beschreibung

Mit diesem Befehl konfigurieren Sie das Verfahren zum Berechnen der Prüfsumme.

Voraussetzung

- Die Default-Liste wird nicht verwendet.
- Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-conn-phs1)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ike-auth {md5|sha1|sha256|sha384|sha512}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`md5`	Message-Digest Algorithm 5	-
`sha1`	Secure Hash Algortihm 1 mit 160 Bit Hashlänge	-
`sha256`	Secure Hash Algorithm 2 mit 256 Bit Hashlänge	-

Parameter	Beschreibung	Wertebereich/Anmerkung
sha384	Secure Hash Algorithm 2 mit 384 Bit Hashlänge	-
sha512	Secure Hash Algorithm 2 mit 512 Bit Hashlänge	-

Ergebnis

Das Verfahren zum Berechnen der Prüfsumme ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase1` an.

Sie deaktivieren die Verwendung der Default-Liste mit dem Befehl `no default-ciphers`.

11.4.7.10 ike-encryption

Beschreibung

Mit diesem Befehl konfigurieren Sie den Verschlüsselungsalgorithmus.

Voraussetzung

- Die Default-Liste wird nicht verwendet.
- Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-conn-phs1)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ike-encryption
{3des|aes128cbc|aes192cbc|aes256cbc|aes128ctr|aes192ctr|aes256ctr|aes128ccm16|aes192c
cm16|aes256ccm16|aes128gcm16|aes192gcm16|aes256gcm16}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Phase 1	
		IKEv1	IKEv2
3des	Triple Data Encryption Standard	x	x
aes128cbc	Advanced Encryption Standard mit 128 Bit	x	x
aes192cbc	Advanced Encryption Standard mit 192 Bit	x	x
aes256cbc	Advanced Encryption Standard mit 256 Bit	x	x
aes128ctr	Advanced Encryption Standard mit 128 Bit im Counter Mode	-	x
aes192ctr	Advanced Encryption Standard mit 192 Bit im Counter Mode	-	x

Parameter	Beschreibung	Phase 1	
		IKEv1	IKEv2
`aes256ctr`	Advanced Encryption Standard mit 256 Bit im Counter Mode	-	x
`aes128ccm16`	Advanced Encryption Standard mit 128 Bit im Counter Mode, unter Verwendung eines 16 Byte Integrity Check Values (ICV)	-	x
`aes192ccm16`	Advanced Encryption Standard mit 192 Bit im Counter Mode, unter Verwendung eines 16 Byte Integrity Check Values (ICV) .	-	x
`aes256ccm16`	Advanced Encryption Standard mit 256 Bit im Counter Mode, unter Verwendung eines 16 Byte Integrity Check Values (ICV)	-	x
`aes128gcm16`	Advanced Encryption Standard mit 128 Bit im Galois Counter Mode, unter Verwendung eines 16 Byte Integrity Check Values (ICV)	-	x
`aes192gcm16`	Advanced Encryption Standard mit 192 Bit im Galois Counter Mode, unter Verwendung eines 16 Byte Integrity Check Values (ICV)	-	x
`aes256gcm16`	Advanced Encryption Standard mit 256 Bit im Galois Counter Mode, unter Verwendung eines 16 Byte Integrity Check Values (ICV)	-	x

x: wird unterstützt

-: wird nicht unterstützt

Ergebnis

Der Verschlüsselungsalgorithmus ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase1` an.

Sie deaktivieren die Verwendung der Default-Liste mit dem Befehl `no default-ciphers`.

11.4.7.11 ike-keyderivation

Beschreibung

Mit diesem Befehl konfigurieren Sie die Diffie-Hellmann-Gruppe (DH), aus der ein Schlüssel erzeugt wird.

Voraussetzung

- Die Default-Liste wird nicht verwendet.
- Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  `cli(config-conn-phs1)#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

`ike-keyderivation {dhgroup <1|2|5|14|15|16|17|18>}`

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`auto`	Automatische Erkennung	-
`dhgroup`	Diffie-Hellmann-Gruppe (DH)	Geben Sie die gewünschte Diffie-Hellmann-Gruppe (DH) an. • `1` • `2` • `5` • `14` • `15` • `16` • `17` • `18`

Ergebnis

Die Diffie-Hellmann-Gruppe (DH) ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase1` an.

Sie deaktivieren die Verwendung der Default-Liste mit dem Befehl `no default-ciphers`.

11.4.7.12 ike-keytries

Beschreibung

Mit diesem Befehl konfigurieren Sie die Anzahl der Wiederholungen für einen fehlgeschlagenen Verbindungsaufbau.

Voraussetzung

Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-phs1)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ike-keytries <num(0-100)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
num	Zeitspanne der DPD-Anfragen	Geben Sie die gewünschte Anzahl an. Bei 0 wird der Verbindungsaufbau unendlich oft zu versucht.

Ergebnis

Die Anzahl ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase1` an.

11.4.7.13 ike-lifetime

Beschreibung

Mit diesem Befehl konfigurieren Sie den Zeitraum, der die Lebensdauer der vereinbarten Schlüssel festlegt. Nach Ablauf der Zeit wird der Schlüssel neu ausgehandelt.

Voraussetzung

Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-phs1)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
ike-lifetime <min(10-2500000)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`min`	Zeitspanne der DPD-Anfragen	Geben Sie die Zeitspanne in Minuten an.

Ergebnis

Die Zeitspanne ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase1` an.

11.4.8 Befehle im IPSEC PHASE2-Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im IPSEC PHASE-Konfigurationsmodus aufrufen können.

Geben Sie im IPSEC CONNECTION-Konfigurationsmodus den Befehl `phase` mit dem Parameter `2` ein, um in diesen Modus zu wechseln.

- Wenn Sie den IPSEC PHASE2-Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im IPSEC CONNECTION-Konfigurationsmodus.
- Wenn Sie den IPSEC PHASE2-Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus

11.4.8.1 auto-fwrules

Beschreibung

Mit diesem Befehl legen Sie fest, dass für die VPN-Verbindung die Firewall-Regel automatisch angelegt wird.

Voraussetzung

Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-phs2)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
auto-fwrules
```

Ergebnis

Für die VPN-Verbindung wird die Firewall-Regel automatisch angelegt.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase2` an.

Sie deaktivieren die Einstellung mit dem Befehl `no auto-fwrules`.

11.4.8.2 no auto-fwrules

Beschreibung

Mit diesem Befehl legen Sie fest, dass für die VPN-Verbindung die Firewall-Regel nicht automatisch angelegt wird.

Voraussetzung

Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-phs2)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no auto-fwrules
```

Ergebnis

Für die VPN-Verbindung wird die Firewall-Regeln nicht automatisch angelegt. Sie müssen die Firewall-Regel manuell erstellen.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase2` an.

Sie aktivieren die Einstellung mit dem Befehl`auto-fwrules`.

11.4.8.3 default-ciphers

Beschreibung

Mit diesem Befehl legen Sie fest, das beim Verbindungsaufbau eine vorgegebene Liste (Default-Liste) an den VPN-Verbindungspartner übermittelt wird. In der Liste sind Kombinationen aus den drei Algorithmen (Encryption, Authentication, Key Derivation) enthalten.

Um eine VPN-Verbindung aufzubauen, muss der VPN-Verbindungspartner mindestens eine dieser Kombinationen unterstützen. Die Kombinationen sind abhängig von der Phase und vom Schlüsselaustauschverfahren (IKE).

Kombination			Phase 1		Phase 2	
Encryption	Authenticati-on	Key Derivation	IKEv1	IKEv2	IKEv1	IKEv2
AES128	SHA1	DH Group 14	x	x	x	x
AES256	SHA512	DH Group 16	x	x	x	x
AES128 CCM 16	SHA256	DH Group 14	-	x	x	x
AES256 CCM 16	SHA512	DH Group 16	-	x	x	x
AES128	SHA1	none	-	-	x	x
AES256	SHA512	none	-	-	x	x
AES128 CCM 16	SHA256	none	-	-	x	x
AES256 CCM 16	SHA512	none	-	-	x	x

x: wird unterstützt

-: wird nicht unterstützt

none: Für die Phase 2 werden keine separaten Schlüssel ausgetauscht. Damit ist Perfect Forward Secrecy (PFS) deaktiviert.

Voraussetzung

Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-phsX)#

X: 1 (Phase 1)

   2 (Phase 2)
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
default-ciphers
```

Ergebnis

Die Default-Liste wird verwendet..

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phaseX` an.

Sie deaktivieren die Verwendung der Default-Liste mit dem Befehl `no default-ciphers`.

11.4.8.4 no default-ciphers

Beschreibung

Mit diesem Befehl deaktivieren Sie die Verwendung der Default-Liste

Voraussetzung

Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-phsX)#
X: 1 (Phase 1)
   2 (Phase 2)
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no default-ciphers
```

Ergebnis

Die Verwendung der Default-List ist deaktiviert. Für die Phase werden die festeingestellten Werte verwendet.

Weitere Hinweise

Sie konfigurieren die festgelegten Werte für die Phase 1 mit den Befehlen `ike-encryption`, `ike-auth` und `ike-keyderivation`.

Sie konfigurieren die festgelegten Werte für die Phase 2 mit den Befehlen `esp-encryption`, `esp-auth` und `esp-keyderivation`.

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase1` oder `show ipsec conn-phase2` an.

Sie aktivieren die Verwendung der Default-Liste mit dem Befehl `default-ciphers`.

11.4.8.5 esp-auth

Beschreibung

Mit diesem Befehl konfigurieren Sie das Verfahren zum Berechnen der Prüfsumme.

Voraussetzung

- Die Default-Liste wird nicht verwendet.
- Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-conn-phs2)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
esp-auth md5|sha1|sha256|sha384|sha512}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`md5`	Message-Digest Algorithm 5	-
`sha1`	Secure Hash Algortihm 1 mit 160 Bit Hashlänge	-
`sha256`	Secure Hash Algorithm 2 mit 256 Bit Hashlänge	-
`sha384`	Secure Hash Algorithm 2 mit 384 Bit Hashlänge	-
`sha512`	Secure Hash Algorithm 2 mit 512 Bit Hashlänge	-

Ergebnis

Das Verfahren zum Berechnen der Prüfsumme ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase2` an.

Sie deaktivieren die Verwendung der Default-Liste mit dem Befehl `no default-ciphers`.

11.4.8.6 esp-encryption

Beschreibung

Mit diesem Befehl konfigurieren Sie den Verschlüsselungsalgorithmus.

Voraussetzung

- Die Default-Liste wird nicht verwendet.
- Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

```
cli(config-conn-phs2)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
esp-encryption {3des|aes128cbc|aes192cbc|aes256cbc|aes128ctr|aes192ctr|aes256ctr|
aes128ccm16|aes192ccm16|aes256ccm16|aes128gcm16|aes192gcm16|aes256gcm16}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Phase 2	
		IKEv1	IKEv2
3des	Triple Data Encryption Standard	x	x
aes128cbc	Advanced Encryption Standard mit 128 Bit	x	x
aes192cbc	Advanced Encryption Standard mit 192 Bit	x	x
aes256cbc	Advanced Encryption Standard mit 256 Bit	x	x
aes128ctr	Advanced Encryption Standard mit 128 Bit im Counter Mode	x	x
aes192ctr	Advanced Encryption Standard mit 192 Bit im Counter Mode	x	x
aes256ctr	Advanced Encryption Standard mit 256 Bit im Counter Mode	x	x
aes128ccm16	Advanced Encryption Standard mit 128 Bit im Counter Mode, unter Verwendung eines 16 Byte Integrity Check Values (ICV)	x	x
aes192ccm16	Advanced Encryption Standard mit 192 Bit im Counter Mode, unter Verwendung eines 16 Byte Integrity Check Values (ICV) .	x	x
aes256ccm16	Advanced Encryption Standard mit 256 Bit im Counter Mode, unter Verwendung eines 16 Byte Integrity Check Values (ICV)	x	x
aes128gcm16	Advanced Encryption Standard mit 128 Bit im Galois Counter Mode, unter Verwendung eines 16 Byte Integrity Check Values (ICV)	x	x

Parameter	Beschreibung	Phase 2	
		IKEv1	IKEv2
`aes192gcm16`	Advanced Encryption Standard mit 192 Bit im Galois Counter Mode, unter Verwendung eines 16 Byte Integrity Check Values (ICV)	x	x
`aes256gcm16`	Advanced Encryption Standard mit 256 Bit im Galois Counter Mode, unter Verwendung eines 16 Byte Integrity Check Values (ICV)	x	x

x: wird unterstützt

-: wird nicht unterstützt

Ergebnis

Der Verschlüsselungsalgorithmus ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase2` an.

Sie deaktivieren die Verwendung der Default-Liste mit dem Befehl `no default-ciphers`.

11.4.8.7 esp-keyderivation

Beschreibung

Mit diesem Befehl konfigurieren Sie die Diffie-Hellmann-Gruppe (DH), aus der ein Schlüssel erzeugt wird.

Voraussetzung

- Die Default-Liste wird nicht verwendet.
- Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-conn-phs2)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
esp-keyderivation {none|dhgroup <1|2|5|14|15|16|17|18>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`none`	Es werden keine Schlüssel ausgetauscht und Perfect Forward Secrecy (PFS) ist deaktivert	-
`dhgroup`	Diffie-Hellmann-Gruppe (DH)	Geben Sie die gewünschte Diffie-Hellmann-Gruppe (DH) an. • `1` • `2` • `5` • `14` • `15` • `16` • `17` • `18`

Ergebnis

Die Diffie-Hellmann-Gruppe (DH) ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase2` an.

Sie deaktivieren die Verwendung der Default-Liste mit dem Befehl `no default-ciphers`.

11.4.8.8 lifebyte

Beschreibung

Mit diesem Befehl konfigurieren Sie das Datenlimit, das die Lebensdauer der vereinbarten Schlüssel festlegt. Nach Ablauf des Datenlimits wird der Schlüssel neu ausgehandelt.

Voraussetzung

Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-phs2)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
lifebyte <integer(0-4294967295)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`integer`	Datenlimit	Geben Sie das Datenlimit in Bytes an.

Ergebnis

Das Datenlimit ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase2` an.

11.4.8.9 lifetime

Beschreibung

Mit diesem Befehl konfigurieren Sie den Zeitraum, der die Lebensdauer der vereinbarten Schlüssel festlegt. Nach Ablauf der Zeit wird der Schlüssel neu ausgehandelt.

Voraussetzung

Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-conn-phs2)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
lifetime <min(10-16666666)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`min`	Zeitspanne	Geben Sie die Zeitspanne in Minuten an.

Ergebnis

Die Zeitspanne ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase2` an.

11.4.8.10 port

Beschreibung

Mit diesem Befehl legen Sie den Port fest, durch den der VPN-Tunnel kommuniziert.

Voraussetzung

- Der VPN-Verbindung ist eine VPN-Gegenstelle zugewiesen
- Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-conn-phs2)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
port {all|range <number(0-65535)-number(0-65535)>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`all`	Gilt für alle Ports.	-
`range`	Schlüsselwort für Port-bereich	
`number`	Porbereich	Geben Sie den Start-Port an. 0 ... 65535
`number`		Geben Sie den End-Port an. 0 ... 65535

Ergebnis

Der Port oder Portbereich ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase2` an.

Sie weisen der VPN-Verbindung mit dem Befehl `rmend name` eine VPN-Gegenstelle zu.

11.4.8.11 proto

Beschreibung

Mit diesem Befehl legen Sie fest, für welches Protokoll die VPN-Verbindung gültig ist.

Voraussetzung

- Der VPN-Verbindung ist eine VPN-Gegenstelle zugewiesen
- Sie befinden sich im IPSEC PHASE-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-conn-phs2)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
proto {all|<integer(0-255)>}
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`all`	Gilt für alle Protokolle	-
`integer`	Protokollnummer	Geben Sie die Nummer für das gewünschte Protokoll an. Eine Liste der Protokollnummern finden Sie auf den Internetseiten von iana.org.

Ergebnis

Das Protokoll ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show ipsec conn-phase2` an.

Sie weisen der VPN-Verbindung mit dem Befehl `rmend name` eine VPN-Gegenstelle zu.

11.5 Zertifikate

In diesem Kapitel werden Befehle beschrieben, die für Zertifikate sind.

11.5.1 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

11.5.1.1 certificate

Beschreibung

Mit diesem Befehl wechseln Sie in den CERT-Konfigurationsmodus.

Voraussetzung

Sie befinden sich jetzt im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
certificate
```

Ergebnis

Sie befinden sich jetzt im CERT-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-cert)#
```

Weitere Hinweise

Sie verlassen den CERT-Konfigurationsmodus mit dem Befehl `end`.

11.5.2 Befehle im CERT-Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im CERT-Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl `certificate` ein, um in diesen Modus zu wechseln.

- Wenn Sie den CERT-Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den CERT-Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

11.5.2.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

show-idx

Beschreibung

Der Befehl listet die geladenen Zertifikate und deren Indizes auf.

Voraussetzung

- Zertifikate sind geladen.
- Sie befinden sich im CERT-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-cert)#
  ```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show-idx
```

Ergebnis

Die Liste wird angezeigt.

show-info

Beschreibung

Dieser Befehl zeigt Informationen zum entsprechenden Zertifikat an, z. B. die Seriennummer.

Voraussetzung

- Sie befinden sich im CERT-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-cert)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show-info idx <number>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`idx`	Nummer, die einem bestimmten Zertifikat entspricht.	Geben Sie die gewünschte Nummer an. 1 ... 100

Ergebnis

Die Informationen zum Zertifikat werden angezeigt.

Weitere Hinweise

Sie zeigen die Indizes des Zertifikats mit dem Befehl `show idx` an.

11.5.2.2 cacert

Beschreibung

Mit diesem Befehl legen Sie für ein CA-Zertifikat die zugehörige Sperrliste fest.

Voraussetzung

- Sie befinden sich im CERT-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-cert)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
cacert <idx number> uri {first|second} <URL>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`idx number`	Nummer, die einem bestimmten Zertifikat entspricht.	Geben Sie die gewünschte Nummer an. 1 ... 100
`uri`	Schlüsselwort für die URL	-
`first`	Zertifikatssperrliste 1. URL	-
`second`	Zertifikatssperrliste 2. URL	-
`URL`	Tragen Sie die URL ein, über die die Sperrliste abgerufen werden kann. Tragen Sie eine Alternativ-URL ein. Wenn die Sperrliste über die 1. URL nicht abrufbar ist, wird die Alternativ-URL verwendet.	Nur editierbar, wenn vom Zertifikat unterstützt.

Ergebnis

Die Sperrliste für das betreffende CA-Zertifikat ist festgelegt.

Weitere Hinweise

Sie zeigen die verfügbaren Zertifikate mit dem Befehl `show-idx` an.

Sie zeigen die Verwendung des Zertifikats mit dem Befehl `show-info` an.

11.5.2.3 del

Beschreibung

Mit diesem Befehl löschen Sie ein bestimmtes Zertifikat oder alle Zertifikate.

Voraussetzung

- Zertifikate sind geladen und werden nirgendwo verwendet.
- Sie befinden sich im CERT-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-cert)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
del { <idx number> | all }
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`idx number`	Nummer, die einem bestimmten Zertifikat entspricht.	Geben Sie die gewünschte Nummer an. 1 ... 100
`all`	Löscht alle Zertifikate.	---

Ergebnis

Das entsprechende Zertifikat ist gelöscht.

Weitere Hinweise

Sie laden Zertifikate dem Befehl `tftp load`.

Sie zeigen die verfügbaren Zertifikate mit dem Befehl `show-idx` an.

Sie zeigen die Verwendung des Zertifikats mit dem Befehl `show-info` an.

11.5.2.4 passphrase

Beschreibung

Mit diesem Befehl legen Sie das Passwort für das entsprechende Zertifikat fest.

Voraussetzung

- Sie befinden sich im CERT-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-cert)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
passphrase <idx number> <key>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`idx number`	Nummer, die einem bestimmten Zertifikat entspricht.	Geben Sie die gewünschte Nummer an. 1 ... 100
`key`	Wert für den Schlüssel	Geben Sie einen gültigen Schlüssel an.

Ergebnis

Das Passwort für das Zertifikat ist festgelegt.

Weitere Hinweise

Sie zeigen die passwortgeschützten Zertifikate mit dem Befehl `passphrase show-idx` an.

11.5.2.5 passphrase show-idx

Beschreibung

Der Befehl listet die Zertifikate auf, die passwortgeschützt sind.

Voraussetzung

- Zertifikate sind geladen.
- Sie befinden sich im CERT-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-cert)#
  ```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
passphrase show-idx
```

Ergebnis

Die Liste wird angezeigt.

Weitere Hinweise

Sie konfigurieren das Passwort mit dem Befehl `passphrase` an.

11.6 OpenVPN

In diesem Kapitel werden Befehle beschrieben, die für OpenVPN-Client relevant sind.

11.6.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

11.6.1.1 show openvpn authentication

Beschreibung

Dieser Befehl zeigt die Sicherheitseinstellungen der OpenVPN-Verbindungen an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show openvpn authentication
```

Ergebnis

Die Einstellungen werden angezeigt.

11.6.1.2 show openvpn connections

Beschreibung

Dieser Befehl zeigt die Konfiguration der OpenVPN-Verbindungen an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show openvpn connections
```

Ergebnis

Die Konfigurationen werden angezeigt.

11.6.1.3 show openvpn remoteend

Beschreibung

Dieser Befehl zeigt die Konfiguration der Gegenstellen (VPN-Endpunkt) an.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show openvpn remoteend
```

Ergebnis

Die Konfigurationen werden angezeigt.

11.6.2 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

11.6.2.1 openvpn

Beschreibung

Mit diesem Befehl wechseln Sie in den OPENVPN-Konfigurationsmodus.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
openvpn
```

Ergebnis

Sie befinden sich jetzt im OPENVPN-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn)#
```

Weitere Hinweise

Sie verlassen den OPENVPN-Konfigurationsmodus mit dem Befehl `end` oder `exit`.

11.6.3 OPENVPN-Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im OPENVPN-Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl `openvpn` ein, um in diesen Modus zu wechseln.

- Wenn Sie den OPENVPN-Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den OPENVPN-Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

11.6.3.1 connection name

Beschreibung

Mit diesem Befehl wechseln Sie in den OPENVPN CONNECTION-Konfigurationsmodus. Falls die passende OpenVPN-Verbindung nicht vorhanden ist, wird zuerst eine OpenVPN-Verbindung angelegt.

Voraussetzung

Sie befinden sich im OPENVPN-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
connection name <string(128)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`string`	Name der OpenVPN-Verbindung	Geben Sie den Namen für die OpenVPN-Verbindung an. Maximal 128 Zeichen

Ergebnis

Sie befinden sich jetzt im OPENVPN CONNECTION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-ov-conn-X)#
```

Weitere Hinweise

Sie verlassen den OPENVPN CONNECTION-Konfigurationsmodus mit dem Befehl `end` oder `exit`.

Sie löschen OpenVPN-Verbindungen mit dem Befehl `no conn name`.

Sie zeigen die Konfiguration der OpenVPN-Verbindung dem Befehl `show openvpn connctions` an.

11.6.3.2 no conn

Beschreibung

Mit diesem Befehl löschen Sie eine bestimmte OpenVPN-Verbindung oder alle OpenVPN-Verbindungen.

Voraussetzung

- Die entsprechende OpenVPN-Verbindung ist angelegt und wird nirgends verwendet.
- Sie befinden sich im OPENVPN-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-openvpn)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no conn {name <name(128)> | all}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`name`	Schlüsselwort für die OpenVPN-Verbindung	-
`string`	Löscht die angegebene OpenVPN-Verbindung	Geben Sie einen gültigen Namen an. Max.128 Zeichen
`all`	Löscht alle OpenVPN-Verbindungen	-

Ergebnis

Die entsprechende OpenVPN-Verbindung ist gelöscht.

Weitere Hinweise

Sie legen die OpenVPN-Verbindung mit dem Befehl `connection name`.

Sie zeigen die verfügbaren OpenVPN-Verbindungen mit dem Befehl `show conn-names` an.

11.6.3.3 remote name

Beschreibung

Mit diesem Befehl wechseln Sie in den OPENVPN REMOTE END-Konfigurationsmodus. In diesem Modus konfigurieren Sie die weiteren Einstellungen.

Falls die passende OpenVPN-Gegenstelle nicht vorhanden ist, wird zuerst die OpenVPN-Gegenstelle angelegt.

Voraussetzung

Sie befinden sich im OPENVPN-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
remote name <name(128)>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`name`	Name der OpenVPN-Gegenstelle	Geben Sie den Namen für die OpenVPN-Gegenstelle an. Maximal 128 Zeichen

Ergebnis

Sie befinden sich jetzt im OPENVPN REMOTE END-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn-rm-X)#
```

X ist ein Platzhalter für den Namen

Weitere Hinweise

Sie verlassen den OpenVPN REMOTE END-Konfigurationsmodus mit dem Befehl `end` oder `exit`.

Sie löschen VPN-Gegenstellen mit dem Befehl `no remote`.

11.6.3.4 no remote

Beschreibung

Mit diesem Befehl löschen Sie eine bestimmte OpenVPN-Gegenstelle oder alle OpenVPN-Gegenstellen.

Voraussetzung

- Die entsprechende OpenVPN-Gegenstelle ist angelegt und wird nirgendwo verwendet.
- Sie befinden sich im OPENVPN-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-openvpn)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no remote {name <name(128)> | all}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`name`	Schlüsselwort für die OpenVPN-Gegenstelle	-
`name`	Löscht die angegebene OpenVPN-Gegenstelle	Geben Sie einen gültigen Namen an. Max.128 Zeichen
`all`	Löscht alle OpenVPN-Gegenstellen	-

Ergebnis

Die entsprechende OpenVPN-Gegenstelle ist gelöscht.

Weitere Hinweise

Sie erstellen eine OpenVPN-Gegenstelle mit dem Befehl `remote name`.

11.6.3.5 shutdown

Beschreibung

Mit diesem Befehl deaktivieren Sie die OpenVPN.

Voraussetzung

Sie befinden sich im OPENVPN-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
shutdown
```

Ergebnis

OpenVPN ist deaktiviert

Weitere Hinweise

Sie aktivieren OpenVPN mit dem Befehl `no shutdown`.

11.6.3.6 no shutdown

Beschreibung

Mit diesem Befehl aktivieren Sie OpenVPN.

Voraussetzung

Sie befinden sich im OPENVPN-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no shutdown
```

Ergebnis

OpenVPN ist aktiviert.

Weitere Hinweise

Sie deaktivieren OpenVPN mit dem Befehl `shutdown`.

11.6.4 Befehle im OPENVPN REMOTE END-Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im OPENVPN REMOTE END-Konfigurationsmodus aufrufen können.

Geben Sie im OPENVPN-Konfigurationsmodus den Befehl `remote end name` ein, um in diesen Modus zu wechseln.

- Wenn Sie den OPENVPN REMOTE END-Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im OPENVPN-Konfigurationsmodus.
- Wenn Sie den OPENVPN REMOTE END-Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

11.6.4.1 connection

Beschreibung

Mit diesem Befehl legen Sie die OpenVPN-Verbindung für die OpenVPN-Gegenstelle fest.

Voraussetzung

Sie befinden sich im OPENVPN REMOTE END-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn-rm-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
connection <name>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`name`	Namen der OpenVPN-Verbindung	Geben Sie einen gültigen Namen an. Maximal 128 Zeichen

Ergebnis

Die OpenVPN-Verbindung ist geändert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show openvpn remoteend` an.

11.6.4.2 port

Beschreibung

Mit diesem Befehl legen Sie den Port fest, durch den der VPN-Tunnel kommuniziert.

Voraussetzung

Sie befinden sich im OPENVPN REMOTE END-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn-rm-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
port <1-65535>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
-	Portnummer	Geben Sie eine gültige Portnummer an. `1 ... 65535`

Ergebnis

Der Port ist festgelegt.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show openvpn remoteend` an.

11.6.4.3 proto

Beschreibung

Mit diesem Befehl ändern Sie das eingestellte Protokoll.

Voraussetzung

- Der Proxy-Server ist konfiguriert.
- Sie befinden sich im OPENVPN REMOTE END-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-openvpn-rm-X)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
proto {udp|tcp [proxy <string (255)>]}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`udp`	UDP-Protokoll	-
`tcp`	TCP-Protokoll	-
`proxy`	Schlüsselwort für den Proxyserver, über der OpenVPN-Tunnel zu der definierten OpenVPN-Gegenstelle aufgebaut wird.	-
`string`	Name des Proxyservers Vorausgesetzt, das Protokoll TCP wird verwendet und der Proxy-Server ist angelegt	Geben Sie den Proxy-Server an. Maximal 255 Zeichen.

Ergebnis

Das Protokoll ist geändert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show openvpn remoteend` an.

11.6.4.4 proxy

Beschreibung

Mit diesem Befehl legen Sie fest, ob der OpenVPN-Tunnel zu der definierten OpenVPN-Gegenstelle über einen Proxy-Server aufgebaut wird.

Voraussetzung

- Der Proxy-Server ist konfiguriert.
- Sie befinden sich im OPENVPN REMOTE END-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-openvpn-rm-X)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
proxy <name>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`name`	Proxy-Servername	Geben Sie den Proxy-Servernamen an. Max.128 Zeichen

Ergebnis

Der Proxy-Server, über den die Verbindung aufgebaut wird, ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show openvpn remoteend` an.

11.6.4.5 remote-addr

Beschreibung

Mit diesem Befehl konfigurieren Sie die WAN-IP-Adresse oder den DNS-Hostnamen der OpenVPN-Gegenstelle.

Voraussetzung

Sie befinden sich im OPENVPN REMOTE END-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn-rm-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
remote-addr <ipaddr|dns>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`ipaddr`	WAN-IP-Adresse	Geben Sie eine gültige IP-Adresse an.
`dns`	DNS-Hostnamen	Geben Sie den Hostnamen an.

Ergebnis

Die Adresse ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show openvpn remoteend` an.

11.6.4.6 show-context

Beschreibung

Dieser Befehl zeigt die verfügbaren OpenVPN-Gegenstellen an.

Voraussetzung

Sie befinden sich im OPENVPN REMOTE END-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn-rm-X)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show context
```

Ergebnis

Die Namen der OpenVPN-Gegenstellen werden aufgelistet.

11.6.5 Befehle im OPENVPN CONNECTION-Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im OPENVPN CONNECTION-Konfigurationsmodus aufrufen können.

Geben Sie im OPENVPN Konfigurationsmodus den Befehl `connection name` ein, um in diesen Modus zu wechseln.

- Wenn Sie den OPENVPN CONNECTION-Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im OPENVPN-Konfigurationsmodus.
- Wenn Sie den OPENVPN CONNECTION-Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

11.6.5.1 auth-algo

Beschreibung

Mit diesem Befehl legen Sie das Verfahren zum Berechnen der Prüfsumme fest.

Voraussetzung

Sie befinden sich im OPENVPN CONNECTION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn-conn-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
auth-algo {sha1|sha224|sha384|sha256|sha512|md5}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`sha1`	Secure Hash Algorithm 1	-
`sha224`	Secure Hash Algorithm 224	-
`sha384`	Secure Hash Algorithm 384	-
`sha256`	Secure Hash Algorithm 256	-
`sha512`	Secure Hash Algorithm 512	-
`md5`	Message Digit Algorithm 5	-

Ergebnis

Das Verfahren ist festgelegt.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show openvpn connections` an.

Sie zeigen die verfügbaren OpenVPN-Verbindungen mit dem Befehl `show auth-names` an.

11.6.5.2 authentication

Beschreibung

Mi diesem Befehl wechseln Sie in den OPENVPN AUTHENTICATION-Konfigurationsmodus.

Voraussetzung

Sie befinden sich im OPENVPN CONNECTION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn-conn-X)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
authentication
```

Ergebnis

Sie befinden sich jetzt im OPENVPN AUTHENTICATION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli((config-openvpn-conn-auth)#
```

Weitere Hinweise

Sie verlassen den OPENVPN AUTHENTICATION-Konfigurationsmodus mit dem Befehl `end` oder `exit`.

11.6.5.3 autoFW

Beschreibung

Mit diesem Befehl konfigurieren Sie die Einstellung Firewall der OpenVPN-Verbindung.

Voraussetzung

Sie befinden sich im OPENVPN CONNECTION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn-conn-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
autoFW {enabled|disabled}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
enabled	Für die OpenVPN-Verbindung werden automatisch die Firewall-Regeln angelegt.	-
disabled	Sie müssen selbst die geeigneten Firewall-Regeln anlegen.	-

Ergebnis

Die Einstellung ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show openvpn connections` an.

Sie zeigen die verfügbaren OpenVPN-Verbindungen mit dem Befehl `show auth-names` an.

11.6.5.4 encryp-algo

Beschreibung

Mit diesem Befehl konfigurieren Sie den Verschlüsselungsalgorithmus der OpenVPN-Verbindung.

Voraussetzung

Sie befinden sich im OPENVPN CONNECTION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn-conn-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
encryp-algo {bfcbc|aes128cbc|aes192cbc|aes256cbc|desed3}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung
bfcbc	Blowfish
aes128cbc	Advanced Encryption Standard mit 128 Bit
aes192cbc	Advanced Encryption Standard mit 192 Bit
aes256cbc	Advanced Encryption Standard mit 256 Bit
desede3	DES-EDE3: Data Encryption Standard 192 Bit Schlüsselläng

Ergebnis

Die Einstellung ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show openvpn connections` an.

Sie zeigen die verfügbaren OpenVPN-Verbindungen mit dem Befehl `show auth-names` an.

11.6.5.5 NAT

Beschreibung

Mit diesem Befehl konfigurieren Sie die Einstellung "IP-Masquerading".

Voraussetzung

Sie befinden sich im OPENVPN CONNECTION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn-conn-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
NAT {enabled|disabled}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`enabled`	Aktiviert die Einstellung "IP-Masquerading"	-
`disabled`	Deaktiviert die Einstellung "IP-Masquerading"	-

Ergebnis

Die Einstellung ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show openvpn connections` an.

Sie zeigen die verfügbaren OpenVPN-Verbindungen mit dem Befehl `show auth-names` an.

11.6.5.6 operation

Beschreibung

Mit diesem Befehl legen Sie fest, wie die Verbindung aufgebaut wird.

Voraussetzung

Sie befinden sich im OPENVPN CONNECTION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn-conn-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
operation {disabled|start|start-di|start-sms}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`disabled`	Die VPN-Verbindung ist deaktiviert.	Default
`start`	Das Gerät versucht, zu der Gegenstelle eine VPN-Verbindung aufzubauen.	-
`start-di`	Beim Eintreten des Ereignisses "Digital In" versucht das Gerät zu der Gegenstelle eine VPN-Verbindung aufzubauen. Vorausgesetzt, dass das Ereignis "Digital In" an die VPN-Verbindung weitergegeben wird.	-
`start-sms`	Nur bei M874, M876 Wenn das Gerät eine Befehl-SMS erhält, wartet das Gerät, bis der Verbindungsaufbau von der Gegenstelle initiiert wird. Vorausgesetzt, dass das Gerät eine Befehl-SMS der Klasse "System" von bestimmten Absendern akzeptiert.	-

Ergebnis

Die Einstellung ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show openvpn connections` an.

Sie zeigen die verfügbaren OpenVPN-Verbindungen mit dem Befehl `show auth-names` an.

11.6.5.7 LZO

Beschreibung

Mit diesem Befehl konfigurieren Sie die Einstellung LZO der OpenVPN-Verbindung.

Voraussetzung

Sie befinden sich im OPENVPN CONNECTION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn-conn-X)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
LZO {yes|no|adaptive}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`yes`	Die Daten werden mit dem LZO-Algorithmus komprimiert.	-
`no`	Die Daten werden nicht komprimiert.	-
`adaptive`	Adaptive Komprimierung, bei welcher der OpenVPN-Stack die Komprimierung regelmäßig überprüft. Wenn die Wirksamkeit der Komprimierung gering ist, wird die Komprimierung abgeschaltet und bei einer späteren Prüfung wieder aktiviert.	

Ergebnis

Die Einstellung ist konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show openvpn connections` an.

Sie zeigen die verfügbaren OpenVPN-Verbindungen mit dem Befehl `show auth-names` an.

11.6.5.8 no LZO

Beschreibung

Mit diesem Befehl deaktivieren Sie die Einstellung LZO der OpenVPN-Verbindung.

Voraussetzung

Sie befinden sich im OPENVPN CONNECTION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn-conn-X)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no LZO
```

Ergebnis

Die Einstellung LZO der OpenVPN-Verbindung ist deaktiviert.

Weitere Hinweise

Sie konfigurieren die Einstellung LZO der OpenVPN-Verbindung mit dem Befehl `LZO`.

11.6.5.9 show auth-names

Beschreibung

Dieser Befehl zeigt an, welches Verfahren zum Berechnen der Prüfsumme von welcher OpenVPN-Verbindung verwendet wird.

Voraussetzung

Sie befinden sich im OPENVPN CONNECTION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn-conn-X)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show auth-names
```

Ergebnis

Die Verwendung wird aufgelistet.

Weitere Hinweise

Sie legen eine OpenVPN-Verbindung mit dem Befehl `connection name` an.

11.6.5.10 show context

Beschreibung

Dieser Befehl zeigt die verfügbaren OpenVPN-Verbindungen an.

Voraussetzung

Sie befinden sich im OPENVPN CONNECTION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn-conn-X)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
show context
```

Ergebnis

Die Namen der OpenVPN-Verbindungen werden aufgelistet.

Weitere Hinweise

Sie legen eine OpenVPN-Verbindung mit dem Befehl `connection name` an.

11.6.6 Befehle im OPENVPN AUTHENTICATION-Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im OPENVPN AUTHENTICATION-Konfigurationsmodus aufrufen können.

Geben Sie im OPENVPN CONNECTION-Konfigurationsmodus den Befehl `authentication` ein, um in diesen Modus zu wechseln.

- Wenn Sie den OPENVPN AUTHENTICATION-Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im OPENVPN CONNECTION-Konfigurationsmodus.
- Wenn Sie den OPENVPN AUTHENTICATION-Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

11.6.6.1 auth

Beschreibung

Mit diesem Befehl legen Sie fest, dass für die Authentifizierung ein Zertifikat verwendet wird.

Voraussetzung

- Das entsprechende Zertifikat ist geladen.
- Sie befinden sich im OPENVPN AUTHENTICATION-Konfigurationsmodus.

  Die Eingabeaufforderung lautet:

  ```
  cli(config-openvpn-conn-auth)#
  ```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
auth cacert <name(255)> macert <name(255)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
-	Zertifikatsauswahl	• `cacert`: CA-Zertifikat • `macert`: Maschinenzertifikat
`name`	Name des CA- oder Maschinenzertifikat	Geben Sie den Zertifikatsnamen an.

Ergebnis

Das Zertifikat ist festgelegt.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show openvpn authentication` an.

Sie löschen die Authentifizierung mit dem Befehl `no auth`.

11.6.6.2 no auth

Beschreibung

Mit diesem Befehl löschen Sie das Authentifizierungsverfahren.

Voraussetzung

Sie befinden sich im OPENVPN AUTHENTICATION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn-conn-auth)#
```

Syntax

Rufen Sie den Befehl ohne Parametrierung auf:

```
no auth
```

Ergebnis

Das Authentifizierungsverfahren ist gelöscht.

11.6.6.3 auth user

Beschreibung

Mit diesem Befehl konfigurieren Sie den Benutzernamen und das Passwort für das CA-Zertifikat.

Voraussetzung

Sie befinden sich im OPENVPN AUTHENTICATION-Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-openvpn-conn-auth)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
auth cacert <string(255)> user <string(255)> pw <string(255)>
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`cacert`	Schlüsselwort für CA-Zertifikat	-
`string`	CA-Zertifikat	Geben Sie den Namen des CA-Zertifikats an. Maximal 255 Zeichen
`user`	Schlüsselwort für den Benutzernamen	-
`string`	Benutzernamen	Geben Sie den Benutzernamen an. Maximal 255 Zeichen
`pw`	Schlüsselwort für das Passwort	-
`string`	Passwort	Geben Sie das Passwort an. Maximal 255 Zeichen

Ergebnis

Die Benutzerdaten sind konfiguriert.

Weitere Hinweise

Sie zeigen diese Einstellung und weitere Informationen mit dem Befehl `show openvpn authentication` an.

Sie löschen die Authentifizierung mit dem Befehl `no auth`.

Diagnose 12

Die Überwachung des Systems und die Fehlerdiagnose erfolgen über verschiedene Wege:

- Events- und Faults-Handling:
  Vordefinierte Ereignisse erzeugen eine Meldung. Diese Meldungen können auf folgenden Wegen verbreitet werden:
  - Eintrag in lokale Logbücher
  - Übertragung zum Syslog-Server
  - Versand als SNMP-Trap
  - Aufleuchten der Fehler-LED
  - Schaltvorgang am digitalen Ausgang
- Syslog-Client:
  Konfiguriert die Übertragung zum Syslog-Server

12.1 Events- und Faults-Handling

Im Events- und Faults-Handling stellen Sie ein, welche Ereignisse bzw. deren Meldungen auf welchem Weg verbreitet werden.

Die Überwachung bestimmter Systemereignisse sowie von Stromversorgung und physikalischen Schnittstellen konfigurieren Sie im Events Konfigurationsmodus.

12.1.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

12.1.1.1 show events config

Beschreibung

Dieser Befehl zeigt die aktuelle Konfiguration für die Weiterleitung der Meldungen der verschiedenen Ereignistypen an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show events config
```

Ergebnis

Die aktuelle Konfiguration der Ereignisanzeige wird angezeigt.

12.1.1.2 show events severity

Beschreibung

Dieser Befehl zeigt an, ab welchem Schweregrad eines Ereignisses ("Info", "Warning" oder "Critical") eine bestimmte Benachrichtigung (Versand einer E-Mail, Eintrag in die Syslog-Tabelle, Eintrag in die Syslog-Datei) erfolgt.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show events severity
```

Ergebnis

Für jede Art der Benachrichtigung wird der zugehörige Schweregrad des Ereignisses angezeigt.

Weitere Hinweise

Sie konfigurieren die Zuordnung von Schweregrad eines Ereignisses und Art der Benachrichtigung mit dem Befehl `severity`.

12.1.1.3 show events faults config

Beschreibung

Dieser Befehl zeigt die aktuelle Konfiguration folgender Fehlerüberwachungen an:

- Überwachung der Stromversorgung auf Stromausfall
- Überwachung der Netzwerkverbindungen auf Änderung des Verbindungsstatus

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show events faults config [{power|link}]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung
`power`	Überwachung der Stromversorgung auf Stromausfall
`link`	Überwachung der Netzwerkverbindungen auf Änderung des Verbindungs-status

Wenn Sie keinen Parameter angeben, werden die Einstellungen für beide Fehlerüberwachungen angezeigt.

Ergebnis

Die aktuelle Konfiguration der ausgewählten Fehlerüberwachung wird angezeigt.

12.1.1.4 show events faults status

Beschreibung

Dieser Befehl zeigt die Statusmeldungen der Fehlerüberwachung von Stromversorgung und Netzwerkverbindungen an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show events faults status
```

Ergebnis

Eine Tabelle mit den Statusmeldungen der Fehlerüberwachung wird angezeigt.

12.1.1.5 show fault counter

Beschreibung

Dieser Befehl zeigt die Anzahl der Fehler seit dem letzten Hochlauf an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show fault counter
```

Ergebnis

Die Anzahl der Fehler wird angezeigt.

Weitere Hinweise

Sie setzen den Zähler für die Fehler mit dem Befehl `clear fault counter` zurück.

12.1.1.6 show fwlog

Beschreibung

Mit diesem Befehl zeigen Sie die Meldungen an, die an der Firewall eingetreten sind. Die Meldungen lassen sich nach Ereignisschwere filtern.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show fwlog [{ info | warning | critical }]
```

Parameter

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`info`	Information	-
`warning`	Warnmeldungen	-
`critical`	Kritische Meldungen	-

Wenn Sie den Befehl ohne Parametrierung aufrufen, werden alle Meldungen angezeigt.

Ergebnis

Der Inhalt des Firewall-Logbuchs wird angezeigt.

12.1.1.7 show logbook

Beschreibung

Mit diesem Befehl zeigen Sie den Inhalt des Logbuchs an. Die Logbucheinträge sind unterschiedlich kategorisiert.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show logbook
```

oder

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show logbook { info | warning | critical }
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung
`info`	Alle Logbucheinträge der Kategorien "Information", "Warnung" und "Kritisch" werden angezeigt.
`warning`	Alle Logbucheinträge der Kategorien "Warnung" und "Kritisch" werden angezeigt.
`critical`	Alle Logbucheinträge der Kategorie "Kritisch" werden angezeigt.

Ergebnis

Der Inhalt des Logbuchs wird angezeigt.

12.1.1.8 show power-line-state

Beschreibung

Dieser Befehl zeigt den Status der Stromversorgung an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show power-line-state
```

Ergebnis

Der Status der Stromversorgung wird angezeigt.

12.1.1.9 show seclog

Beschreibung

Mit diesem Befehl zeigen Sie die Meldungen an, die bei der Kommunikation über einen gesicherten VPN-Tunnel aufgetreten sind. Die Meldungen lassen sich nach Ereignisschwere filtern.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
show seclog [{ info | warning | critical }]
```

Parameter

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich / Anmerkung
`info`	Information	-
`warning`	Warnmeldungen	-
`critical`	Kritische Meldungen	-

Wenn Sie den Befehl ohne Parametrierung aufrufen, werden alle Meldungen angezeigt.

Ergebnis

Der Inhalt des Sicherheits-Logbuchs wird angezeigt.

12.1.2 clear fault counter

Beschreibung

Mit diesem Befehl setzen Sie den Zähler zurück, der die Anzahl der Fehler seit dem letzten Hochlauf anzeigt.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
clear fault counter
```

Ergebnis

Der Zähler steht auf "0".

Weitere Hinweise

Sie zeigen die Anzahl der Fehler seit dem letzten Hochlauf mit dem Befehl `show fault counter` an.

12.1.3 clear fwlog

Beschreibung

Mit diesem Befehl löschen Sie den Inhalt des Firewall-Logbuchs.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
clear fwlog
```

Ergebnis

Der Inhalt des Firewall-Logbuchs ist gelöscht.

12.1.4 clear logbook

Beschreibung

Mit diesem Befehl löschen Sie den Inhalt des Logbuchs.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
clear logbook
```

Ergebnis

Der Inhalt des Logbuchs ist gelöscht.

12.1.5 clear seclog

Beschreibung

Mit diesem Befehl löschen Sie den Inhalt des Sicherheits-Logbuchs.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
clear seclog
```

Ergebnis

Der Inhalt des Sicherheits-Logbuchs ist gelöscht.

12.1.6 fault report ack

Beschreibung

Manche Fehler lassen sich quittieren und damit aus der Fehlerliste entfernen, z. B. ein Fehler des Ereignisses "Kalt-/Warmstart".

Mit diesem Befehl können Sie diese Fehler quittieren bzw. aus der Fehlerliste entfernen.

Voraussetzung

Sie befinden sich im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

```
cli#
```

Syntax

Rufen Sie den Befehl mit folgendem Parameter auf:

```
fault report ack <fault-state-id>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertbereich/Anmerkung
`fault-state-id`	ID des Fehlers	Geben Sie die ID des Fehlers ein. Die ID ermitteln Sie mit dem Befehl "`show events faults status`".

Ergebnis

Der Fehler ist quittiert und aus der Fehlerliste entfernt.

12.1.7 no logging console

Beschreibung

Mit diesem Befehl deaktivieren Sie das Mitschreiben von Ein- und Ausgaben auf die Konsole.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
no logging console
```

Ergebnis

Die Funktion zum Mitschreiben auf der Konsole ist deaktiviert.

Weitere Hinweise

Sie aktivieren die Einstellung mit dem Befehl `logging console`.

Der Defaultwert der Funktion ist "deaktiviert".

12.1.8 logging console

Beschreibung

Mit diesem Befehl aktivieren Sie das Mitschreiben von Ein- und Ausgaben auf die Konsole.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
logging console
```

Ergebnis

Die Funktion Mitschreiben auf der Konsole ist aktiviert.

Weitere Hinweise

Sie deaktivieren die Einstellung mit dem Befehl `no logging console`.

Der Defaultwert der Funktion ist "deaktiviert".

12.1.9 Befehle im globalen Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im globalen Konfigurationsmodus aufrufen können.

Geben Sie im Privileged EXEC Modus den Befehl `configure terminal` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

Sie verlassen den globalen Konfigurationsmodus mit dem Befehl `end` oder `exit` und befinden sich dann wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im globalen Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

12.1.9.1 events

Beschreibung

Mit diesem Befehl wechseln Sie in den EVENTS Konfigurationsmodus.

Voraussetzung

Sie befinden sich im globalen Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
events
```

Ergebnis

Sie befinden sich jetzt im EVENTS Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-events)#
```

Weitere Hinweise

Sie verlassen den EVENTS Konfigurationsmodus mit dem Befehl `end` oder `exit`.

12.1.10 Befehle im Events Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im EVENTS Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl `events` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

- Wenn Sie den EVENTS Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den EVENTS Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im EVENTS Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

12.1.10.1 add log

Beschreibung

Mit diesem Befehl erstellen Sie einen Eintrag im Logbuch.

Voraussetzung

Sie befinden sich im EVENTS Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-events)#
```

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
add log <log-entry>
```

Dabei hat der Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
log-entry	Eintrag in das Logbuch	max. 150 Zeichen

Ergebnis

Der Eintrag in das Logbuch ist erfolgt.

12.1.10.2 client config

Beschreibung

Mit diesem Befehl aktivieren Sie einen der Clients, welche die Meldungen des Geräts bearbeiten bzw. weiterleiten.

Folgende Clients stehen zur Verfügung:

- `syslog`: sendet die Meldungen an den Syslog-Server
- `trap`: sendet die Meldungen als SNMP-Trap an einen konfigurierten Empfänger
- `email`: versendet die Meldungen als E-Mail

Voraussetzung

Sie befinden sich im EVENTS Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-events)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
client config {syslog|trap|email|all}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung
syslog	aktiviert den Client, der die Meldungen zum Syslog-Server überträgt
trap	aktiviert den Client, der die SNMP-Traps überträgt
email	aktiviert den Client, der die E-Mails überträgt
all	aktiviert alle Clients zugleich

Ergebnis

Die Funktion des ausgewählten Client für die Übertragung ist aktiviert.

Weitere Hinweise

Sie zeigen den Status der Events und der Clients mit dem Befehl `show events config` an.

Sie deaktivieren einen Client mit dem Befehl `no client config`.

12.1.10.3 no client config

Beschreibung

Mit diesem Befehl deaktivieren Sie einen der Clients, welche die Meldungen des Geräts bearbeiten bzw. weiterleiten.

Voraussetzung

Sie befinden sich im EVENTS Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-events)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no client config {syslog|trap|email|all}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung
`syslog`	deaktiviert den Client, der die Meldungen zum Syslog-Server überträgt
`trap`	deaktiviert den Client, der die SNMP-Traps überträgt
`email`	deaktiviert den Client, der die E-Mails überträgt
`all`	deaktiviert alle Clients zugleich

Ergebnis

Der ausgewählte Client für die Übertragung ist deaktiviert.

Weitere Hinweise

Sie zeigen den Status der Events und der Clients mit dem Befehl `show events config` an.

Sie aktivieren die Funktion mit dem Befehl `client config`.

12.1.10.4 event config

Beschreibung

Mit diesem Befehl konfigurieren Sie, welcher der verschiedenen Meldungstypen des Geräts gespeichert oder verschickt werden soll.

Folgende Events bzw. Meldungstypen stehen zur Verfügung:

- Meldung bei Kalt- oder Warmstart
- Meldung bei Statusänderung einer physikalischen Schnittstelle
- Meldung bei fehlerhafter Anmeldung
- Meldung bei Statusänderung der Stromversorgung
- Meldung bei Statusänderung der Fehlerüberwachung
- Meldung beim Anwenden von VPN
- Meldung beim Anwenden der Firewallregeln
- Meldung beim Ändern des Verbindungsstatus
- Meldung beim Verbindungsaufbau und bei Änderung der Konfiguration
- Meldung bei Statusänderung des digitalen Eingangs.
- Meldung bei Fehler im Zusammenhang mit Secure NTP
- Meldung bei persistenter Speicherung der Konfiguration
- Meldung bei einem nicht konfigurierbaren Eintrag in der Log-Tabelle

Diese Meldungen können von den Clients auf verschiedene Weise bearbeitet werden:

- Eintrag in das Logbuch des Geräts
- Senden der Meldung an den Syslog Server des Systems
- Versenden einer E-Mail
- Senden einer SNMP Trap
- Aufleuchten der Fehler-LED
- Schaltvorgang am digitalen Ausgang

Voraussetzung

Sie befinden sich im EVENTS Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-events)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
event config { cold-warmstart | linkchange | authentication-failure | faultstate-
change | security-log | firewall-log | ddns-client-log | system-general-log | system-
```

```
connection-status | digital-in | vpn-tunnel | secure-ntp | config-change| service-
information | all} {logtable | syslog | email | trap | faults | sms | digital-out |
vpn-tunnel | all}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung
`cold-warmstart`	Meldung bei Kalt- oder Warmstart
`linkchange`	Meldung bei Statusänderung eine physikalischen Schnittstelle
`authentication-failure`	Meldung beim fehlerhafter Anmeldung
`faultstate-change`	Meldung bei Statusänderung der Fehlerüberwachung
`security-log`	Meldung beim Anwenden von IPsec
`firewall-log`	Meldung beim Anwenden einer Firewallregel
`ddns-client-log`	Meldung bein Synchronisieren des DDNS-Clients mit dem im DDNS-Provider registrierten Hostnamen
`system-general-log`	Meldung bei Verbindungsaufbau und bei Änderung der Konfiguration
`system-connection-status`	Meldung bei Statusänderung der Verbindung
`digital-in`	Meldung bei Änderung des digitalen Eingangs
`vpn-tunnel`	Meldung bei Änderung von VPN (IPsec, OpenVPN, SINEMA RC)
`secure-ntp`	Meldung, wenn das Gerät die Systemzeit von einem gesicherten NTP-Server erhält.
`config-change`	Meldung bei persistenter Speicherung der Konfiguration
`service-information`	Meldung bei einem nicht konfigurierbaren Eintrag in der Log-Tabelle
`all`	Alle Meldungen
`logtable`	Client, der die Logbuch-Einträge bearbeitet
`syslog`	Client, der die Meldungen zum Sylog-Server überträgt
`email`	Client, der die E-Mails überträgt
`trap`	Client, der die SNMP Traps überträgt
`faults`	Fehler LED leuchtet auf. Die Einstellung ist nur bei Kalt- oder Warmstart möglich.
`digital-out`	Steuert den digitalen Ausgang an oder signalisiert die Zustandsänderung mit der LED "DO".
`firewall`	Führt den benutzerdefinierten Regelsatz aus.
`vpn-tunnel`	Steuert die VPN-Verbindung (Aufbau/ Abbau)
`all`	alle Clients zugleich

Ergebnis

Die Einstellung, welche Meldung des Geräts gespeichert oder verschickt werden soll, ist konfiguriert.

Weitere Hinweise

Sie zeigen den Status der Events und der Clients mit dem Befehl `show events config` an.

Sie löschen Einstellungen mit dem Befehl `no event config`.

Die Clients werden mit diesem Befehl nicht aktiviert.

Verwenden Sie zum Aktivieren der Clients den Befehl `client config`.

Hinweis

Ändern von mehreren Meldungstypen oder Clients

Sie können bei einem Befehlsaufruf nur einen Meldungstyp und einen Client auswählen.

Wenn Sie mehrere Meldungstypen oder Clients bearbeiten wollen, kann es günstiger sein, zunächst die Option `all` zu wählen und danach einzelne Elemente zu deaktivieren.

12.1.10.5 no event config

Beschreibung

Mit diesem Befehl konfigurieren Sie, welcher der verschiedenen Meldungstypen des Geräts nicht mehr gespeichert oder verschickt werden soll.

Voraussetzung

Sie befinden sich im EVENTS Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-events)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no event config { cold-warmstart | linkchange | authentication-failure | faultstate-
change | security-log | firewall-log | ddns-client-log | system-general-log | system-
connection-status | digital-in | vpn-tunnel | secure-ntp | config-change | service-
information | all} {logtable | syslog | email | trap | faults | sms | digital-out |
vpn-tunnel | fiewall | all}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung
`cold-warmstart`	Meldung bei Kalt- oder Warmstart
`linkchange`	Meldung bei Statusänderung eine physikalischen Schnittstelle
`authentication-failure`	Meldung beim fehlerhafter Anmeldung
`faultstate-change`	Meldung bei Statusänderung der Fehlerüberwachung
`security-log`	Meldung beim Anwenden von IPsec
`firewall-log`	Meldung beim Anwenden einer Firewallregel
`ddns-client-log`	Meldung bein Synchronisieren des DDNS-Clients mit dem im DDNS-Provider registrierten Hostnamen

Parameter	Beschreibung
`system-general-log`	Meldung bei Verbindungsaufbau und bei Änderung der Konfiguration
`system-connection-status`	Meldung bei Statusänderung der Verbindung
`digital-in`	Meldung bei Änderung des digitalen Eingangs
`vpn-tunnel`	Meldung bei Änderung von VPN (IPsec, OpenVPN, SINEMA RC)
`secure-ntp`	Meldung, wenn das Gerät die Systemzeit von einem gesicherten NTP-Server erhält.
`config-change`	Meldung bei persistenter Speicherung der Konfiguration
`service-information`	Meldung bei einem nicht konfigurierbaren Eintrag in der Log-Tabelle
`all`	Alle Meldungen
`logtable`	Client, der die Logbuch-Einträge bearbeitet
`syslog`	Client, der die Meldungen zum Sylog-Server überträgt
`email`	Client, der die E-Mails überträgt
`trap`	Client, der die SNMP Traps überträgt
`faults`	Fehler LED leuchtet auf. Die Einstellung ist nur bei Kalt- oder Warmstart möglich.
`digital-out`	Steuert den digitalen Ausgang an oder signalisiert die Zustandsänderung mit der LED "DO".
`vpn-tunnel`	Steuert die VPN-Verbindung (Aufbau/ Abbau)
`firewall`	Führt den benutzerdefinierten Regelsatz aus.
`all`	alle Clients zugleich

Ergebnis

Die Einstellung, welche Meldungen des Gerätes nicht gespeichert oder verschickt werden soll, ist konfiguriert.

Weitere Hinweise

Sie zeigen den Status der Events und der Clients mit dem Befehl `show events config` an.

Sie konfigurieren, welcher der verschiedenen Meldungstypen des Geräts gespeichert oder verschickt werden soll, mit dem Befehl `event config`.

12.1.10.6 link

Beschreibung

Mit diesem Befehl konfigurieren und aktivieren Sie die Überwachung der physikalischen Netzwerkverbindungen auf Kabelbruch bzw. Ziehen oder Einstecken des Steckers.

Voraussetzung

Sie befinden sich im EVENTS Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-events)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
link {up|down}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`up`	nur das Herstellen einer Verbindung wird gemeldet	-
`down`	nur das Trennen einer Verbindung wird gemeldet	-

Ergebnis

Die Einstellungen zur Überwachung der physikalischen Netzwerkverbindungen sind konfiguriert.

Weitere Hinweise

Die Anzeige der aktuellen Einstellung rufen Sie mit dem Befehl `show events faults config` auf.

Sie deaktivieren die Funktion mit dem Befehl `no link`.

12.1.10.7 no link

Beschreibung

Mit diesem Befehl deaktivieren Sie die Überwachung der physikalischen Netzwerkverbindungen auf Kabelbruch bzw. Ziehen oder Einstecken des Steckers.

Voraussetzung

Sie befinden sich im EVENTS Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli(config-events)#
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no link {up|down}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`up`	Die Meldung beim Herstellen einer Verbindung wird deaktiviert	-
`down`	Die Meldung beim Trennen einer Verbindung wird deaktiviert	-

Ergebnis

Die Einstellungen zur Überwachung der physikalischen Netzwerkverbindungen sind konfiguriert.

Weitere Hinweise

Die Anzeige der aktuellen Einstellung rufen Sie mit dem Befehl `show events faults config` auf.

Sie aktivieren die Funktion mit dem Befehl `link`.

12.1.10.8 severity

Beschreibung

Mit diesem Befehl konfigurieren Sie die Schwellenwertstufen für das Versenden von Systemereignisbenachrichtigungen.

Voraussetzung

Sie befinden sich im EVENTS Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli (config-events) #
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
severity {mail | log | syslog } {info | warning | critical }
```

Dabei haben die Parameter folgende Bedeutung:

Beispiel

Parameter	Beschreibung	Wertebereich / Anmerkung
`mail`	Legt den Schwellwert für den Versand der Systemereignismeldungen per E-Mail fest.	-
`log`	Legt den Schwellwert für das Eintragen der Systemereignismeldungen in die Log-Tabelle fest.	Defaultwert

Parameter	Beschreibung	Wertebereich / Anmerkung
`syslog`	Legt den Schwellwert für das Eintragen der Systemereignismeldungen in die Syslog-Datei fest.	-
`info`	Die Meldungen aller Stufen werden versendet bzw. protokolliert.	Die Meldungen aller Stufen werden versendet bzw. protokolliert-
`warning`	Die Meldung dieser Stufe und der Stufe "critical" werden versendet bzw. protokolliert	-
`critical`	Nur die Meldungen dieser Stufe werden versendet bzw. protokolliert.	-

Ergebnis

Die Einstellungen sind konfiguriert.

Die Funktion severity ist aktiviert.

Weitere Hinweise

Sie deaktivieren die Einstellung mit dem Befehl `no severity`.

Sie zeigen den Status dieser Funktion und weitere Informationen `show events config` an

12.1.10.9 no severity

Beschreibung

Mit diesem Befehl deaktivieren Sie die Einstellung der Schwellenwertstufen für das Versenden von Systemereignisbenachrichtigungen.

Voraussetzung

Sie befinden sich im EVENTS Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli (config-events) #
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
no severity { mail | log | syslog }
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`mail`	Die Einstellung des Schwellwerts für den Versand der Systemereignismeldungen per E-Mail wird deaktiviert.	-
`log`	Die Einstellung des Schwellwerts für den Eintrag der Systemereignismeldungen in die Log-Tabelle wird deaktiviert.	-
`syslog`	Die Einstellung des Schwellwerts für den Eintrag der Systemereignismeldungen in die Syslog-Datei wird deaktiviert.	-

Wenn Sie keinen Parameter aus der Parameterliste auswählen, wird der voreingestellte Wert verwendet.

Ergebnis

Die Einstellungen zur Versendung von Systemereignismeldungen sind konfiguriert.

Weitere Hinweise

Sie aktivieren die Einstellung mit dem Befehl `severity`.

Sie zeigen den Status dieser Funktion und weitere Informationen `show events severity` an.

12.2 Syslog Client

Mit den Befehlen dieses Kapitels werden folgende Einstellungen konfiguriert:

- Übertragung der Meldungen zum Syslog-Server
- Lokales Puffern und Speichern von Meldungen
- Annehmen und Weiterleiten von Meldungen von anderen Geräten (Relay-Betrieb)

12.2.1 Die "show"-Befehle

In diesem Kapitel werden Befehle beschrieben, mit denen Sie verschiedene Einstellungen anzeigen.

Mit dem `do [Befehl]` können Sie die Befehle aus dem Privileged EXEC Modus in jedem Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

12.2.1.1 show events syslogserver

Beschreibung

Dieser Befehl zeigt die Einträge der konfigurierten Syslog-Server an.

Voraussetzung

Sie befinden sich im User EXEC Modus oder im Privileged EXEC Modus.

Die Eingabeaufforderung lautet:

`cli>` oder `cli#`

Syntax

Rufen Sie den Befehl ohne Parameter auf:

```
show events syslogserver
```

Ergebnis

Die Einträge der konfigurierten Syslog-Server werden angezeigt.

12.2.2 Befehle im Events Konfigurationsmodus

In diesem Kapitel werden Befehle beschrieben, die Sie im EVENTS Konfigurationsmodus aufrufen können.

Geben Sie im globalen Konfigurationsmodus den Befehl `events` ein, um in diesen Modus zu wechseln.

Befehle zu anderen Themen, die im globalen Konfigurationsmodus aufgerufen werden, finden Sie in den jeweiligen Kapiteln an entsprechender Stelle.

- Wenn Sie den EVENTS Konfigurationsmodus mit dem Befehl `exit` verlassen, dann befinden Sie sich wieder im globalen Konfigurationsmodus.
- Wenn Sie den EVENTS Konfigurationsmodus mit dem Befehl `end` verlassen, dann befinden Sie sich wieder im Privileged EXEC Modus.

Befehle aus dem Privileged EXEC Modus können Sie mit dem `do [Befehl]` im EVENTS Konfigurationsmodus ausführen.

Dabei ersetzen Sie `[Befehl]` durch den Befehl, den Sie ausführen wollen.

12.2.2.1 syslogserver

Beschreibung

Mit diesem Befehl konfigurieren Sie die Syslog-Server-Adresse.

Voraussetzung

Sie befinden sich im EVENTS Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli (config-events) #
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
syslogserver {ipv4 <ucast_addr> | fqdn-name <FQDN>} [<port(1-65535)>]
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ipv4`	Schlüsselwort für eine IP-Adresse	-
`ucast_addr`	IPv4-Adresse des Syslog-Servers	Geben Sie eine gültige IPv4-Adresse an.
`fqdn-name`	Schlüsselwort für einen Domainnamen	-
`FQDN`	Domainname (Fully Qualified Domain Name)	Maximal 100 Zeichen
`port`	Serverport	1 .. 65535 Default: 514

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Wenn Sie keinen Parameter aus der Parameterliste auswählen, wird der voreingestellte Wert verwendet.

Ergebnis

Die Einstellungen für den Syslog-Server sind konfiguriert.

Weitere Hinweise

Sie deaktivieren die Einstellung mit dem Befehl `no syslogserver`.

Sie zeigen den Status dieser Funktion und weitere Informationen mit dem Befehl `show events config` an.

12.2.2.2 no syslogserver

Beschreibung

Mit diesem Befehl konfigurieren Sie die Syslog-Server-Adresse.

Voraussetzung

Sie befinden sich im EVENTS Konfigurationsmodus.

Die Eingabeaufforderung lautet:

```
cli (config-events) #
```

Syntax

Rufen Sie den Befehl mit folgender Parametrierung auf:

```
syslogserver {ipv4 <ucast_addr> | fqdn-name <FQDN>}
```

Dabei haben die Parameter folgende Bedeutung:

Parameter	Beschreibung	Wertebereich/Anmerkung
`ipv4`	Schlüsselwort für eine IP-Adresse	-
`ucast_addr`	IPv4-Adresse des Syslog-Servers	Geben Sie eine gültige IPv4-Adresse an.
`fqdn-name`	Schlüsselwort für einen Domainnamen	-
`FQDN`	Domainname (Fully Qualified Domain Name)	Maximal 100 Zeichen

Zur Bezeichnung von Adressen und Schnittstellen beachten Sie das Kapitel "Schnittstellenbezeichnungen und Adressen (Seite 42)".

Ergebnis

Die Einstellungen für den Syslog-Server sind deaktiviert.

Weitere Hinweise

Sie aktivieren die Einstellung mit dem Befehl `syslogserver`.

Sie zeigen den Status dieser Funktion und weitere Informationen mit dem Befehl `show events config` an.

Index

A

add log, 623
addr, 149, 538
addr-mode, 539
Adresse des Netzübergangs, 46
aggressive, 558
    no aggressive, 558
alias, 82
    no alias, 83
auth, 608
    no auth, 609
auth cacert, 551
    no auth, 554
auth psk
    no auth, 554
auth psk, 552
auth remcert, 553
    no auth, 554
auth user, 609
    no auth, 609
auth username
    no auth username, 373
auth usernamet, 372
auth-algo, 600
authentication, 544, 601
autoenrollment interval, 150
autoFW, 601
autofwnat, 151
    no autofwnat, 153
auto-fwrules, 569
    no auto-fwrules, 570
auto-save, 112
    no auto-save, 113

B

base bridge mode, 199

C

cacert, 583
cachenxdomain, 311
    no cachenxdomain, 312
certificate, 580
change password, 448
clear counters, 68
clear fault counter, 618
clear fwlog, 618
clear history, 56
clear line vty, 69
clear logbook, 619
clear screen, 47
clear seclog, 619
clear spanning-tree counters, 250
clear spanning-tree detected protocols, 249
clear vrrp3 statistics, 391
CLI-Befehle
    Symbolik Darstellung, 40
cli-console-timeout, 78
    no cli-console-timeout, 79
configure terminal, 69
connection, 595
connection name, 530, 590
    no conn name, 591
    no connection all, 532
    no connection name, 531
connection type, 152
conn-mode, 540
coordinates height, 73
coordinates latitude, 74
coordinates longitude, 75
crl-policy, 530

D

das delete, 119
das discover interface, 115
das mac blink, 118
das mac ip, 117
das mac name, 116
dcp forwarding, 274
dcp server, 266
    no dcp server, 267
ddnsclient, 306
default-ciphers, 559, 571
    no default-ciphers, 560, 572
del (Certificate), 584
delete, 96
device id, 154
device pw, 155
digital output close, 134
digital output open, 135
di-input set address, 471

di-input set ruleset, 472
di-input show-idx, 473
disable, 70
dnsclient, 305
dnsproxy, 306
do, 48
dpd, 561
    no dpd, 562
dpd-period, 562
dpd-timeout, 563
duplex, 83
    no duplex, 84

E

enable, 71
encryp-algo, 602
esp-auth, 573
esp-encryption, 574
esp-keyderivation, 575
event config, 626
    no event config, 628
events, 622
exit, 50

F

factoryclean, 127
fault report ack, 620
firewall, 357, 468
firewallnat, 416
firmware-on-plug, 126
    no firmware-on-plug, 127
flowcontrol, 385
forced disconnect, 230
forced disconnect time, 231

G

Glossar, 4
grep, 53
Gültigkeitsbereich, 3

H

help, 51

I

icmp name
    no icmp, 475
icmp name set type, 476
icmp name type, 473
icmp show-names, 477
icmp show-types-codes, 477
idle timeout icmp, 478
idle timeout tcp, 479
idle timeout udp, 479
ike-auth, 564
ike-encryption, 565
ike-keyderivation, 566
ike-keytries, 567
ike-lifetime, 568
interface, 76
    no interface, 77
interface (VRRP3), 396
    no interface, 397
interface ppp, 229
interface range, 200
    no interface range, 201
interface vlan, 232
interval, 145
ip address, 220, 233, 233, 275, 276
    no ip address, 234, 277
ip dhcp client mode, 282, 283
ip dhcp config-file-request, 281
    no ip dhcp config-file-request, 282
ip dhcp-server, 287
    no ip dhcp-server, 288
ip dhcp-server icmp-probe, 289
    no ip dhcp-server icmp-probe, 288
ip dhcp-server pool
    no ip dhcp-server pool, 291
ip dhcp-server pool, 290
ip echo-reply, 267
    no ip echo-reply, 268
ip http, 351, 354
    no ip http, 351
ip http https redirection, 355
ip route, 269
    no ip route, 270
ip routing, 271
ipsec, 529
ipsec connection show-idx, 417
IPv4
    Notation, 45
IPv4-Adresse, 45
ipv4rule, 480, 486
    no ipv4rule, 484
ipv4rule ipsec connection, 494

ipv4rule set, 493
ipv4rule set action, 483, 484
ipv4rule set dstip, 485
ipv4rule set log, 487
ipv4rule set prior, 488
ipv4rule set ruleset, 489
ipv4rule set service, 490
ipv4rule set srcip, 492
ipv4rule show interfaces, 494
ipv4rule show-rules, 495
ipv6 unicast-routing, 271

K

k-proto, 544

L

lease-time, 292
lifebyte, 576
lifetime, 577
link, 629
    no link, 630
lldp, 85
    no lldp, 86
load tftp, 93
loadsave, 95
local-id, 554
    no local-id, 555
loc-subnet, 545
login authentication, 439
loginpage, 450
logon, 139
    no logon, 139
logon idx authority, 140
logon idx fragment, 141
logon idx path, 142
logon idx query, 142
logon show-idx, 143
logout, 71
LZO, 605

M

mac-address-table aging, 388
    no mac-address-table aging, 389
mac-address-table aging-time, 390
manual srv, 307
    no manual srv, 308
map protocol, 202
    no map protocol, 203
masquerading, 418
    no masquerading, 419
masquerading show-idx, 418
mtu, 209

N

name, 222
    no name, 223
napt show-idx, 420
napt type ipv4, 421
    no napt, 422
    no napt all, 423
NAT, 603
nat-keep-alive, 533
negotiation, 87
    no negotiation, 88
netmap destination type ipv4, 424
    no netmap, 429
    no netmap all, 430
netmap show-idx, 426
netmap source type ipv4, 427
    no netmap, 429
    no netmap all, 430
network, 293
no ip address, 221
no login authentication, 440
no LZO, 606
no passive-listening, 242
no passive-listening bpdu-vlan-flood, 241
no role, 453
no sinema, 122
no snmp filterprofile, 335
no user-account-ext, 459
no user-group, 461
ntp, 173
ntp secure, 177
    no ntp secure, 177
ntp server, 180
    no ntp server, 180
ntp server id, 174
    no ntp server id, 175
ntp server interface, 181
    no ntp server interface, 183
ntp server secure, 176
ntp server secure interface, 184
    no ntp server secure interface, 185
ntp time diff, 178

O

openvpn, 589
operation, 546, 604
option, 294
    no option, 297
option value-hex, 295
option value-string, 296
    no option, 297, 297

P

panel-button control-restart, 163
    no panel-button-restart, 164
passive-listening, 241
passive-listening bpdu-vlan-flood, 240
passphrase, 585
passphrase show-idx, 586
password, 104, 235, 317
    no password, 106
password policy, 451
phase, 547
ping, 72
plug, 124
pool-enable, 298
    no pool-enable, 299
port, 156, 373, 578, 596
    no port, 374
ports, 224
    no ports, 225
prerule all ipv4, 496
prerule cloudconnector ipv4, 497
prerule dhcp ipv4, 498
prerule dns ipv4, 499
prerule http ipv4, 500
prerule https ipv4, 501
prerule ipsec ipv4, 502
prerule ipv4 show-int, 503
prerule ping ipv4, 503
prerule snmpm ipv4, 504
prerule ssh ipv4, 505
prerule systime ipv4, 506
prerule telnet ipv4, 507
presetplug, 125
proto, 579, 596
proto name, 508
    no proto, 509
proto show-names, 510
protocol-vlan, 205
    no protocol-vlan, 204
proxy, 156, 597
    no proxy, 157
proxyserver, 357

R

radius authorization-mode, 441
radius-server, 442
    no radius-server, 444
receiver-address, 375
    no receiver-address, 375
rem-id, 556
rem-id
    no rem-id, 557
remote name, 592
    no remote, 593
remote-addr, 598
remote-end name, 534
    no remote-end all, 536
    no remote-end name, 535
restart, 107
rmend name, 548
role, 445, 451
router vrrp3, 394
    no router vrrp3, 395
ruleset
    no ruleset, 513
ruleset name, 512
ruleset show-idx, 513
rulset idx, 511

S

save filetype, 94
security, 376
    no security, 377
send test mail, 369
sender-address, 378
    no sender-address, 378
serv name
    no srv, 359
server type, 309
service, 314
    no service, 315
Service & Support, 4
service name, 514
    no service, 516
service name set dst, 517
service name set prot, 518
service name set src, 519
service show-names, 520
set-interface, 300

severity, 631
no severity, 632
sftp filename, 100
sftp load, 101
sftp save, 102
sftp server, 103
show auth-names, 606
show cli-console-timeout, 59
show context, 599, 607
show coordinates, 60
show das info, 114
show dcp forwarding, 262
show dcp server, 263
show ddnsclient overview, 304
show device information, 60
show digital input, 132
show digital output, 133
show dnsclient information, 304
show dst info, 165
show events config, 612
show events faults config, 613
show events faults status, 614
show events sender email, 368
show events severity, 612
show events smtp-port, 368
show events smtp-server, 367
show events syslogserver, 634
show fault counter, 614
show firewall icmp-services ipv4, 464
show firewall information, 465
show firewall ip-protocols, 465
show firewall ip-rules ipv4, 466
show firewall ip-services, 466
show firewall pre-rules ipv4, 467
show firewall ruleset, 467
show firewall ruleset assignment, 468
show firewallnat masquerading, 413
show firewallnat napt, 414
show firewallnat netmap, 414
show firewallnat src-nat, 415
show flow-control, 383
show fwlog, 615
show history, 57
show im, 62
show interface mtu, 63
show interfaces, 61
show interfaces ... counters, 64
show ip arp, 278
show ip dhcp client, 280
show ip dhcp server pools, 286
show ip dhcp-server bindings, 285
show ip dns, 261
show ip http secure server status, 353
show ip http server status, 350
show ip interface, 66
show ip route, 263
show ip routing, 264
show ip ssh, 380
show ip static route, 264
show ip telnet, 265
show ipsec conn-authentication, 525
show ipsec connections, 526
show ipsec conn-phase1, 526
show ipsec conn-phase2, 527
show ipsec information, 527
show ipsec remoteend, 528
show lldp neighbors, 65
show lldp status, 65
show loadsave files, 91
show loadsave sftp, 92
show loadsave tftp, 92
show logbook, 616
show mac-address-table aging-status, 387
show mac-address-table aging-time, 386
show ntp info, 172
show ntp server info, 179
show openvpn authentication, 587
show openvpn connections, 588
show openvpn remoteend, 588
show passive-listening, 239
show password-policy, 445
show plug, 123
show power-line-state, 616
show ppp information, 228
show proxyserver table, 356
show radius server, 438
show radius statistics, 438
show running-config, 109
show seclog, 617
show sinema, 120
show sinemarc, 147
show snmp, 320
show snmp community, 320
show snmp engineID, 321
show snmp filter, 321
show snmp group, 322
show snmp group access, 322
show snmp inform statistics, 323
show snmp notif, 323
show snmp targetaddr, 324
show snmp targetparam, 324
show snmp tcp, 325
show snmp user, 326
show snmp viewtree, 326

show sntp broadcast-mode status, 186
show sntp status, 187
show sntp unicast-mode status, 187
show spanning-tree, 243
show spanning-tree active, 244
show spanning-tree bridge, 245
show spanning-tree detail, 246
show spanning-tree interface, 246
show spanning-tree interface layer2-gateway-port, 247
show spanning-tree root, 248
show srs, 136
show srs overview, 137
show ssl server-cert, 353
show time, 166
show user-accounts, 446
show user-groups, 447
show users, 448
show versions, 67
show vlan, 195
show vlan device info, 196
show vlan learning params, 196
show vlan port config, 197
show vlan protocols-group, 198
show vrrp3, 392
show vrrp3 interface, 393
show vrrp3 track, 393
show web-session-timeout, 129
show-idx, 581
show-info (Certificate), 582
shutdown
    no shutdown (DNS Proxy), 313
    no shutdown (DNS-Client), 310
    no shutdown (Firewall), 521
    no shutdown (IPsec), 537
    no shutdown (OpenVPN), 594
    no shutdown (PPP), 237
    no shutdown (SINEMA RC), 159
    no shutdown (SRS), 144
    shutdown (DNS Proxy), 313
    shutdown (DNS-Client), 310
    shutdown (Firewall), 520
    shutdown (IPsec), 536
    shutdown (OpenVPN), 593
    shutdown (PPP), 236
    shutdown (SINEMA RC), 158
    shutdown (SRS), 144
shutdown complete, 88, 210
    no shutdown, 89, 210
SIMATIC NET-Glossar, 4
SIMATIC NET-Handbuch, 4
sinema, 121
sinemarc, 148
smtp-server
    no smtp-server, 371
snmp
    client config, 624
    no client config, 625
snmp access, 329
    no snmp access, 331
snmp agent version, 328
snmp community index, 332
    no snmp community index, 333
snmp filterprofile, 334
snmp group, 336
    no snmp group, 337
snmp notify, 338
    no snmp notify, 339
snmp targetaddr, 339
    no snmp targetaddr, 341
snmp targetparams, 342
    no snmp targetparams, 344
snmp user, 346
    no snmp user, 347
snmp v1-v2 readonly, 344
    no snmp v1-v2 readonly, 345
snmp view, 347
    no snmp view, 349
snmpagent, 327
    no snmpagent, 328
sntp, 188
sntp client addressing-mode, 192
sntp time diff, 189
sntp unicast-server, 190
    no sntp unicast-server, 191
spanning-tree, 251
    no spanning-tree, 251
spanning-tree (Eigenschaften), 255
    no spanning-tree, 257
spanning-tree (Zeiteinstellungen), 252
    no spanning-tree, 254
spanning-tree auto-edge, 258
    no spanning-tree auto-edge, 259
speed, 90
src-nat show-idx, 431
src-nat type ipv4, 432
    no src-nat, 434
    no src-nat all, 434
srs, 137
srv name, 358
srv name addr, 360
srv name auth, 361
srv name port, 362
srv name pw, 363
srv name type, 364

srv name user, 364
srv show-names, 366
ssh-server, 381
    no ssh-server, 382
static-lease, 301
    no static-lease, 302
subnet, 541
subnet-vlan, 205
    no subnet-vlan, 206
Subnetzmaske, 45
switchport acceptable-frame-type, 211
    no switchport acceptable-frame-type, 212
switchport ingress-filter, 213
    no switchport ingress-filter, 213
switchport mode, 214
    no switchport mode, 216
switchport priority default, 216
    no switchport priority default, 217
switchport pvid, 218
    no switchport pvid, 219
syslogserver, 636
    no syslogserver, 637
system contact, 80
system location, 80
system name, 81

T

telnet-server, 272
    no telnet-server, 273
test, 379
tftp filename, 97
tftp load, 98
tftp save, 99
tftp server, 100
    laden, 93
tftp/sftp server
    speichern, 94
time, 167
time dst date, 168
    no time dst, 170
time dst recurring, 169
time set, 171
timeout, 548
track interface, 398
    no track interface, 399
track links, 400
    no track links, 401
Training, 4
type ppo-ex, 237

U

user-account, 454
    no user-account, 457
useraccount ruleset
    no useraccount ruleset, 523
user-account ruleset, 522
useraccount show-idx, 522
user-account-ext, 458
user-group, 460
userhost, 316
username, 238, 317, 462

V

validate cert, 146
verification cacert, 160
verification fingerprint, 161
vir-ip, 542, 549
    no vir-ip, 543, 550
vlan, 207
    no vlan, 208
vrrp associated-ip (VRRP3), 403
    no vrrp associated-ip, 404
vrrp ipv4 (VRRP3)
    no vrrp ipv4, 406
vrrp primary-ip (VRRP3), 405
vrrp priority (VRRP3), 407
    no vrrp priority, 408
vrrp timer (VRRP3), 408
    no vrrp-timer, 410
vrrp track decrement, 411
    no vrrp track, 412
vrrp vrid-track, 402
    no vrrp vrid-track, 402

W

web-session-timeout, 130
    no web-session-timeout, 131
Wertebereich für IPv4-Adresse, 45
whoami, 449
write, 128
write startup-config, 111