# Menüreferenz LCOS 8.60

LCOS
[LANCOM OPERATING SYSTEM]

LANCOM
Systems

# Inhalt

1 Einleitung....14
1.1 Über diese Dokumentation....14
Bestandteile der Dokumentation....14
LCOS, das Betriebssystem der LANCOM-Geräte....15
Gültigkeit....15
An der Erstellung dieser Dokumentation ….....15
1.2 Die Konfiguration mit Telnet....15
Telnet-Sitzung starten....15
Die Sprache der Konsole auf Deutsch ändern....16
Telnet-Sitzung beenden....16
Die Struktur im Kommandozeilen-Interface....16
1.3 Befehle für die Kommandozeile....17
Funktionen zum Editieren der Befehle....20
Funktionstasten für die Kommandozeile....21
1.4 Die Konfiguration mit WEBconfig....22
2 Setup....23
2.1 Name....23
2.2 WAN....23
2.2.18 Backup-St.-Sekunden....23
2.2.10 RR-Versuche....23
2.2.9 Schutz....24
2.2.2 Einwahl-Gegenstellen....24
2.2.3 RoundRobin....26
2.2.4 Layer....27
2.2.5 PPP....29
2.2.6 Ankommende Rufnummern....32
2.2.8 Skripte....33
2.2.11 Router-Interface....33
2.2.13 Manuelle Wahl....35
2.2.17 Kanal-Liste....35
2.2.19 DSL-Breitband-Gegenstellen....37
2.2.20 IP-Liste....40
2.2.21 PPTP-Gegenstellen....42
2.2.22 Radius....44
2.2.23 Polling-Tabelle....47
2.2.24 Backup-Gegenstellen....49
2.2.25 Aktions-Tabelle....50
2.2.26 MTU-Liste....53
2.2.30 Zusaetzliche-PPTP-Gateways....54
2.3 Gebuehren....70

2.3.12 Budgets-Zuruecksetzen....70
2.3.1 Budget-Einheiten....71
2.3.16 Aktivieren-Reserve....71
2.3.8 DSL-Breitband-Minuten-Budget....71
2.3.13 Einwahl-Minuten-Budget....71
2.3.6 Gesamt-Einheiten....71
2.3.11 Reserve-DSL-Breitband-Budget....72
2.3.3 Rest-Budget....72
2.3.9 Rest-DSL-Breitband-Minuten-Aktiv....72
2.3.14 Rest-Einwahl-Minuten....72
2.3.10 Router-DSL-Breitband-Budget....72
2.3.4 Router-Einheiten....72
2.3.15 Router-ISDN-Seriell-Minuten-Aktiv....72
2.3.2 Tage-pro-Periode....73
2.3.5 Tabelle-Budget....73
2.3.7 Zeit-Tabelle....73
2.4 LAN....74
2.4.3 Heap-Reserve....74
2.4.2 MAC-Adresse....75
2.4.9 Trace-Level....75
2.4.8 Trace-MAC....75
2.4.10 IEEE802.1x....75
2.5 Bridge....77
2.5.4 Aging-Minuten....77
2.5.1 Aktiv....77
2.5.2 Gegenstelle....77
2.5.7 LAN-Interface....78
2.5.8 VLAN-ID....78
2.5.3 Bridge-Tabelle....78
2.5.5 LAN-Einstellung....78
2.5.6 WAN-Einstellung....80
2.7 TCP-IP....82
2.7.1 Aktiv....82
2.7.11 ARP-Aging-Minuten....82
2.7.8 DNS-Backup....83
2.7.7 DNS-Default....83
2.7.22 ICMP-bei-ARP-Timeout....83
2.7.10 NBNS-Backup....83
2.7.9 NBNS-Default....84
2.7.20 Nichtlok.-ARP-Replies....84
2.7.6 Zugangs-Liste....84
2.7.16 ARP-Tabelle....85
2.7.17 Loopback-Liste....86
2.7.21 Alive-Test....87

2.7.30 Netzliste....89
2.8 IP-Router....92
2.8.1 Aktiv....92
2.8.12 Ende-WAN-Pool....93
2.8.6 ICMP-Redirect-Senden....93
2.8.14 Nutzung-Default-Listen....93
2.8.5 Proxy-ARP....93
2.8.11 Start-WAN-Pool....94
2.8.22 WAN-Tag-Erzeugung....94
2.8.2 IP-Routing-Tabelle....94
2.8.7 Routing-Methode....97
2.8.8 RIP....98
2.8.9 1-N-NAT....108
2.8.10 Firewall....115
2.8.13 Default-Zeit-Liste....133
2.8.19 N-N-NAT....134
2.8.20 Load-Balancer....136
2.8.21 VRRP....137
2.8.23 Tag-Tabelle....140
2.9 SNMP....141
2.9.3 Administrator....142
2.9.11 Kommentar-1....142
2.9.12 Kommentar-2....142
2.9.13 Kommentar-3....142
2.9.14 Kommentar-4....142
2.9.16 Kommentar-5....143
2.9.17 Kommentar-6....143
2.9.17 Kommentar-7....143
2.9.17 Kommentar-8....143
2.9.6 Loesche-Monitor....144
2.9.10 Passw.Zwang-fuer-SNMP-Lesezugriff....144
2.9.15 Read-Only-Community....144
2.9.5 Register-Monitor....144
2.9.4 Standort....145
2.9.1 Traps-senden....145
2.9.20 Volle-Host-MIB....145
2.9.2 IP-Traps....145
2.9.7 Monitor-Tabelle....146
2.10 DHCP....148
2.10.7 Default-Gueltigkeit-Minuten....148
2.10.6 Max.-Gueltigkeit-Minuten....148
2.10.19 User-Class-Identifier....148
2.10.8 DHCP-Tabelle....149
2.10.9 Hosts....150

2.10.10 Alias-Liste....152
2.10.18 Ports....152
2.10.20 Netzliste....153
2.10.21 Zusaetzliche-Optionen....159
2.11 Config....160
2.11.9 Admin.-EAZ-MSN....161
2.11.41 Admin-Geschlecht....161
2.11.42 Assert-Action....161
2.11.16 Bildschirmhoehe....161
2.11.5 Config-Aging-Minutes....162
2.11.60 CPU-Last-Intervall....162
2.11.40 Crash-Meldung....162
2.11.10 Display-Kontrast....163
2.11.18 LED-Test....163
2.11.39 Lizenzablauf-Email....163
2.11.7 Login-Fehler....163
2.11.4 max. Verbindungen....164
2.11.33 Outband-Aging-Minutes....164
2.11.3 Pass.Zwang-fuer-SNMP-Lesezugriff....164
2.11.17 Prompt....164
2.11.32 Reset-Knopf....165
2.11.8 Sperr-Minuten....166
2.11.6 Sprache....166
2.11.25 SSH-Port....166
2.11.23 Telnet-Port....166
2.11.24 Telnet-SSL-Port....167
2.11.13 TFTP-Client....167
2.11.15 Zugriffstabelle....169
2.11.20 Cron-Tabelle....171
2.11.21 Admins....174
2.11.26 SSH-Authentisierungs-Methoden....176
2.11.27 Predef.-Admins....177
2.11.30 Update-Client....177
2.11.31 Standortverifikation....180
2.11.35 Monitortrace....182
2.11.43 Funktionstasten....183
2.11.50 LL2M....184
2.12 WLAN....184
2.12.114 Aggregat-Wiederholungs-Limit....184
2.12.38 ARP-Behandlung....185
2.12.48 Benutze-vollen-Kanalsatz....185
2.12.44 Erlaube-illegale-Assoziation-ohne-Authentifizierung....185
2.12.115 Globale-Krypto-Sequenz-Pruefung-auslassen....186
2.12.3 Heap-Reserve....186

2.12.13 IAPP-Announce-Interval....186
2.12.14 IAPP-Handover-Timeout....186
2.12.60 IAPP-IP-Netzwerk....187
2.12.12 IAPP-Protokoll....187
2.12.47 Idle-Timeout....187
2.12.26 Inter-SSID-Verkehr....188
2.12.100 Karten-Reinit-Zyklus....188
2.12.36 Land....188
2.12.41 Mail-Adresse....188
2.12.46 Nur-Indoor-Betrieb....189
2.12.108 Radar-Last-Schwellwert....189
2.12.101 Rausch-Messzyklus....189
2.12.105 Therm.-Rekal.-Messzyklus....190
2.12.103 Trace-MAC....190
2.12.116 Trace-Pakete....190
2.12.110 Trace-Stufe....190
2.12.27 Ueberwachung-Stationen....191
2.12.8 Zugriffsmodus....191
2.12.7 Zugangs-Liste....191
2.12.29 RADIUS-Zugriffspruefung....193
2.12.45 RADIUS-Accounting....197
2.12.50 Signalmittelung....201
2.12.51 Raten-Adaption....203
2.12.70 VLAN-Gruppenschluessel-Abbildung....204
2.12.107 Radar-Muster-Schwellwerte....205
2.12.109 Rausch-Offsets....206
2.12.111 Rausch-Immunitaet....207
2.13 LANCAPI....209
2.13.3 UDP-Port....209
2.13.1 Zugangs-Liste....209
2.13.6 Interface-Liste....210
2.13.7 Prioritaeten-Liste....211
2.14 Zeit....211
2.14.2 Aktuelle-Zeit....212
2.14.5 Anwahl-Versuche....212
2.14.1 Hol-Methode....212
2.14.11 Sommerzeit....212
2.14.13 Zeit-holen....213
2.14.3 Zeit-Rufnummer....213
2.14.10 Zeitzone....213
2.14.12 Umstellungen-Sommerzeit....214
2.14.15 Feiertage....215
2.14.16 Zeitrahmen....215
2.15 LCR....216

2.15.2 Lancapi-Nutzung....217
2.15.1 Router-Nutzung....217
2.15.4 Zeit-Liste....217
2.16 NetBIOS....219
2.16.9 Abgleich....219
2.16.1 Aktiv....220
2.16.11 Gültigkeit....220
2.16.2 Scope-ID....220
2.16.14 Suchdienst-Unterstuetzung....220
2.16.10 WAN-Update-Minuten....221
2.16.8 Watchdogs....221
2.16.4 Gegenstellen....221
2.16.5 Gruppen-Liste....222
2.16.6 Host Liste....223
2.16.7 Server-Liste....225
2.16.12 Netzwerke....226
2.17 DNS....227
2.17.1 Aktiv....227
2.17.3 DHCP-verwenden....228
2.17.2 Domain....228
2.17.12 Domain-aufloesen....228
2.17.7 Gueltigkeit....228
2.17.4 NetBIOS-verw....229
2.17.5 DNS-Liste....229
2.17.6 Filter-Liste....230
2.17.8 Dyn.-DNS-Liste....231
2.17.9 DNS-Weiterleitungen....231
2.17.10 Service-Location-Liste....232
2.17.11 Dynamische-SRV-Liste....233
2.17.13 Sub-Domains....233
2.18 Accounting....234
2.18.1 Aktiv....234
2.18.10 Diskriminator....234
2.18.6 Loeschen-Accounting-Liste....234
2.18.3 Sortieren-nach....235
2.18.2 Speichern-Flashrom....235
2.18.4 Aktuelle-User....235
2.18.5 Accounting-Liste....236
2.18.8 Zeit-Schnappschuss....237
2.18.9 Letzter Schnappschuss....238
2.19 VPN....239
2.19.11 AggrMode-IKE-Group-Default....239
2.19.10 AggrMode-Proposal-List-Default....240
2.19.8 Aktiv....240

2.19.22 Erlaube-Entferntes-Netzwerk-Auswahl....240
2.19.25 Flexibler-ID-Vergleich....241
2.19.15 legacy-dyn-VPN(LCOS5.0x)-support....241
2.19.14 MainMode-IKE-Group-Default....241
2.19.13 MainMode-Proposal-List-Default....241
2.19.24 Max-gleichzeitige-Verbindungen....242
2.19.16 NAT-T-Aktiv....242
2.19.26 NAT-T-Port-fuer-Rekeying....242
2.19.20 QuickMode-PFS-Group-Default....242
2.19.19 QuickMode-Proposal-List-Default....243
2.19.21 QuickMode-Shorthold-Zeit-Default....243
2.19.23 SA-Aufbau-gemeinsam....243
2.19.27 SSL- Encaps. erlaubt....244
2.19.17 Vereinfachtes-Zertifikats-RAS-Aktiv....244
2.19.3 Isakmp....244
2.19.4 Proposals....246
2.19.5 Zertifikate-Schluessel....253
2.19.7 Layer....255
2.19.9 VPN-Gegenstellen....257
2.19.12 Zusaetzliche-Gateway-Liste....261
2.20 LAN-Bridge....273
2.20.12 Alterungs-Zeit....273
2.20.2 Bridge-Prioritaet....273
2.20.7 Forward-Delay....274
2.20.6 Hello-Time....274
2.20.8 Isolierter-Modus....274
2.20.5 Max-Age....274
2.20.1 Protokoll-Version....275
2.20.4 Verkapselungs-Tabelle....275
2.20.10 Protokoll-Tabelle....275
2.20.11 Port-Daten....279
2.20.13 Prioritaets-Zuordnung....281
2.20.20 Spannning-Tree....282
2.20.30 IGMP-Snooping....285
2.21 HTTP....291
2.21.2 Seitenueberschriften....291
2.21.1 Dokumentenwurzel....291
2.21.6 Fehlerseiten-Stil....291
2.21.15 HTTP-Kompression....292
2.21.9 Max.-Tunnel-Verbindungen....292
2.21.7 Port....292
2.21.3 Schrift-Familie....292
2.21.5 Seitenueberschriften....293
2.21.11 Sitzungs-Timeout....293

2.21.8 SSL-Port....293
2.21.13 Standard-Design....293
2.21.10 Tunnel-Idle-Timeout....293
2.21.18 SSL-Versions....294
2.21.14 Geräteinformation-anzeigen....294
2.21.16 Server-Ports-offen-halten....295
2.21.20 Rollout-Wizard....296
2.21.30 Datei-Server....300
2.22 SYSLOG....301
2.22.1 Aktiv....301
2.22.5 Meldungs-Tabellen-Reihenfolge....301
2.22.4 Port....301
2.22.2 Tabelle-SYSLOG....301
2.22.3 Facility-Mapper....303
2.23 Schnittstellen....304
2.23.19 PCM-SYNC-SOURCE....304
2.23.18 Permanente-L1-Aktivierung....304
2.23.1 S0....305
2.23.4 DSL....306
2.23.6 ADSL-Interface....308
2.23.7 Modem-Mobilfunk....310
2.23.8 VDSL....311
2.23.20 WLAN....312
2.23.21 LAN-Schnittstellen....346
2.23.30 Ethernet-Ports....348
2.23.40 Modem....350
2.23.41 Mobilfunk....353
2.23.50 Analog....357
2.24 Public-Spot-Modul....358
2.24.19 Neuer-Benutzer-Assistent....358
2.24.3 Anbieter-Tabelle....362
2.24.2 Benutzer-Tabelle....365
2.24.31 Freie Netze....366
2.24.15 Port-Tabelle....367
2.24.8 Seitentabelle....367
2.24.20 VLAN-Tabelle....368
2.24.7 Accounting-Meldezyklus....369
2.24.1 Authentifizierungs-Modus....369
2.24.16 Auto-Löschen-Benutzer-Tabelle....369
2.24.30 Freier-Server....369
2.24.22 Geräte-Hostname....370
2.24.14 Idle-Timeout....370
2.24.12 Kommunikations-Port....370
2.24.21 Login-Seiten-Typ....370

2.24.9 Roaming-Schluessel....371
2.24.17 Server-Datenbank-liefern....371
2.24.6 Server-Verzeichnis....371
2.24.5 Traffic-Limit-Bytes....371
2.24.18 Verbiete-Mehrfach-Logins....372
2.24.26 Stations-Tabellen-Limit....372
2.25 RADIUS....372
2.25.4 Auth.-Timeout....372
2.25.5 Auth.-Wiederholung....373
2.25.9 Backup-Abfrage-Strategie....373
2.25.10 Server....373
2.26 NTP....386
2.26.2 Aktiv....386
2.26.4 BC-Intervall....386
2.26.3 BC-Modus....387
2.26.7 RQ-Intervall....387
2.26.12 RQ-Versuche....387
2.26.11 RQ-Addresse....387
2.27 Mail....388
2.27.5 Benutzername....388
2.27.7 E-Mail-Absender....389
2.27.11 Loopback-Addr....389
2.27.6 Passwort....389
2.27.4 POP3-Port....390
2.27.3 POP3-Server....390
2.27.10 Pufferanzahl....390
2.27.8 Sendewiederholung-(Min)....390
2.27.2 Serverport....391
2.27.1 SMTP-Server....391
2.27.9 Vorhaltezeit-(Std)....391
2.30 IEEE802.1x....391
2.30.3 Radius-Server....392
2.30.4 Ports....393
2.31 PPPoE....396
2.31.1 Aktiv....396
2.31.3 Service....397
2.31.4 Session-Limit....397
2.31.2 Namenliste....397
2.31.5 Ports....398
2.32 VLAN....399
2.32.4 Aktiv....399
2.32.5 Tag-Wert....399
2.32.1 Netzwerke....399
2.32.2 Port-Tabelle....400

2.33 Voice-Call-Manager....401
2.33.1 Operating....402
2.33.2 General....402
2.33.3 Users....407
2.33.4 Line....423
2.33.5 Call-Router....447
2.33.7 Groups....451
2.33.8 Protokollierung....454
2.34 Drucker....455
2.34.1 Drucker....455
2.34.2 Zugangs-Liste....457
2.35 ECHO-Server....458
2.35.1 Aktiv....458
2.35.3 TCP-Timeout....458
2.35.2 Zugriffstabelle....458
2.36 Performance-Monitoring....459
2.36.2 RttMonAdmin....459
2.36.3 RttMonEchoAdmin....460
2.36.4 RttMonStatistics....461
2.37 WLAN-Management....465
2.37.6 AP-automatisch-einbinden....465
2.37.7 AP-einbinden....466
2.37.9 AP-Verbindung-trennen....466
2.37.5 CAPWAP-Port....466
2.37.8 Defaultkonfiguration-verwenden....466
2.37.31 Intervall-zur-Bereinigung-der-Statustabellen....467
2.37.33 Lizenzlimit....467
2.37.32 Lizenzzahl....467
2.37.19 Starte-automatische-Funkfeldoptimierung....467
2.37.30 WTP-Password-synchron-halten....468
2.37.1 AP-Konfiguration....468
2.37.10 Benachrichtigung....502
2.37.34 WLC-Cluster....504
2.37.27 Zentrales-Firmware-Management....506
2.37.17 RADIUS-Server....510
2.37.20 Zugangs-Liste....511
2.39 Zertifikate....513
2.39.1 SCEP-Client....513
2.39.2 SCEP-CA....521
2.39.3 CRLs....528
2.29.6 OCSP-Client....530
2.40 GPS....533
2.40.1 Aktiv....533
2.41 UTM....534

2.41.2 Content-Filter....534
2.42 ADSL....565
2.42.1 Trace-Modus....565
2.42.4 Ueberwachungszeit(Std)....566
2.42.3 Verbindungsabbrueche....566
2.52 COM-Ports....566
2.52.1 Geraete....566
2.52.2 COM-Port-Server....567
2.52.3 WAN....575
2.52.4 Serielle-Konfig....576
2.53 Temperatur-Monitor....576
2.53.1 Obergrenze-Grad....576
2.53.2 Untergrenze-Grad....577
2.54 TACACS....577
2.54.3 Accounting....577
2.54.1 Autentifizierung....577
2.54.2 Authorisierung....577
2.54.10 Rückgriff auf lokale Benutzer....578
2.54.6 Shared-Secret....578
2.54.12 SNMP-GET-Anfragen-Accounting....578
2.54.11 SNMP-GET-Anfragen-Authorisierung....579
2.54.13 Umgehe-Tacacs-fuer-CRON/Skripte/Aktions-Tabelle....579
2.54.7 Verschlüsselung....579
2.54.14 Wert-zu-Authorisierungsanfrage-hinzufuegen....580
2.54.9 Server....580
2.56 Automatisches-Laden....581
2.56.1 Firmware-und-Loader....581
2.56.2 Konfiguration-und-Skript....582
2.59 WLAN-Management....582
2.59.120 Log-Eintraege....582
2.59.1 Statische-WLC-Konfiguration....582
2.60 Automatisches-Laden....583
2.60.1 Netzwerk....584
2.60.56 USB....587
2.63 Paket-Capture....588
2.63.1 LCOSCap-In-Betrieb....588
2.63.2 LCOSCap-Port....589
2.200 SIP-ALG....589
2.200.1 Operating....589
3 Firmware....590
3.7 Feature-Word....590
3.3 Modus-Firmsafe....590
3.4 Timeout-Firmsafe....591
3.1 Versions-Tabelle....591

3.1.1 Ifc....591
3.1.2 Modul....591
3.1.3 Version....591
3.1.4 Seriennummer....591
3.2 Tabelle-Firmsafe....591
3.2.1 Position....592
3.2.2 Status....592
3.2.3 Version....592
3.2.4 Datum....592
3.2.5 Groesse....592
3.2.6 Index....592
4 Sonstiges....593
4.5 Kaltstart....593
4.2 System-Boot....593
4.1 Manuelle-Wahl....593
4.1.2 Abbau....593
4.1.1 Aufbau....593
4.1.4 Testruf....593
4.6 Voice-Call-Manager....594
4.6.1 Line....594
4.6.2 Groups....594

# 1 Einleitung

## 1.1 Über diese Dokumentation

### Bestandteile der Dokumentation

Die Dokumentation Ihres Gerätes besteht aus folgenden Teilen:

- Installation Guide

  In dieser Kurzanleitung finden Sie Antworten auf die folgende Fragen:

  - Welche Software muss zur Konfiguration installiert werden?
  - Wie wird das Gerät angeschlossen?
  - Wie kann das Gerät über LANconfig, WEBconfig oder die serielle Schnittstelle erreicht werden?
  - Wie startet man die Setup-Assistenten (z.B. zur Einrichtung des Internetzugangs)?
  - Wie wird ein Gerätereset durchgeführt?
  - Wo gibt es weitere Informationen und Hilfe?

- Benutzerhandbuch oder Hardware-Schnellübersicht

  Das Benutzerhandbuch oder die Hardware-Schnellübersicht enthalten alle Informationen, die zur raschen Inbetriebnahme Ihres Gerätes notwendig sind. Außerdem finden Sie hier alle wichtigen technischen Spezifikationen.

- Handbuch TK-Anlagenfunktionen (nur bei Modellen mit VoIP-Unterstützung)

  Im Handbuch TK-Anlagenfunktionen finden Sie eine ausführliche Schritt-für-Schritt-Anleitung, um einen LANCOM VoIP Router als Telefonanlage für einen Einzelstandort in Betrieb zu nehmen. Ferner werden dort die wichtigsten Bedienhinweise für Teilnehmer und den Anschluss von Endgeräten beschrieben.

- Referenzhandbuch

  Das Referenzhandbuch und geht ausführlich auf Themen ein, die übergreifend für mehrere Modelle gelten.

  Die Beschreibungen im Referenzhandbuch orientieren sich überwiegend an der Konfiguration mit LANconfig. Für jeden LANconfig-Dialog wird außerdem der zugehörige Pfad angegeben, unter dem die entsprechenden Parameter bei der Konfiguration mit WEBconfig zu finden sind, z B.:

  LANconfig: Wireless LAN / 802.11i/WEP / WPA- / Einzel-WEP-Einstellungen

  WEBconfig: LCOS-Menübaum / Setup / Schnittstellen / WLAN / Verschluesselung

  Die Pfade für die Konfiguration über die Konsole/Telnet lassen sich daraus ableiten und werden daher nicht explizit aufgeführt. Der Telnetpfad zu den Verschlüsselungseinstellungen lautet z. B.:

  ```
  cd Setup/Schnittstellen/WLAN/Verschluesselung
  ```

- Menü-Referenz

  Die vorliegende Menü-Referenz beschreibt alle Parameter von LCOS, dem Betriebssystem der LANCOM-Geräte. Diese Beschreibung unterstützt den Anwender bei der Konfiguration der Geräte mit WEBconfig bzw. über die Konsole (Telnet).

  Die Parameter werden in der Menü-Referenz in der Reihenfolge der Pfade aufgeführt, wie sie bei der Konfiguration mit WEBconfig erreicht werden können. Zu jedem Parameter werden neben der Beschreibung auch die möglichen Eingabewerte und die Standardbelegung wiedergegeben.

Alle Dokumente, die Ihrem Produkt nicht in ausgedruckter Form beiliegen, finden als Acrobat-Dokument (PDF-Datei) unter www.lancom.de/download oder auf dem Datenträger, der Ihrem Produkt beiliegt.

### LCOS, das Betriebssystem der LANCOM-Geräte

Alle Router, Gateways, Controller und Access Points von LANCOM Systems setzen dasselbe Betriebssystem ein: LCOS. Das von LANCOM Systems selbst entwickelte Betriebssystem ist von außen nicht angreifbar und bietet so eine hohe Sicherheit. Darüber hinaus steht die konsistente Verwendung von LCOS für eine komfortable und durchgängige Bedienung über alle LANCOM-Produkte. Das umfangreiche Featureset ist für alle LANCOM-Produkte (bei entsprechender Unterstützung durch die Hardware) gleich verfügbar und wird durch kostenlose, regelmäßige Software-Updates ständig weiterentwickelt.

In diesem Handbuch gelten folgende Abgrenzungen von Software, Hardware und Hersteller:

- LCOS bezeichnet das geräteunabhängige Betriebssystem
- LANCOM steht als Oberbegriff für alle LANCOM-Router und LANCOM Router Access Points
- LANCOM Systems steht als Kurzform für den Hersteller, die LANCOM Systems GmbH

### Gültigkeit

Die vorliegende Menü-Referenz gilt für alle LANCOM Router und LANCOM Access Points mit einem Firmwarestand Version 8.60 oder neuer.

Die in dieser Menü-Referenz beschriebenen Funktionen und Einstellungen werden nicht von allen Modellen bzw. allen Firmware-Versionen unterstützt.

### An der Erstellung dieser Dokumentation …

… haben mehrere Mitarbeiter/innen aus verschiedenen Teilen des Unternehmens mitgewirkt, um Ihnen die bestmögliche Unterstützung bei der Nutzung Ihres LANCOM-Produktes anzubieten.

Sollten Sie einen Fehler finden, oder einfach nur Kritik oder Anregung zu dieser Dokumentation äußern wollen, senden Sie bitte eine E-Mail direkt an:

info@lancom.de

Sollten Sie zu den in diesem Handbuch besprochenen Themen noch Fragen haben oder zusätzliche Hilfe benötigen, steht Ihnen unser Internet-Server www.lancom.derund um die Uhr zur Verfügung. Hier finden Sie im Bereich 'Support' viele Antworten auf häufig gestellte Fragen (FAQs). Darüber hinaus bietet Ihnen die Wissensdatenbank einen großen Pool an Informationen. Aktuelle Treiber, Firmware, Tools und Dokumentation stehen für Sie jederzeit zum Download bereit. Außerdem steht Ihnen der LANCOM-Support zur Verfügung. Telefonnummern und Kontaktadressen des LANCOM-Supports finden Sie in einem separaten Beileger oder auf der LANCOM Systems-Homepage.

## 1.2 Die Konfiguration mit Telnet

### Telnet-Sitzung starten

Über Telnet starten Sie die Konfiguration z.B. aus der Windows-Kommandozeile mit dem Befehl:

- `C:\>telnet 10.0.0.1`

Telnet baut dann eine Verbindung zum Gerät mit der eingegebenen IP-Adresse auf.

Nach der Eingabe des Passworts (sofern Sie eines zum Schutz der Konfiguration vereinbart haben) stehen Ihnen alle Konfigurationsbefehle zur Verfügung.

Linux und Unix unterstützen auch Telnet-Sitzungen über SSL-verschlüsselte Verbindungen. Je nach Distribution ist es dazu ggf. erforderlich, die Standard-Telnet-Anwendung durch eine SSL-fähige Version zu ersetzen. Die verschlüsselte Telnet-Verbindung wird dann mit dem folgenden Befehl gestartet:

- `C:\>telnet -z ssl 10.0.0.1 telnets`

## Die Sprache der Konsole auf Deutsch ändern

Der Terminalmodus steht in den Sprachen Deutsch und Englisch zur Verfügung. LANCOM Geräte werden werkseitig auf Englisch als Konsolensprache eingestellt. Im weiteren Verlauf dieser Dokumentation werden alle Konfigurationsbefehle in ihrer deutschen Form angegeben. Zur Änderung der Konsolensprache auf Deutsch verwenden Sie folgende Befehle:

WEBconfig: LCOS-Menübaum / Setup / Config-Module / Language

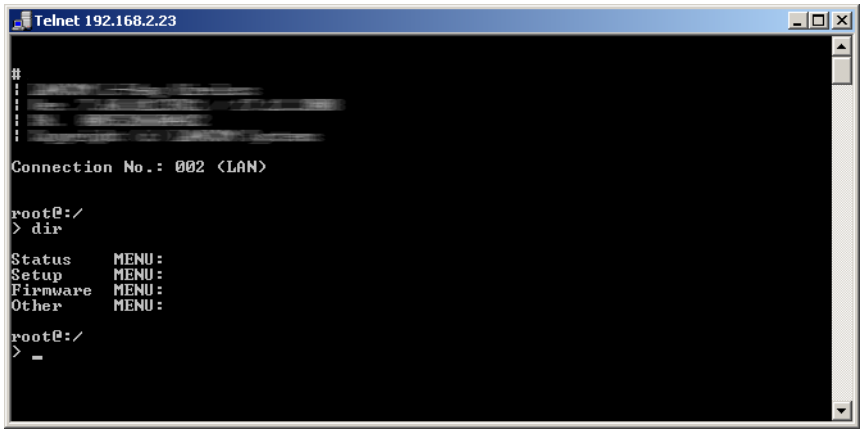
## Telnet-Sitzung beenden

Um die Telnet-Sitzung zu beenden, geben Sie an der Eingabeaufforderung den Befehl `exit` ein:

- `C:\>exit`

## Die Struktur im Kommandozeilen-Interface

Das LANCOM Kommandozeilen-Interface ist stets wie folgt strukturiert:




- **Status**

  Enthält die Zustände und Statistiken aller internen Module des Gerätes

- **Setup**

  Beinhaltet alle einstellbaren Parameter aller internen Module des Gerätes

- **Firmware**

  Beinhaltet das Firmware-Management

- **Sonstiges**

  Enthält Aktionen für Verbindungsauf- und abbau, Reset, Reboot und Upload

## 1.3 Befehle für die Kommandozeile

Das LANCOM Kommandozeilen-Interface kann mit den folgenden DOS- oder UNIX-ähnlichen Befehlen bedient werden. Die verfügbaren LCOS-Menübefehle können durch Aufrufen des HELP-Kommandos jederzeit auf der Kommandozeile angezeigt werden.

Zum Ausführen einiger Befehle sind Supervisor-Rechte erforderlich.

| Befehl | Beschreibung |
|---|---|
| beginscript | Versetzt eine Konsolensitzung in den Script-Modus. In diesem Zustand werden die im Folgenden eingegebenen Befehle nicht direkt in den Konfigurations-RAM im LANCOM übertragen, sondern zunächst in den Script-Speicher des Gerätes. |
| cd [PFAD] | Wechselt das aktuelle Verzeichnis.<br>Verschiedene Kurzformen werden unterstützt, z.B. "cd ../.." kann verkürzt werden zu "cd ..." etc. |
| del [PFAD]* | Löscht eine komplette Tabelle in dem mit `Path` angegebenen Zweig des Menübaums. |
| default [-r] [PFAD] | Setzt einzelne Parameter, Tabellen oder ganze Menübäume in die Grundkonfiguration zurück. Zeigt `PATH` auf einen Zweig des Menübaums, muss zwingend die option `-r` (recursive) angegeben werden. |
| dir [PFAD] list [PFAD] ls [PFAD] ll [PFAD] | Zeigt den Inhalt des aktuellen Verzeichnisses an.<br>Der angehängte Parameter „-a“ gibt zusätzlich zu den Inhalten der Abfrage auch die zugehörigen SNMP-IDs aus. Dabei beginnt die Ausgabe mit der SNMP-ID des Gerätes, gefolgt von der SNMP-ID des aktuellen Menüs. Vor den einzelnen Einträgen finden Sie dann die SNMP-IDs der Unterpunkte. |
| do [PFAD] [<Parameter>] | Führt die Aktion [PATH] im aktuellen Verzeichnis aus. Zusätzliche Parameter können mit angegeben werden. |
| echo <ARG>... | Argument auf Konsole ausgeben |
| exit/quit/x | Beendet die Kommandozeilen-Sitzung |
| feature <code> | Freischaltung eines SW-Features mit dem angegebenen Feature-Code |
| flash Yes/No | Die Änderungen an der Konfiguration über die Befehle an der Kommandozeile werden standardmäßig (flash yes) direkt in den boot-resistenten Flash-Speicher der Geräte geschrieben. Wenn das Aktualisieren der Konfiguration im Flash unterdrückt wird (flash no), werden die Änderungen nur im RAM gespeichert, der beim Booten gelöscht wird. |
| history | Zeigt eine Liste der letzen ausgeführten Befehle. Mit dem Befehl `!#` können die Befehle der Liste unter Ihrer Nummer (#) direkt aufgerufen werden: Mit `!3` wird z.B. der dritte Befehl der Liste ausgeführt. |
| killscript | Löscht den noch nicht verarbeiteten Inhalt einer Scriptsession. Die Scriptsession wird über den Namen ausgewählt. |
| loadconfig | Konfiguration per TFTP-Client in das Gerät laden |

| Befehl | Beschreibung |
|---|---|
| loadfirmware | Firmware per TFTP-Client in das Gerät laden |
| loadscript | Script per TFTP-Client in das Gerät laden |
| passwd | Ändern des Passworts |
| passwd -n neues [altes] | Passwort ändern (Keine Eingabeaufforderung) |
| ping [IP-Adresse oder Name] | Sendet einen ICMP echo request an die angegebene IP-Adresse |
| readconfig | Anzeige der kompletten Konfiguration in der Geräte-Syntax |
| readmib | Anzeige der SNMP Management Information Base |
| readscript [-n] [-d] [-c] [-m] [PFAD] | Erzeugt in einer Konsolensitzung eine Textausgabe von allen Befehlen und Parametern, die für die Konfiguration des LANCOM im aktuellen Zustand benötigt werden. |
| repeat <INTERVAL> <Kommando> | Wiederholt das Kommando alle INTERVAL Sekunden, bis der Vorgang durch neue Eingaben beendet wird |
| sleep [-u] Wert[suffix] | Verzögert die Verarbeitung der Konfigurationsbefehle um eine bestimmte Zeitspanne oder terminiert sie auf einen bestimmten Zeitpunkt. Als Suffix sind `s`, `m`, oder `h` für Sekunden, Minuten, oder Stunden erlaubt, ohne Suffix arbeitet der Befehl in Millisekunden. Mit dem Optionsschalter `-u` nimmt das sleep-Kommando Zeitpunkte im Format `MM/DD/YYYY hh:mm:ss` (englisch) oder im Format `TT.MM.JJJJ hh:mm:ss` (deutsch) entgegen. Die Parametrierung als Termin wird nur akzeptiert, wenn die Systemzeit gesetzt ist. |
| stop | Beendet den PING-Befehl |
| set [PFAD] <Wert(e)> | Setzt einen Konfigurationsparameter auf einen bestimmten Wert.<br>Handelt es sich beim Konfigurationsparameter um einen Tabellenwert, so muss für jede Spalte ein Wert angegeben werden.<br>Dabei übernimmt das Zeichen * als Eingabewert einen vorhandenen Tabelleneintrag unverändert. |
| set [PFAD] ? | Auflistung der möglichen Eingabewerte für einen Konfigurationsparameter.<br>Wird kein Name angegeben, so werden die möglichen Eingabewerte für alle Konfigurationsparameter im aktuellen Verzeichnis angegeben |
| setenv <NAME> <WERT> | Umgebungsvariable setzen |
| unsetenv <NAME> | Umgebungsvariable löschen |
| getenv <NAME> | Umgebungsvariable ausgeben (kein Zeilenvorschub) |
| printenv | Komplette Umgebung ausgeben |
| show <Optionen> | Anzeige spezieller interner Daten.<br>`show ?` zeigt alle verfügbaren Informationen an, z.B. letzte Boot-Vorgänge (bootlog), Firewall Filterregeln (filter), VPN-Regeln (VPN) und Speicherauslastung (mem und heap) |

| Befehl | Beschreibung |
|---|---|
| sysinfo | Anzeige der Systeminformationen (z.B. Hardware/Softwareversion etc.) |
| testmail | Schickt eine E-Mail. Parameter siehe 'testmail ?' |
| time | Zeit setzen (TT.MM.JJJJ hh:mm:ss) |
| trace […] | Konfiguration der Diagnose-Ausgaben. |
| who | Aktive Sitzungen auflisten |
| writeconfig | Laden einer neuen Konfigurationsfile in der Geräte-Syntax. Alle folgenden Zeilen werden als Konfigurationswerte interpretiert, solange bis zwei Leerzeilen auftreten |
| writeflash | Laden einer neuen Firmware-Datei (nur via TFTP) |
| !! | Letztes Kommando wiederholen |
| !<num> | Kommando <num> wiederholen |
| !<prefix> | Letztes mit <prefix> beginnendes Kommando wiederholen |
| #<blank> | Kommentar |

- PFAD:
  - Pfadname für ein Menü oder einen Parameter, getrennt durch / oder \
  - .. bedeutet eine Ebene höher
  - . bedeutet aktuelle Ebene
- WERT:
  - möglicher Eingabewert
  - "" ist ein leerer Eingabewert
- NAME:
  - Sequenz von _ 0..9 A..Z
  - erstes Zeichen darf keine Ziffer sein
  - keine Unterscheidung Groß/Kleinschreibung
- Alle Befehle, Verzeichnis- und Parameternamen können verkürzt eingegeben werden - solange sie eindeutig sind. Zum Beispiel kann der Befehl "`sysinfo`" zu "`sys`" verkürzt werden, oder aber "`cd Management`" zu "`cd ma`". Die Eingabe "`cd /s`" dagegen ist ungültig, da dieser Eingabe sowohl "`cd /Setup`" als auch "`cd /Status`" entspräche.
- Verzeichnisse können über die entsprechende SNMP-ID angesprochen werden. Der Befehl "`cd /2/8/10/2`" bewirkt z.B. das gleiche wie "`cd /Setup/IP-Router/Firewall/Regel-Tabelle`".
- Mehrere Werte in einer Tabellezeile können mit **einem** Befehl verändert werden, z.B. in der Regeltabelle der Firewall:
  - `set WINS UDP` setzt das Protokoll der Regel WINS auf UDP
  - `set WINS UDP ANYHOST` setzt das Protokoll der Regel WINS auf UDP und die Destination auf ANYHOST
  - `set WINS * ANYHOST` setzt ebenfalls die Destination der Regel WINS auf ANYHOST, durch das Sternchen wird das Protokoll unverändert übernommen

- Die Werte in einer Tabellenzeile können alternativ über den Spaltennamen oder die Positionsnummer in geschweiften Klammern angesprochen werden. Der Befehlt `set ?` in der Tabelle zeigt neben dem Namen und den möglichen Eingabewerten auch die Positionsnummer für jede Spalte an. Die Destination hat in der Regeltabelle der Firewall z.B. die Nummer 4:
  - `set WINS {4} ANYHOST` setzt die Destination der Regel WINS auf ANYHOST
  - `set WINS {destination} ANYHOST` setzt auch die Destination der Regel WINS auf ANYHOST
  - `set WINS {dest} ANYHOST` setzt die Destination der Regel WINS auf ANYHOST, weil die Angabe von "dest" hier ausreichend für eine eindeutige Spaltenbezeichnung ist.
- Namen, die Leerzeichen enthalten, müssen in Anführungszeichen ("") eingeschlossen werden.
- Für Aktionen und Befehle steht eine kommandospezifische Hilfefunktion zur Verfügung, indem die Funktion mit einem Fragezeichen als Parameter aufgerufen wird. Zum Beispiel zeigt der Aufruf `ping ?` die Optionen des eingebauten ping Kommandos an.
- Eine vollständige Auflistung der zur Verfügung stehenden Konsolen-Kommandos erhalten Sie durch die Eingabe von `?` auf der Kommandozeile.

## Funktionen zum Editieren der Befehle

Mit den folgenden Befehlen können die Befehle auf der Kommandozeile bearbeitet werden. Die "ESC key sequences" zeigen zum Vergleich die Tastenkombinationen, die auf typischen VT100/ANSI-Terminals verwendet werden:

| Funktion | Esc key sequences | Beschreibung |
|---|---|---|
| Pfeil nach oben | ESC [A | Springt in der Liste der letzten ausgeführten Befehle eine Position nach oben, in Richtung älterer Befehle. |
| Pfeil nach unten | ESC [B | Springt in der Liste der letzten ausgeführten Befehle eine Position nach unten, in Richtung neuerer Befehle. |
| Pfeil nach rechts | Ctrl-F ESC [C | Bewegt die Einfügemarke eine Position nach rechts. |
| Pfeil nach links | Ctrl-B ESC [D | Bewegt die Einfügemarke eine Position nach links. |
| Home oder Pos1 | Ctrl-A ESC [A ESC [1˜ ( | Bewegt die Einfügemarke an das erste Zeichen der Zeile. |
| Ende | Ctrl-E ESC [F ESC OF ESC [4˜ | Bewegt die Einfügemarke an das letzte Zeichen der Zeile. |
| Einfg | ESC [ ESC [2˜ | Schaltet um zwischen Einfügemodus und Überschreibemodus. |
| Entf | Ctrl-D ESC <BS> ESC [3˜ | Löscht das Zeichen an der aktuellen Position der Einfügemarke oder beendet die Telnet-Sitzung, wenn die Zeile leer ist. |
| erase | <BS><DEL> | Löscht das nächste Zeichen links neben der Einfügemarke. |
| erase-bol | Ctrl-U | Löscht alle Zeichen links neben der Einfügemarke. |
| erase-eol | Ctrl-K | Löscht alle Zeichen rechts neben der Einfügemarke. |
| Tabulator | | Komplettiert die Eingabe von der aktuellen Position der Einfügemarke zu einem Befehl oder Pfad der LCOS-Menüstruktur:<br>**1.** Wenn es genau eine Möglichkeit gibt, den Befehl bzw. den Pfad zu vervollständigen, so wird diese Möglichkeit in die Zeile übernommen. |

| Funktion | Esc key sequences | Beschreibung |
|---|---|---|
| | | **2.** Wenn es mehrere Möglichkeiten gibt, den Befehl bzw. den Pfad zu vervollständigen, so wird dies durch einen Hinweiston beim Drücken der Tab-Taste angezeigt. Mit einem erneuten Druck auf die Tab-Taste wird eine Liste mit allen Möglichkeiten angezeigt, mit denen die Eingabe vervollständigt werden kann. Geben Sie dann z. B. einen weiteren Buchstaben ein, um ein eindeutiges Vervollständigen der Eingabe zu ermöglichen.<br>**3.** Wenn es keine Möglichkeit gibt, den Befehl bzw. den Pfad zu vervollständigen, so wird dies durch einen Hinweiston beim Drücken der Tab-Taste angezeigt. Es werden keine weiteren Aktionen ausgeführt. |

## Funktionstasten für die Kommandozeile

WEBconfig: Setup / Config / Funktionstasten

Mit den Funktionstasten haben Sie die Möglichkeit, häufig genutzte Befehlssequenzen zu speichern und an der Kommandozeile komfortabel aufzurufen. In der entsprechenden Tabelle werden den Funktionstasten F1 bis F12 die Befehle so zugeordnet, wie sie an der Kommandozeile eingegeben werden.

- Taste

  Bezeichnung der Funktionstaste.

  Mögliche Werte:

  - Auswahl aus den Funktionstasten F1 bis F12.

  Default:

  - F1

- Abbildung

  Beschreibung des Befehls bzw. der Tastenkombination, die bei Aufruf der Funktionstaste an der Kommandozeile ausgeführt werden soll.

  Mögliche Werte:

  - Alle an der Kommandozeile möglichen Befehle bzw. Tastenkombinationen

  Default:

  - Leer

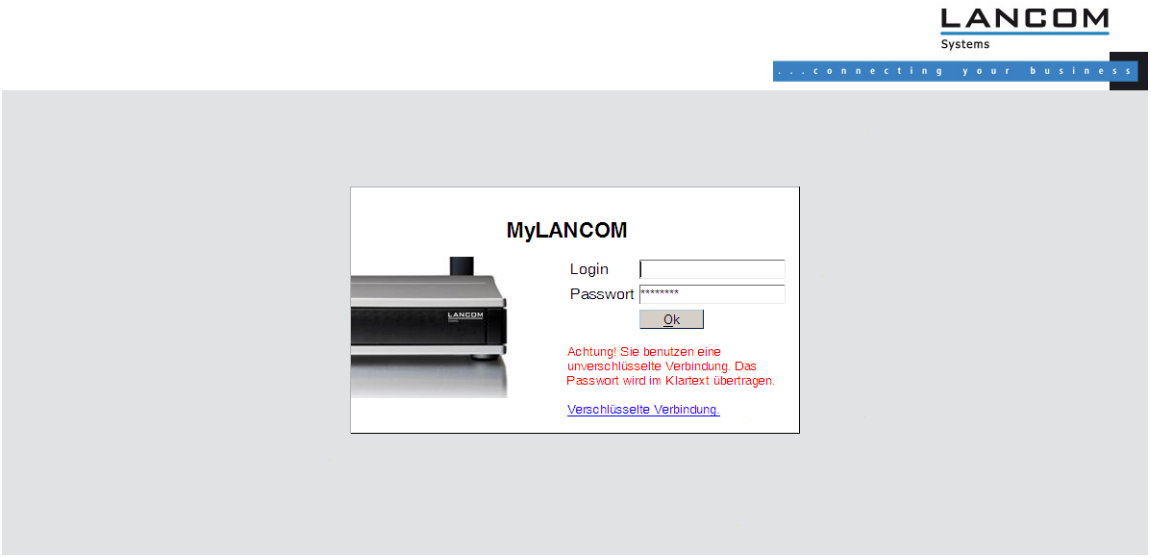
  Besondere Werte:

  - Das Caret-Zeichen ^ wird verwendet, um spezielle Steuerungsbefehle mit ASCII-Werten unterhalb von 32 abzubilden.
  - ^A steht für Strg-A (ASCII 1)
  - ^Z steht für Strg-Z (ASCII 26)
  - ^[ steht für Escape (ASCII 27)
  - ^^ Ein doppeltes Caret-Zeichen steht für das Caret-Zeichen selbst.

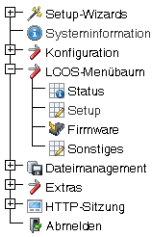
Wenn Sie ein Caret-Zeichen direkt gefolgt von einem anderen Zeichen in ein Dialogfeld oder in einem Editor eingeben, wird das Betriebssystem diese Sequenz möglicherweise als ein anderes Sonderzeichen deuten. Aus der Eingabe von Caret-Zeichen + A macht ein Windows-Betriebssystem z. B. ein Â. Um das Caret-Zeichen selbst aufzurufen, geben Sie vor dem folgenden Zeichen ein Leerzeichen ein. Aus Caret-Zeichen + Leerzeichen + A wird dann die Sequenz ^A.

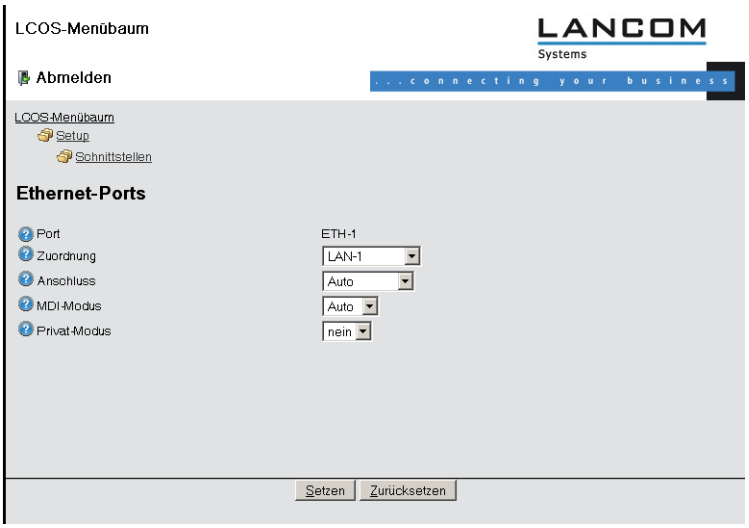
# 1.4 Die Konfiguration mit WEBconfig

Sie können die Einstellungen des Gerätes über einen beliebigen Webbrowser vornehmen. Im LANCOM ist die Konfigurationssoftware WEBconfig integriert. Sie benötigen lediglich einen Webbrowser, um auf WEBconfig zuzugreifen. In einem Netzwerk mit DHCP-Server erreichen Sie das Gerät im Webbrowser unter seiner IP-Adresse.




Der Menübereich "LCOS-Menübaum" bietet die Konfigurationsparameter in der gleichen Struktur an, wie Sie auch unter Telnet verwendet wird. Mit einem Klick auf das Fragezeichen können Sie für jeden Konfigurationsparameter eine Hilfe aufrufen.



# 2 Setup

In diesem Menü finden Sie die Einstellungen des Gerätes.

**Pfad Telnet:** /Setup

## 2.1 Name

In diesem Feld können Sie einen beliebigen Namen für Ihr Gerät eintragen.

**SNMP-ID:** 2.1

**Pfad Telnet:** /Setup

**Mögliche Werte:**

- max. 16 Zeichen

## 2.2 WAN

Dieses Menü enthält die Konfiguration des Wide-Area-Network (WAN).

**SNMP-ID:** 2.2

**Pfad Telnet:** /Setup

### 2.2.18 Backup-St.-Sekunden

Wartezeit bei Ausfall einer Gegenstelle, nach der die Backup-Verbindung aufgebaut wird.

**SNMP-ID:** 2.2.18

**Pfad Telnet:** /Setup/WAN

**Mögliche Werte:**

- max. 4 Zeichen

**Default:** 30

### 2.2.10 RR-Versuche

Geben sie hier die Anzahl der Rückrufversuche bei Verbindungen mit automatischem Rückruf an.

**SNMP-ID:** 2.2.10

**Pfad Telnet:** /Setup/WAN

**Mögliche Werte:**

- 0 bis 9 Versuche

**Default:** 3

## 2.2.9 Schutz

Hier stellen Sie ein, unter welchen Umständen das Gerät ankommende Rufe annimmt.

**SNMP-ID:** 2.2.9

**Pfad Telnet:** /Setup/WAN/Schutz

**Mögliche Werte:**

- kein: das Gerät nimmt alle Anrufe entgegen.
- Nummer: das Gerät nimmt einen Ruf nur entgegen, wenn der Anrufer in der Nummernliste steht und seine Rufnummer übermittelt wird.
- geprueft:das Gerät nimmt einen Ruf nur entgegen, wenn der Anrufer in der Nummernliste steht, seine Rufnummer übermittelt wird und die übermittelte Rufnummer von der Vermittlungsstelle geprüft wurde.

**Default:** kein

## 2.2.2 Einwahl-Gegenstellen

Konfigurieren Sie hier die ISDN-Gegenstellen, zu denen Ihr Router Verbindungen aufbauen und Daten übertragen soll.

**SNMP-ID:** 2.2.2

**Pfad Telnet:** /Setup/WAN

Werden in zwei Gegenstellenlisten (z. B. DSL-Breitband-Gegenstellen und Einwahl-Gegenstellen) Einträge mit identischen Namen für die Gegenstelle vorgenommen, verwendet das LANCOM beim Verbindungsaufbau zu der entsprechenden Gegenstelle automatisch das “schnellere” Interface. Das andere Interface wird in diesem Fall als Backup verwendet. Werden in der Liste der DSL-Breitband-Gegenstellen weder Access Concentrator noch Service angegeben, stellt der Router eine Verbindung zum ersten AC her, der sich auf die Anfrage über die Vermittlungsstelle meldet. Für ein ggf. vorhandenes DSLoL-Interface gelten die gleichen Einträge wie für ein DSL-Interface. Die Einträge dazu werden in der Liste der DSL-Breitband-Gegenstellen vorgenommen.

### 2.2.2.1 Gegenstelle

Geben Sie hier den Namen der Gegenstelle ein.

**SNMP-ID:** 2.2.2.1

**Pfad Telnet:** /Setup/WAN/Einwahl-Gegenstellen

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen.

**Default:** Leer

### 2.2.2.2 Rufnummer

Eine Rufnummer wird nur benötigt, wenn die Gegenstelle angerufen werden soll. Das Feld kann leer bleiben, wenn lediglich Rufe angenommen werden sollen. Mehrere Rufnummern für dieselbe Gegenstelle können in der RoundRobin-Liste eingetragen werden.

**SNMP-ID:** 2.2.2.2

**Pfad Telnet:** /Setup/WAN/Einwahl-Gegenstellen

**Mögliche Werte:**

- max. 31 Zeichen

**Default:** Leer

### 2.2.2.3 B1-HZ

Die Verbindung wird abgebaut, wenn sie für die eingestellte Dauer nicht benutzt wurde.

**SNMP-ID:** 2.2.2.3

**Pfad Telnet:** /Setup/WAN/Einwahl-Gegenstellen

**Mögliche Werte:**

- 0 bis 9999

**Default:** 0

### 2.2.2.4 B2-HZ

Haltezeit für Bündelungen: Der zweite B-Kanal in einer Bündelung wird abgebaut, wenn er für die eingestellte Dauer nicht benutzt wurde.

**SNMP-ID:** 2.2.2.4

**Pfad Telnet:** /Setup/WAN/Einwahl-Gegenstellen

**Mögliche Werte:**

- 0 bis 9999

**Default:** 0

### 2.2.2.5 Layername

Wählen Sie einen Eintrag aus der Layer-Liste aus, der für diese Gegenstelle verwendet werden soll.

In der Layer-Liste befinden sich bereits einige Einträge mit häufig benötigten Standardeinstellungen, die Sie hier verwenden können. Den Eintrag PPPHDLC z. B. sollten sie verwenden, um zu einem Internetprovider eine PPP-Verbindung aufzubauen.

**SNMP-ID:** 2.2.2.5

**Pfad Telnet:** /Setup/WAN/Einwahl-Gegenstellen

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Layer.

**Default:** Leer

### 2.2.2.6 Rückruf

Wenn Sie den Rückruf einschalten, dann wird ein Ruf von dieser Gegenstelle nicht direkt angenommen, sondern die Gegenstelle zurückgerufen.

Dies ist z. B. nützlich um bei der Gegenseite die Telefongebühren zu minimieren.

Wählen Sie mit Überprüfung des Namens, wenn Sie sicherstellen wollen, dass sich die Gegenstelle authentifizieren muss, bevor der Rückruf erfolgt.

Wenn Sie das schnelle Verfahren wählen, dann kann der Rückruf innerhalb weniger Sekunden erfolgen. Die Gegenstelle muss dieses Verfahren unterstützen und Sie müssen auf der Gegenseite die Option Rückruf erwarten einschalten. Außerdem muss die Gegenstelle in der Nummernliste eingetragen sein.

**SNMP-ID:** 2.2.2.6

**Pfad Telnet:** /Setup/WAN/Einwahl-Gegenstellen

**Mögliche Werte:**

- Nein: Es wird nicht zurückgerufen.
- Auto: Wenn die Gegenstelle in der Nummernliste gefunden wird, so wird diese zurückgerufen. Hierzu wird der Ruf zunächst abgelehnt und, sobald der Kanal wieder frei ist, zurückgerufen (Dauer ca. 8 Sekunden). Wird die Gegenstelle nicht in der Nummernliste gefunden, so wird sie zunächst als DEFAULT-Gegenstelle angenommen, und der Rückruf wird während der Protokollverhandlung ausgehandelt. Dabei fällt eine Gebühr von einer Einheit an.
- Name: Bevor ein Rückruf erfolgt, wird immer eine Protokollverhandlung durchgeführt, auch wenn die Gegenstelle in der Nummernliste gefunden wurde (z. B. für Rechner mit Windows, die sich auf dem Gerät einwählen). Dabei fallen
- geringe Gebühren an.
- fast: Wenn die Gegenstelle in der Nummernliste gefunden wird, wird der schnelle Rückruf durchgeführt, d.h., der LANCOM sendet ein spezielles Signal zur Gegenstelle und ruft sofort zurück, wenn der Kanal wieder frei ist. Nach ca. 2 Sekunden steht die Verbindung. Nimmt die Gegenstelle den Ruf nicht unmittelbar nach dem Signal zurück, so erfolgt zwei Sekunden später ein Rückfall auf das normale Rückrufverfahren (Dauer wieder ca. 8 Sekunden). Dieses Verfahren steht nur an DSS1-Anschlüssen zur Verfügung.
- Looser: Benutzen Sie die Option 'Looser', wenn von der Gegenstelle ein Rückruf erwartet wird. Diese Einstellung erfüllt zwei Aufgaben gleichzeitig. Zum einen sorgt sie dafür, dass ein eigener Verbindungsaufbau zurückgenommen wird, wenn ein Ruf von der gerade angerufenen Gegenstelle hereinkommt, zum anderen wird mit dieser Einstellung die Funktion aktiviert, auf das schnelle Rückruf-Verfahren reagieren zu können. D.h., um den schnellen Rückruf nutzen zu können, muss sich der Anrufer im 'Looser'-Modus befinden, während beim Angerufenen der Rückruf auf 'LANCOM Systems' eingestellt sein muss.

**Default:** Nein

Die Einstellung 'Name' bietet die höchste Sicherheit, wenn sowohl ein Eintrag in der Nummernliste als auch in der PPP-Liste konfiguriert ist. Die Einstellung 'LANCOM' ermöglicht die schnellste Rückrufmethode zwischen zwei LANCOM Systems-Routern.

Bei Windows-Gegenstellen muss die Einstellung 'Name' gewählt werden.

## 2.2.3 RoundRobin

Wenn eine Gegenstelle unter mehreren Rufnummern erreichbar ist, können Sie zusätzliche Rufnummern in dieser Liste eingeben.

**SNMP-ID:** 2.2.3

**Pfad Telnet:** /Setup/WAN

### 2.2.3.1 Gegenstelle

Wählen Sie hier den Namen einer Gegenstelle aus der Gegenstellen-Liste.

**SNMP-ID:** 2.2.3.1

**Pfad Telnet:** /Setup/WAN/RoundRobin

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen

**Default:** Leer

### 2.2.3.2 Round-Robin

Geben Sie hier die weiteren Rufnummern für diese Gegenstelle ein. Trennen Sie die einzelnen Rufnummern durch Bindestriche.

**SNMP-ID:** 2.2.3.2

**Pfad Telnet:** /Setup/WAN/RoundRobin

#### 2.2.3.3 Anf

Geben Sie an, ob der nächste Verbindungsaufbau mit der zuletzt erfolgreich erreichten Nummer oder immer mit der ersten Nummer durchgeführt werden soll.

**SNMP-ID:** 2.2.3.3

**Pfad Telnet:** /Setup/WAN/RoundRobin

**Mögliche Werte:**

- Erster
- letzter

**Default:** letzter

### 2.2.4 Layer

Stellen Sie hier einzelne Protokolle zu 'Layern' zusammen, die beim Übertragen von Daten zu anderen Routern benutzt werden sollen.

**SNMP-ID:** 2.2.4

**Pfad Telnet:** /Setup/WAN

#### 2.2.4.1 Layername

Unter diesem Namen wird der Layer in den Gegenstellenlisten ausgewählt.

**SNMP-ID:** 2.2.4.1

**Pfad Telnet:** /Setup/WAN/Layer

**Mögliche Werte:**

- max. 9 Zeichen

**Default:** leer

#### 2.2.4.2 Encaps.

Für die Datenpakete können Sie zusätzliche Kapselungen einstellen.

**SNMP-ID:** 2.2.4.2

**Pfad Telnet:** /Setup/WAN/Layer

**Mögliche Werte:**

- Transparent: Keine zusätzliche Kapselung.
- Ethernet: Kapselung als Ethernet-Frames.
- LLC-MUX: Multiplexing über ATM mit LLC/SNAP-Kapselung nach RFC 2684. Mehrere Protokolle können im selben VC (Virtual Channel) übertragen werden.
- VC-MUX: Multiplexing über ATM durch Aufbau zusätzlicher VCs nach RFC 2684.

**Default:** ETHER

#### 2.2.4.3 Lay-3

Folgende Optionen stehen für die Vermittlungsschicht (oder Netzwerkschicht) zur Verfügung:

**SNMP-ID:** 2.2.4.3

**Pfad Telnet:** /Setup/WAN/Layer

**Mögliche Werte:**

- Transparent: Es wird kein zusätzlicher Header eingefügt.
- PPP: Der Verbindungsaufbau erfolgt nach dem PPP-Protokoll (im synchronen Modus, d.h. bitorientiert).

  Die Konfigurationsdaten werden der PPP-Tabelle entnommen.
- AsyncPPP: Wie 'PPP', nur wird der asynchrone Modus verwendet. PPP arbeitet also zeichenorientiert.
- ... mit Script: Alle Optionen können wahlweise mit eigenem Script ausgeführt werden. Das Script wird in der Script-Liste angegeben.
- DHCP: Zuordnung der Netzwerkparameter über DHCP.

**Default:** PPP

### 2.2.4.4 Lay-2

In diesem Feld wird der obere Teil der Sicherungsschicht (Data Link Layer) konfiguriert.

**SNMP-ID:** 2.2.4.4

**Pfad Telnet:** /Setup/WAN/Layer

**Mögliche Werte:**

- Transparent: Es wird kein zusätzlicher Header eingefügt.
- X.75LAPB: Verbindungsaufbau nach X.75 und LAPM (Link Access Procedure Balanced).
- PPPoE: Kapselung der PPP-Protokollinformationen in Ethernet-Frames.

**Default:** X.75LAPB

### 2.2.4.5 L2-Opt.

Hier können Sie die Kompression der übertragenen Daten und die Bündelung von Kanälen aktivieren. Die gewählte Option wird nur dann wirksam, wenn sie sowohl von den verwendeten Schnittstellen als auch von den gewählten Layer-2- und Layer-3-Protokollen unterstützt wird. Weitere Informationen finden Sie im Abschnitt 'ISDN-Kanalbündelung mit MLPPP'

**SNMP-ID:** 2.2.4.5

**Pfad Telnet:** /Setup/WAN/Layer

**Mögliche Werte:**

- keine
- Kompression
- Kanalbündelung
- Kompr. + Bündelung

**Default:** keine

### 2.2.4.6 Lay-1

In diesem Feld wird der untere Teil der Sicherungsschicht (Data Link Layer) für die WAN-Layer konfiguriert.

**SNMP-ID:** 2.2.4.6

**Pfad Telnet:** /Setup/WAN/Layer

**Mögliche Werte:**

- AAL-5: ATM-Anpassungsschicht
- ETH: Transparentes Ethernet nach IEEE 802.3.

- HDLC64K: Sicherung und Synchronisation der Datenübertragung nach HDLC (im 7- oder 8-bit-Modus).
- HDLC56K: Sicherung und Synchronisation der Datenübertragung nach HDLC (im 7- oder 8-bit-Modus).
- V110_9K6: Übertragung nach V.110 mit maximal 9.600 bit/Sekunde, z. B. für Einwahl per HSCSD-Mobiltelefon
- V110_19K2: Übertragung nach V.110 mit maximal 19.200 bit/Sekunde
- V110_38K4: Übertragung nach V.110 mit maximal 38.400 bit/Sekunde
- Serial: Für Verbindungen über ein Analog-Modem oder Mobilfunkmodem mit AT-Schnittstelle. Das Modem kann an das Gerät angeschlossen sein an der seriellen Schnittstelle (Outband) oder mit USB-nach-Seriell Wandler an einer USB-Schnittstelle. Einige Modelle verfügen über einen CardBus-Slot zur Aufnahme einer entsprechenden Karte. Einige Modelle verfügen über ein integriertes, internes Modem.
- Modem: Für Verbindungen über die interne Modememulation beim Einsatz als V.90 Hostmodem über ISDN. Die Verwendung des internen Modems erfordert ggf. eine zusätzliche Software-Option für der Gerät.
- VDSL: VDSL2-Datenübertragung nach ITU G.993.2

**Default:** HDLC64K

Die Umfang der möglichen Werte ist abhängig vom verwendeten Hardware-Modell.

## 2.2.5 PPP

Damit Ihr Router PPP- bzw. PPTP-Verbindungen aufbauen kann, müssen Sie in dieser Liste für jede Gegenstelle die entsprechenden Parameter wie Name und Passwort eintragen.

**SNMP-ID:** 2.2.5

**Pfad Telnet:** /Setup/WAN

### 2.2.5.1 Gegenstelle

Geben Sie hier den Namen der Gegenstelle ein. Dieser Name muss mit einem Eintrag in der Liste der Gegenstellen übereinstimmen.

Sie können auch direkt einen Namen aus der Liste der Gegenstellen auswählen.

**SNMP-ID:** 2.2.5.1

**Pfad Telnet:** /Setup/WAN/PPP

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen.

**Default:** Leer

**Besondere Werte:** DEFAULT: Bei der PPP-Verhandlung meldet sich die einwählende Gegenstelle mit ihrem Namen beim LANCOM an. Anhand des Namens kann das LANCOM aus der PPP-Tabelle die zulässigen Werte für die Authentifizierung entnehmen. Manchmal kann die Gegenstelle bei Verhandlungsbeginn nicht über Rufnummer (ISDN-Einwahl), IP-Adresse (PPTP-Einwahl) oder MAC-Adresse (PPPoE-Einwahl) identifiziert werden, die zulässigen Protokolle können also im ersten Schritt nicht ermittelt werden. In diesen Fällen wird die Authentifizierung zunächst mit den Protokollen vorgenommen, die für die Gegenstelle mit dem Namen DEFAULT aktiviert sind. Wenn die Gegenstelle mit diesen Einstellungen erfolgreich authentifiziert wurde, können auch die für die Gegenstelle zulässigen Protokolle ermittelt werden.

Wenn bei der Authentifizierung mit den unter DEFAULT eingetragenen Protokollen ein Protokoll verwendet wurde, das für die Gegenstelle nicht erlaubt ist, dann wird eine erneute Authentifizierung mit den erlaubten Protokollen durchgeführt.

### 2.2.5.10 Rechte

Gibt die Protokolle an, die zu dieser Gegenstelle geroutet werden können.

**SNMP-ID:** 2.2.5.10

**Pfad Telnet:** /Setup/WAN/PPP

**Mögliche Werte:**

- IP
- IP+NBT
- IPX
- IP+IPX
- IP+NBT+IPX

**Default:** IP

### 2.2.5.11 Authent-response

Verfahren zur Sicherung der PPP-Verbindung, die der Router bei der Einwahl in eine Gegenstelle anbietet.

**SNMP-ID:** 2.2.5.11

**Pfad Telnet:** /Setup/WAN/PPP

**Mögliche Werte:**

- PAP
- CHAP
- MS-CHAP
- MS-CHAPv2 (Mehrfachauswahl möglich)

**Default:** PAP, CHAP, MS-CHAP, MS-CHAPv2

Das LANCOM verwendet nur die hier aktivierten Protokolle, eine andere Verhandlung mit der Gegenstelle ist nicht möglich.

### 2.2.5.2 Authent.request

Verfahren zur Sicherung der PPP-Verbindung, die der Router von der Gegenstelle erwartet.

**SNMP-ID:** 2.2.5.2

**Pfad Telnet:** /Setup/WAN/PPP

**Mögliche Werte:**

- PAP
- CHAP
- MS-CHAP
- MS-CHAPv2
- (Mehrfachauswahl möglich)

**Default:** kein Eintrag

### 2.2.5.3 Passwort

Passwort, das von Ihrem Router an die Gegenstelle übertragen wird (falls gefordert). Ein * in der Liste zeigt an, dass ein Eintrag vorhanden ist.

**SNMP-ID:** 2.2.5.3

**Pfad Telnet:** /Setup/WAN/PPP

**Mögliche Werte:**

- max. 32 Zeichen

**Default:** leer

### 2.2.5.4 Zeit

Zeit zwischen zwei Überprüfungen der Verbindung mit LCP (siehe auch LCP). Diese Zeit geben Sie in Vielfachen von 10 Sekunden ein (also z. B. 2 für 20 Sekunden). Der Wert ist gleichzeitig die Zeit zwischen zwei Überprüfungen der Verbindung nach CHAP. Diese Zeit geben Sie in Minuten ein. Für Gegenstellen mit Windows-Betriebssystem muss die Zeit auf '0' gesetzt werden!

**SNMP-ID:** 2.2.5.4

**Pfad Telnet:** /Setup/WAN/PPP

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

### 2.2.5.5 Wdh.

Anzahl der Wiederholungen für den Überprüfungsversuch. Mit mehreren Wiederholungen schalten Sie den Einfluss kurzfristiger Leitungsstörungen aus. Erst wenn alle Versuche erfolglos bleiben, wird die Verbindung abgebaut. Der zeitliche Abstand zwischen zwei Wiederholungen beträgt 1/10 der Zeit zwischen zwei Überprüfungen. Gleichzeitig die Anzahl der „Configure Requests", die der Router maximal aussendet, bevor es von einer Leitungsstörung ausgeht und selber die Verbindung abbaut.

**SNMP-ID:** 2.2.5.5

**Pfad Telnet:** /Setup/WAN/PPP

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 5

### 2.2.5.6 Username

Name, mit dem sich Ihr Router bei der Gegenstelle anmeldet. Ist hier kein Eintrag vorhanden, wird der Gerätename Ihres Routers verwendet.

**SNMP-ID:** 2.2.5.6

**Pfad Telnet:** /Setup/WAN/PPP

**Mögliche Werte:**

- max. 64 Zeichen

### 2.2.5.7 Conf

Mit diesem Parameter wird die Arbeitsweise des PPPs beeinflusst. Der Parameter ist in der RFC 1661 definiert und wird hier nicht näher beschrieben. Falls Sie keine PPP-Verbindungen aufbauen können, finden Sie in dieser

RFC im Zusammenhang mit der PPP-Statistik des Routers Hinweise zur Behebung der Störung. Im allgemeinen sind die Default-Einstellungen ausreichend. Dieser Parameter kann nur über LANconfig, SNMP oder TFTP verändert werden!

**SNMP-ID:** 2.2.5.7

**Pfad Telnet:** /Setup/WAN/PPP

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 10

### 2.2.5.8 Fail

Mit diesem Parameter wird die Arbeitsweise des PPPs beeinflusst. Der Parameter ist in der RFC 1661 definiert und wird hier nicht näher beschrieben. Falls Sie keine PPP-Verbindungen aufbauen können, finden Sie in diesem RFC im Zusammenhang mit der PPP-Statistik des Routers Hinweise zur Behebung der Störung. Im allgemeinen sind die Default-Einstellungen ausreichend. Dieser Parameter kann nur über LANconfig, SNMP oder TFTP verändert werden!

**SNMP-ID:** 2.2.5.8

**Pfad Telnet:** /Setup/WAN/PPP

**Mögliche Werte:**

- max. 10 numerische Zeichen

**Default:** 5

### 2.2.5.9 Term

Mit diesem Parameter wird die Arbeitsweise des PPPs beeinflusst. Der Parameter ist in der RFC 1661 definiert und wird hier nicht näher beschrieben. Falls Sie keine PPP-Verbindungen aufbauen können, finden Sie in diesem RFC im Zusammenhang mit der PPP-Statistik des Routers Hinweise. Im allgemeinen sind die Default-Einstellungen ausreichend. Dieser Parameter kann nur über LANconfig, SNMP oder TFTP verändert werden.

**SNMP-ID:** 2.2.5.9

**Pfad Telnet:** /Setup/WAN/PPP

**Mögliche Werte:**

- max. 10 numerische Zeichen

**Default:** 2

## 2.2.6 Ankommende Rufnummern

Anhand der Rufnummern in dieser Liste kann Ihr Router erkennen, von welcher Gegenstelle ein ankommender Ruf stammt.

**SNMP-ID:** 2.2.6

**Pfad Telnet:** /Setup/WAN

### 2.2.6.1 Rufnummer

Tragen Sie hier die Rufnummer ein, die übermittelt wird, wenn Sie von einer bestimmten Gegenstelle angerufen werden.

Normalerweise ist das die Nummer der Gegenstelle zusammen mit der zugehörigen Ortsvorwahl samt führender Null, z. B. 0221445566.

Bei Gegenstellen im Ausland müssen Sie noch die entsprechende Ländervorwahl mit zwei führenden Nullen voranstellen, z. B. 0049221445566.

**Pfad Telnet**: LCOS Menübaum/Setup/WAN/Ankommende-Rufnummern

### 2.2.6.2 Gegenstelle

Tragen Sie den Namen der betreffenden Gegenstelle ein.

Wenn der Router eine Gegenstelle anhand ihrer Rufnummer identifiziert hat, dann wird in der Liste der Gegenstellen ein Eintrag mit dem diesem Namen gesucht und die zugehörigen Einstellungen für die Verbindung verwendet.

**Pfad Telnet**: LCOS Menübaum/Setup/WAN/Ankommende-Rufnummern

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen

**Default:** Leer

## 2.2.8 Skripte

Wenn beim Verbinden mit einer Gegenstelle die Abarbeitung eines Login-Scripts notwendig ist, dann tragen Sie es hier ein.

**SNMP-ID:** 2.2.8

**Pfad Telnet:** /Setup/WAN

### 2.2.8.1 Gegenstelle

Geben Sie hier den Namen der Gegenstelle ein. Diese Gegenstelle sollte bereits in der Liste der Gegenstellen vorhanden sein.

Sie können auch direkt einen Eintrag aus der Liste der Gegenstellen auswählen.

**SNMP-ID:** 2.2.8.1

**Pfad Telnet:** /Setup/WAN/Scripte

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen

**Default:** Leer

### 2.2.8.2 Skripte

Geben Sie hier das Login-Script für diese Gegenstelle ein.

Damit dieses Script verwendet wird, müssen Sie in der Liste der Gegenstellen für diese Gegenstelle einen Layer mit passenden Protokollen einstellen.

**SNMP-ID:** 2.2.8.2

**Pfad Telnet:** /Setup/WAN/Scripte

## 2.2.11 Router-Interface

Hier können Sie für jedes vom Router verwendete WAN-Interface weitere Einstellungen (wie z. B. die Rufnummer) eingeben.

**SNMP-ID:** 2.2.11

**Pfad Telnet:** /Setup/WAN

### 2.2.11.1 Ifc

WAN-Interface, auf das sich die Einstellungen aus diesem Eintrag beziehen.

**SNMP-ID:** 2.2.11.1

**Pfad Telnet:** /Setup/WAN/Router-Interface

**Mögliche Werte:**

- Auswahl aus der Liste der verfügbaren WAN-Interfaces, z. B. S0-1, S0-2 oder EXT.

### 2.2.11.2 MSN/EAZ

Geben Sie hier die Rufnummern für dieses Interface an, auf denen der Router eingehende Rufe annehmen soll. In der Regel sind diese Nummern die Rufnummern des ISDN-Anschlusses ohne Vorwahl (MSN) beziehungsweise hinter einer Telefonanlage die interne Rufnummer (interne MSN). Sie können mehr als eine Nummer eingeben, indem Sie die einzelnen Nummern durch Semikolon voneinander trennen. Dabei wird die erste Rufnummer für ausgehende Rufe verwendet.

**SNMP-ID:** 2.2.11.2

**Pfad Telnet:** /Setup/WAN/Router-Interface

**Mögliche Werte:**

- max. 30 Zeichen

**Default:** leer

Wenn Sie hier eine beliebige Nummer außerhalb Ihres MSN-Nummernpools angeben, nimmt der Router gar keine Rufe mehr an.

Wenn Sie hier keine Nummer angeben, nimmt der Router jeden Ruf an.

### 2.2.11.3 CLIP

Aktivieren Sie diese Option, wenn eine vom Router angerufene Gegenstelle Ihre Rufnummer nicht sehen soll.

**SNMP-ID:** 2.2.11.3

**Pfad Telnet:** /Setup/WAN/Router-Interface

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

Diese Funktion muss von Ihrem Netzbetreiber unterstützt werden.

### 2.2.11.8 Y-Verbindung

Legen Sie in der Router-Interface-Liste mit dem Eintrag für die Y-Verbindung fest, was geschehen soll, wenn während einer laufenden Verbindung mit Kanalbündelung der Wunsch nach einer zweiten Verbindung zu einer anderen Gegenstelle angemeldet wird.

Y-Verbindung Ein: Der Router unterbricht die Bündelverbindung, um die zweite Verbindung zur anderen Gegenstelle aufzubauen. Wenn der zweite Kanal wieder frei wird, holt sich die Bündelverbindung diesen Kanal automatisch wieder zurück (bei statischer Bündelung immer, bei dynamischer nur bei Bedarf).

Y-Verbindung Aus: Der Router hält die bestehende Bündelverbindung, die zweite Verbindung muss warten.

**SNMP-ID:** 2.2.11.8

**Pfad Telnet:** /Setup/WAN/Router-Interface

**Mögliche Werte:**

- Ein
- Aus

**Default:** Ein

Bitte beachten Sie, dass bei Verwendung der Kanalbündelung die Kosten für zwei Verbindungen anfallen. Dabei sind keine weiteren Verbindungen über die LANCAPI möglich! Setzen Sie die Kanalbündelung also nur dann ein, wenn die doppelte Übertragungsleistung auch tatsächlich ausgenutzt werden kann.

### 2.2.11.9 Rufannahme

Geben Sie hier an, ob Anrufe auf diesem ISDN-Interface entgegengenommen werden sollen oder nicht.

**SNMP-ID:** 2.2.11.9

**Pfad Telnet:** /Setup/WAN/Router-Interface

**Mögliche Werte:**

- Alle
- keinen

**Default:** Alle

Haben Sie eine MSN zur Geräte-Konfiguration angegeben (Management / Admin), so werden Anrufe mit dieser MSN ungeachtet der hiesigen Auswahl angenommen.

## 2.2.13 Manuelle Wahl

Dieses Menü enthält die Einstellungen für das Manuelle Wählen.

**SNMP-ID:** 2.2.13

**Pfad Telnet:** /Setup/WAN

### 2.2.13.2 Abbau

Trennt die Verbindung zur Gegenstelle, die als Parameter angegeben wird.

**SNMP-ID:** 2.2.13.2

**Pfad Telnet:** /Setup/WAN/Manuelle-Wahl

**Mögliche Werte:**

- Parameter: Name einer im Gerät definierten Gegenstelle.

### 2.2.13.1 Aufbau

Baut eine Verbindung zur Gegenstelle auf, die als Parameter angegeben wird.

**SNMP-ID:** 2.2.13.1

**Pfad Telnet:** /Setup/WAN/Manuelle-Wahl

**Mögliche Werte:**

- Parameter: Name einer im Gerät definierten Gegenstelle.

## 2.2.17 Kanal-Liste

Hier können Sie festlegen, über welche Kanäle die Verbindungen zu bestimmten Gegenstellen hergestellt werden sollen.

**SNMP-ID:** 2.2.17

**Pfad Telnet:** /Setup/WAN

### 2.2.17.1 Gegenstelle

Wählen Sie hier den Namen einer Gegenstelle aus der Gegenstellen-Liste.

**SNMP-ID:** 2.2.17.1

**Pfad Telnet:** /Setup/WAN/Kanal-Liste

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen.

**Default:** Leer

### 2.2.17.2 min

Legen Sie fest, wie viele Kanäle zu dieser Gegenstelle aufgebaut werden sollen.

Es werden beim Verbindungsaufbau zunächst so viele Kanäle aufgebaut, wie unter Mindestens angegeben. Bei Bedarf werden automatisch weitere Kanäle aufgebaut, aber niemals mehr, als unter Höchstens angegeben.

**SNMP-ID:** 2.2.17.2

**Pfad Telnet:** /Setup/WAN/Kanal-Liste

**Mögliche Werte:**

- max. 2 Zeichen

**Default:** 0

### 2.2.17.3 max

Legen Sie fest, wie viele Kanäle zu dieser Gegenstelle aufgebaut werden sollen.

Es werden beim Verbindungsaufbau zunächst so viele Kanäle aufgebaut, wie unter Mindestens angegeben. Bei Bedarf werden automatisch weitere Kanäle aufgebaut, aber niemals mehr, als unter Höchstens angegeben.

**SNMP-ID:** 2.2.17.3

**Pfad Telnet:** /Setup/WAN/Kanal-Liste

**Mögliche Werte:**

- max. 2 Zeichen

**Default:** 0

### 2.2.17.4 Anf

Hier können Sie festlegen, welche und in welcher Reihenfolge Kanäle oder Interfaces für diese Verbindung verwendet werden sollen. Dies ist insbesondere dann sinnvoll, wenn sie eine Verbindung fest an bestimmte Interfaces binden wollen oder wenn eine Kanalbündelung über mehr als 2 Kanäle erfolgen soll. Wenn Sie dieses Feld frei lassen, dann werden alle verfügbaren Kanäle oder Interfaces in beliebiger Reihenfolge verwendet.

Einen Kanal definieren Sie, indem Sie den Namen des Interfaces angeben (z. B. S0, G703 oder EXT, falls vorhanden), gefolgt von einem Bindestrich, gefolgt von der Nummer des Interfaces (außer X21, welches ohne Interface-Nummer eindeutig ist). Bei einigen Interfaces kann bei Bedarf zusätzlich eine Kanalnummer angegeben werden (z. B. bedeutet S0-1-2 Kanal 2 am SO-Bus 1). Weitere Kanal-Definitionen werden durch Semikolon voneinander getrennt.

S0-1 ist beispielsweise beide Kanäle von S0-Bus 1, S0-3-2 ist der zweite Kanal auf dem dritten S0- Bus. Wenn Sie in das Feld S0-1-1;S0-3-2 eintragen, dann werden diese Kanäle in der angegebenen Reihenfolge verwendet.

**SNMP-ID:** 2.2.17.4

**Pfad Telnet:** /Setup/WAN/Kanal-Liste

**Mögliche Werte:**

- Liste der möglichen Interfaces.

**Default:** Leer

ADSL und DSL sind zwar gültige Interface-Namen, ihre Verwendung wird jedoch schon durch die entsprechenden DSL-Ports im Gegenstellen-Eintrag bzw. durch den verwendeten Layer vorgegeben.

## 2.2.19 DSL-Breitband-Gegenstellen

Konfigurieren Sie hier die DSL-Breitband-Gegenstellen, zu denen Ihr Router Verbindungen aufbauen und Daten übertragen soll.

**SNMP-ID:** 2.2.19

**Pfad Telnet:** /Setup/WAN

### 2.2.19.1 Gegenstelle

Geben Sie hier den Namen der Gegenstelle ein.

**SNMP-ID:** 2.2.19.1

**Pfad Telnet:** /Setup/WAN/DSL-Breitband-Gegenstellen

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen.

**Default:** leer

### 2.2.19.10 Servicename

Die Service-Parameter helfen Ihnen, Ihren Internet-Provider zu spezifizieren. Kontaktieren Sie Ihren Hersteller, um diese Parameter in Erfahrung zu bringen.

**SNMP-ID:** 2.2.19.10

**Pfad Telnet:** /Setup/WAN/Manuelle-Wahl/Gegenstellen/Servicename

**Mögliche Werte:**

- max. 32 numerische Zeichen

**Default:** leer

### 2.2.19.11 ATM-VPI

Geben Sie hier den VPI (Virtual Path Identifier) und den VCI (Virtual Channel Identifier) für Ihre ADSL-Verbindung ein.

Diese Werte werden Ihnen von Ihrem ADSL-Netzbetreiber mitgeteilt. Übliche Werte für VPI/VCI sind zum Beispiel: 0/35, 0/38, 1/32, 8/35, 8/48.

**SNMP-ID:** 2.2.19.11

**Pfad Telnet:** /Setup/WAN/DSL-Breitband-Gegenstellen

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

### 2.2.19.12 ATM-VCI

Geben Sie hier den VPI (Virtual Path Identifier) und den VCI (Virtual Channel Identifier) für Ihre ADSL-Verbindung ein.

Diese Werte werden Ihnen von Ihrem ADSL-Netzbetreiber mitgeteilt. Übliche Werte für VPI/VCI sind zum Beispiel: 0/35, 0/38, 1/32, 8/35, 8/48.

**SNMP-ID:** 2.2.19.12

**Pfad Telnet:** /Setup/WAN/DSL-Breitband-Gegenstellen

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

### 2.2.19.13 ben.-def.-MAC

Tragen Sie hier die zu verwendende eigene MAC-Adresse ein, wenn eine benutzerdefinierte Adresse erforderlich ist.

**SNMP-ID:** 2.2.19.13

**Pfad Telnet:** /Setup/WAN/DSL-Breitband-Gegenstellen

**Mögliche Werte:**

- max. 12 Zeichen

**Default:** 0

### 2.2.19.14 DSL-Ifc(s)

Geben Sie hier die Port-Nummer des DSL-Ports an. Es können auch mehrere angegeben werden. Separieren Sie die Liste entweder mit Kommata (1,2,3,4) oder teilen Sie diese in Bereiche (1-4) auf. Aktivieren Sie die Kanal-Bündelung im verwendeten Layer, um DSL-Anschlüsse zu bündeln .

**Pfad Telnet:** /Setup/WAN/Gegenstellen/DSL-Ifc(s)

**Mögliche Werte:**

- maximal 8 alphanumerische Zeichen

**Default:** leer

### 2.2.19.15 MAC-Typ

Wählen Sie hier aus, welche MAC-Adresse verwendet werden soll. Muss für die Gegenstelle eine bestimmte MAC- Adresse (Benutzerdefiniert) definiert sein, so kann diese im folgenden Feld angegeben werden.

Wird Lokal gewählt, so werden anhand der Geräte-MAC-Adresse weitere virtuelle Adressen für jede WAN-Verbindung gebildet.

Wird Global gewählt, so wird die Geräte-MAC-Adresse für alle Verbindungen verwendet.

**SNMP-ID:** 2.2.19.15

**Pfad Telnet:** /Setup/WAN/DSL-Breitband-Gegenstellen

**Mögliche Werte:**

- global
- lokal
- benutzerdefiniert

**Default:** lokal

### 2.2.19.16 VLAN-ID

Tragen Sie hier die spezifische ID des VLANs ein, um es auf der DSL-Verbindung eindeutig zu identifizieren.

**SNMP-ID:** 2.2.19.16

**Pfad Telnet:** /Setup/WAN/DSL-Breitband-Gegenstellen

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

### 2.2.19.2 Haltezeit / SH Zeit

Geben Sie an, nach wieviel Sekunden die Verbindung zu dieser Gegenstelle getrennt werden soll, wenn in dieser Zeit keine Daten mehr übertragen worden sind.

**SNMP-ID:** 2.2.19.2

**Pfad Telnet:** /Setup/WAN/DSL-Breitband-Gegenstellen

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

**Besondere Werte:** 9999: Der Wert 9999 sorgt für einen sofortigen Verbindungsaufbau ohne zeitliche Begrenzung.

### 2.2.19.3 AC-Name

Über die Parameter Access concentrator und Service wird der zu verwendende Internet-Anbieter eindeutig identifiziert.

Diese Parameter werden Ihnen von Ihrem Internet-Anbieter mitgeteilt.

**SNMP-ID:** 2.2.19.3

**Pfad Telnet:** /Setup/WAN/DSL-Breitband-Gegenstellen

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** leer

### 2.2.19.4 Servicename

Über die Parameter Access concentrator und Service wird der zu verwendende Internet-Anbieter eindeutig identifiziert.

Diese Parameter werden Ihnen von Ihrem Internet-Anbieter mitgeteilt.

**SNMP-ID:** 2.2.19.4

**Pfad Telnet:** /Setup/WAN/DSL-Breitband-Gegenstellen

**Mögliche Werte:**

- max. 32 Zeichen

**Default:** leer

### 2.2.19.5 Layername

Wählen Sie den Kommunikations-Layer aus, der für diese Verbindung verwendet werden soll. Die Konfiguration dieser Layer ist im folgenden Abschnitt beschrieben.

**SNMP-ID:** 2.2.19.5

**Pfad Telnet:** /Setup/WAN/DSL-Breitband-Gegenstellen

**Mögliche Werte:**

- max. 9 Zeichen

**Default:** leer

### 2.2.19.9 AC-Name

Die Parameter für den Access Concentrator und den Service identifizieren den Internet-Provider eindeutig. Diese Parameter teilt Ihnen Ihr Internet-Provider mit.

**SNMP-ID:** 2.2.19.9

**Pfad Telnet:** /Setup/WAN/Manuelle-Wahl/Gegenstellen/AC-Name

**Mögliche Werte:**

- Max. 64 numerische Zeichen

**Default:** leer

## 2.2.20 IP-Liste

Wenn bestimmte Gegenstellen die für eine Verbindung benötigten IP-Parameter nicht automatisch übermitteln, dann tragen Sie diese Werte hier ein.

**SNMP-ID:** 2.2.20

**Pfad Telnet:** /Setup/WAN

### 2.2.20.1 Gegenstelle

Geben Sie hier einen Netbios-Nameserver an, der bei Ausfall des ersten NBNS verwendet werden soll.

**SNMP-ID:** 2.2.20.1

**Pfad Telnet:** /Setup/WAN/IP-Liste

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen.

**Default:** leer

### 2.2.20.2 IP-Adresse

Wenn Ihr Internet-Anbieter Ihnen eine feste, im Internet gültige IP-Adresse zugewiesen hat, dann tragen Sie diese hier ein. Andernfalls lassen Sie dieses Feld leer.

Wenn Sie in Ihrem lokalen Netz einen privaten Adress-Bereich verwenden und dem Gerät eine Adresse aus diesem Bereich zuweisen wollen, dann tragen Sie diese Adresse nicht hier, sondern unter Intranet IP-Adresse ein.

**SNMP-ID:** 2.2.20.2

**Pfad Telnet:** /Setup/WAN/IP-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.2.20.3 IP-Netzmaske

Geben Sie hier die zur obigen Adresse gehörige Netzmaske ein.

**SNMP-ID:** 2.2.20.3

**Pfad Telnet:** /Setup/WAN/IP-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.2.20.4 Gateway

Geben Sie hier die Adresse des Standard-Gateways ein.

**SNMP-ID:** 2.2.20.4

**Pfad Telnet:** /Setup/WAN/IP-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.2.20.5 DNS-Default

Geben Sie hier die Adresse eines Nameservers ein, an den DNS-Anfragen weitergeleitet werden sollen.

Wenn Sie einen Internetprovider oder eine andere Gegenstelle haben, die dem Router beim Einloggen automatisch einen Nameserver zuweist, dann können Sie dieses Feld leer lassen.

**SNMP-ID:** 2.2.20.5

**Pfad Telnet:** /Setup/WAN/IP-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.2.20.6 DNS-Backup

Geben Sie hier einen Nameserver an, der bei Ausfall des ersten DNS verwendet werden soll.

**SNMP-ID:** 2.2.20.6

**Pfad Telnet:** /Setup/WAN/IP-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.2.20.7 NBNS-Default

Geben Sie hier die Adresse eines Netbios-Nameservers ein, an den NBNS-Anfragen weitergeleitet werden sollen.

Wenn Sie einen Internetprovider oder eine andere Gegenstelle haben, die dem Router beim Einloggen automatisch einen Netbios-Nameserver zuweist, dann können Sie dieses Feld leer lassen.

**SNMP-ID:** 2.2.20.7

**Pfad Telnet:** /Setup/WAN/IP-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.2.20.8 NBNS-Backup

IP-Adresse des NetBIOS-Nameservers, an den NBNS-Anfragen weitergeleitet werden sollen. Default: 0.0.0.0. Die IP-Adresse des LANCOM Wireless in diesem Netzwerk wird als NBNS-Server übermittelt, wenn der NetBIOS-Proxy für dieses Netzwerk aktiviert ist. Ist der NetBIOS-Proxy für dieses Netzwerk nicht aktiv, so wird die IP-Adresse aus den globalen TCP/IP-Einstellungen als NBNS-Server übermittelt.

**SNMP-ID:** 2.2.20.8

**Pfad Telnet:** /Setup/WAN/IP-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.2.20.9 Masq.-IP-Addr.

Die Maskierungs-IP-Adresse ist optional. Sie kann eine andere Adresse vorgeben, hinter der unabhängig von der beim Verbindungsaufbau zugewiesenen Adresse maskiert wird.

Ist die Maskierungs-IP-Adresse nicht gesetzt, dann wird zur Maskierung die beim Verbindungsaufbau zugewiesene Adresse verwendet.

**SNMP-ID:** 2.2.20.9

**Pfad Telnet:** /Setup/WAN/IP-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

Diese Einstellung ist zum Beispiel dann erforderlich, wenn während der PPP-Verhandlung eine private Adresse (172.16.x.x) zugewiesen wird. Damit wäre eine normale Maskierung nicht möglich, da solche Adressen im Internet gefiltert werden.

## 2.2.21 PPTP-Gegenstellen

In dieser Tabelle können Sie PPTP-Gegenstellen anzeigen und hinzufügen.

**SNMP-ID:** 2.2.21

**Pfad Telnet:** /Setup/WAN

### 2.2.21.1 Gegenstelle

Die Bezeichnung aus der Liste der DSL-Breitband-Gegenstellen.

**SNMP-ID:** 2.2.21.1

**Pfad Telnet:** /Setup/WAN/PPTP-Gegenstellen

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen

**Default:** Leer

### 2.2.21.3 Port

IP-Port, über den das PPTP-Protokoll läuft. Dem Protokollstandard gemäß sollte immer Port '1.723' angegeben sein.

**SNMP-ID:** 2.2.21.3

**Pfad Telnet:** /Setup/WAN/PPTP-Gegenstellen

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

### 2.2.21.4 SH-Zeit

Geben Sie an, nach wieviel Sekunden die Verbindung zu dieser Gegenstelle getrennt werden soll, wenn in dieser Zeit keine Daten mehr übertragen worden sind.

**SNMP-ID:** 2.2.21.4

**Pfad Telnet:** /Setup/WAN/PPTP-Gegenstellen

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

**Besondere Werte:** Der Wert 9999 sorgt für einen sofortigen Verbindungsaufbau ohne zeitliche Begrenzung.

### 2.2.21.5 Rtg-tag

Routing-Tag für diesen Eintrag.

**SNMP-ID:** 2.2.21.5

**Pfad Telnet:** /Setup/WAN/PPTP-Gegenstellen

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

### 2.2.21.6 IP-Adresse

Geben Sie hier die IP-Adresse der PPTP-Gegenstelle ein.

**SNMP-ID:** 2.2.21.6

**Pfad Telnet:** /Setup/WAN/Manuelle-Wahl/PPTP-Gegenstellen/IP-Adresse

**Mögliche Werte:**

- maximal 63 alphanumerische Zeichen

**Default:** leer

### 2.2.21.7 Verschlüsselung

Geben Sie hier die Schlüssellänge an.

**SNMP-ID:**

2.2.21.7

**Pfad Telnet:**

**Setup** > **WAN** > **PPTP-Gegenstellen**

**Mögliche Werte:**

Aus

40 bit

56 bit

128 bit

**Default:**

Aus

## 2.2.22 Radius

Dieses Menü enthält die Einstellungen für den RADIUS-Server.

**SNMP-ID:** 2.2.22

**Pfad Telnet:** /Setup/WAN

### 2.2.22.1 Aktiv

Schaltet die RADIUS-Authentifizierung ein oder aus.

**SNMP-ID:** 2.2.22.1

**Pfad Telnet:** /Setup/WAN/RADIUS

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

### 2.2.22.3 Auth.-Port

Der TCP/UDP-Port, über den der externe RADIUS-Server erreicht werden kann.

**SNMP-ID:** 2.2.22.3

**Pfad Telnet:** /Setup/WAN/RADIUS

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 1812

### 2.2.22.10 Auth.-Protokolle

Verfahren zur Sicherung der PPP-Verbindung, die der externe RADIUS-Server erlaubt.

Wenn die Gegenstelle ein Internetprovider ist, den Ihr Router anrufen soll, sollten Sie hier kein Verfahren selektieren.

**SNMP-ID:** 2.2.22.10

**Pfad Telnet:** /Setup/WAN/RADIUS

**Mögliche Werte:**

- MS-CHAPv2
- MS-CHAP
- CHAP
- PAP

**Default:** MS-CHAPv2, MS-CHAP, CHAP, PAP

Wenn alle Verfahren selektiert sind, wird jeweils das nächste Verfahren zur Authentifizierung herangezogen, falls das vorherige fehlgeschlagen ist. Wenn keines der Verfahren selektiert ist, wird von der Gegenstelle keine Authentifizierung gefordert.

### 2.2.22.6 CLIP-Operation

Bei der Einwahl von Gegenstellen kann die interne Rufnummernliste oder alternativ ein externer RADIUS-Server zur Authentifizierung verwendet werden.

**SNMP-ID:** 2.2.22.6

**Pfad Telnet:** /Setup/WAN/RADIUS

**Mögliche Werte:**

- Ja: Aktiviert die Nutzung eines externen RADIUS-Servers für die Authentifizierung von Einwahlgegenstellen. Ein in der Rufnummernliste vorhandener, passender Eintrag hat allerdings Vorrang.
- Nein: Es wird kein externer RADIUS-Server für die Authentifizierung von Einwahlgegenstellen verwendet.
- Exklusiv: Aktiviert die Nutzung eines externen RADIUS-Servers als ausschließliche Möglichkeit für die Authentifizierung von Einwahlgegenstellen. Die Rufnummernliste wird nicht berücksichtigt.

**Default:** Nein

Die Einwahlgegenstellen müssen im RADIUS-Server so konfiguriert werden, dass der Name des Eintrags der Rufnummer der einwählenden Gegenstelle entspricht.

### 2.2.22.7 CLIP-Passwort

Kennwort für die Anmeldung von Einwahlgegenstellen an einem externen RADIUS-Server.

**SNMP-ID:** 2.2.22.7

**Pfad Telnet:** /Setup/WAN/RADIUS

**Mögliche Werte:**

- max. 31 Zeichen

**Default:** leer

Die Einwahlgegenstellen müssen im RADIUS-Server so konfiguriert werden, dass alle Einträge für Rufnummern das hier konfigurierte Kennwort verwenden.

### 2.2.22.8 Loopback-Addr.

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

Als Adresse werden verschiedene Eingabeformen akzeptiert:

Name der IP-Netzwerke, deren Adresse eingesetzt werden soll.

"INT" für die Adresse des ersten Intranets.

"DMZ" für die Adresse der ersten DMZ (Achtung: wenn es eine Schnittstelle Namens "DMZ" gibt, dann wird deren Adresse genommen).

LB0 ... LBF für die 16 Loopback-Adressen.

Desweiteren kann eine beliebige IP-Adresse in der Form x.x.x.x angegeben werden.

**SNMP-ID:** 2.2.22.8

**Pfad Telnet:** /Setup/WAN/RADIUS

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

**Default:** leer

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, wird die zugehörige IP-Adresse verwendet.

### 2.2.22.5 PPP-Operation

Bei der Einwahl von PPP-Gegenstellen können die internen Benutzer-Authentifizierungsdaten aus der PPP-Liste oder alternativ ein externer RADIUS-Server zur Authentifizierung verwendet werden.

**SNMP-ID:** 2.2.22.5

**Pfad Telnet:** /Setup/WAN/RADIUS

**Mögliche Werte:**

- Ja: Aktiviert die Nutzung eines externen RADIUS-Servers für die Authentifizierung von PPP-Gegenstellen. Ein in der PPP-Liste vorhandener, passender Eintrag hat allerdings Vorrang.
- Nein: Es wird kein externer RADIUS-Server für die Authentifizierung von PPP-Gegenstellen verwendet.
- Exklusiv: Aktiviert die Nutzung eines externen RADIUS-Servers als ausschließliche Möglichkeit für die Authentifizierung von PPP-Gegenstellen. Die PPP-Liste wird nicht berücksichtigt.

**Default:** Nein

Wenn Sie die PPP-Arbeitsweise auf 'Exklusiv' schalten, werden die internen Benutzer-Authentifizierungsdaten ignoriert, ansonsten haben diese Vorrang.

### 2.2.22.9 Protokoll

Für die Authentifizierung bei einem externen Server kann als Übertragungsprotokoll RADIUS über UDP oder RADSEC über TCP mit TLS verwendet werden.

**SNMP-ID:** 2.2.22.9

**Pfad Telnet:** /Setup/WAN/RADIUS

**Mögliche Werte:**

- RADIUS
- RADSEC

**Default:** RADIUS

### 2.2.22.4 Schlüssel

Geben Sie hier die den Schlüssel (Shared-Secret) Ihres RADIUS-Servers an, mit dem Sie zentral die Benutzer verwalten.

**SNMP-ID:** 2.2.22.4

**Pfad Telnet:** /Setup/WAN/RADIUS

**Default:** leer

### 2.2.22.2 Server-Addresse

Geben Sie hier die IP-Adresse Ihres RADIUS-Servers an, mit dem Sie zentral die Benutzer verwalten.

**SNMP-ID:** 2.2.22.2

**Pfad Telnet:** /Setup/WAN/RADIUS

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

## 2.2.23 Polling-Tabelle

In dieser Tabelle können für nicht PPP-basierte Gegenstellen bis zu 4 IP-Adressen angegeben werden, deren Erreichbarkeit zur Überwachung der Verbindung überprüft werden.

**SNMP-ID:** 2.2.23

**Pfad Telnet:** /Setup/WAN

### 2.2.23.1 Gegenstelle

Name der Gegenstelle, die über diesen Eintrag geprüft werden soll.

**SNMP-ID:** 2.2.23.1

**Pfad Telnet:** /Setup/WAN/Polling-Tabelle

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen.

**Default:** Leer

### 2.2.23.2 IP-Adresse-1

IP-Adressen, an die zur Prüfung der Gegenstelle ICMP-Requests gesendet werden.

**SNMP-ID:** 2.2.23.2

**Pfad Telnet:** /Setup/WAN/Polling-Tabelle

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.2.23.3 Zeit

Geben Sie hier das Ping-Intervall in Sekunden ein.

**SNMP-ID:** 2.2.23.3

**Pfad Telnet:** /Setup/WAN/Polling-Tabelle

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

**Besondere Werte:** Wenn sie sowohl hier als auch bei den Wiederholungen 0 eingeben, werden Standardwerte benutzt.

### 2.2.23.4 Wdh.

Bleibt die Antwort auf einen Ping aus, wird die Gegenstelle in kürzeren Intervallen geprüft. Im Sekundentakt versucht das Gerät dann erneut, die Gegenstelle zu erreichen. Die Anzahl der Wiederholungen gibt an, wie oft dieser Versuch wiederholt wird. Wird hier eine „0“ eingetragen, gilt der Standardwert von 5 Wiederholungen.

**SNMP-ID:** 2.2.23.4

**Pfad Telnet:** /Setup/WAN/Polling-Tabelle

**Mögliche Werte:**

- 0 bis 255
- 0: Verwende Default
- Default: 5 Wiederholungen

**Default:** 0

### 2.2.23.5 IP-Adresse-2

IP-Adressen, an die zur Prüfung der Gegenstelle ICMP-Requests gesendet werden.

**SNMP-ID:** 2.2.23.5

**Pfad Telnet:** /Setup/WAN/Polling-Tabelle

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.2.23.6 IP-Adresse-3

IP-Adressen, an die zur Prüfung der Gegenstelle ICMP-Requests gesendet werden.

**SNMP-ID:** 2.2.23.6

**Pfad Telnet:** /Setup/WAN/Polling-Tabelle

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.2.23.7 IP-Adresse-4

IP-Adressen, an die zur Prüfung der Gegenstelle ICMP-Requests gesendet werden.

**SNMP-ID:** 2.2.23.7

**Pfad Telnet:** /Setup/WAN/Polling-Tabelle

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.2.23.8 Loopback-Addr.

Absenderadresse, die in den Ping eingetragen wird und auf der auch die Ping-Antwort erwartet wird. Als Loopback-Adresse können eingetragen werden: Name eines definierten IP-Netzwerks. 'INT' für die IP-Adresse im ersten Netzwerk mit der Einstellung 'Intranet'. 'DMZ' für die IP-Adresse im ersten Netzwerk mit der Einstellung 'DMZ'.

**SNMP-ID:** 2.2.23.8

**Pfad Telnet:** /Setup/WAN/Polling-Tabelle

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

**Default:** leer

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, wird die zugehörige IP-Adresse verwendet. Name einer Loopback-Adresse. Beliebige andere IP-Adresse.

## 2.2.24 Backup-Gegenstellen

In dieser Tabelle wird für jede Gegenstelle eine Liste der möglichen Backup-Verbindungen angegeben.

**SNMP-ID:** 2.2.24

**Pfad Telnet:** /Setup/WAN

### 2.2.24.1 Gegenstelle

Wählen Sie hier den Namen einer Gegenstelle aus der Gegenstellen-Liste.

**SNMP-ID:** 2.2.24.1

**Pfad Telnet:** /Setup/WAN/Backup-Gegenstellen

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen

**Default:** Leer

### 2.2.24.2 Alternative-Gegenstellen

Geben Sie hier eine oder mehrere Gegenstellen für Backup-Verbindungen an.

**SNMP-ID:** 2.2.24.2

**Pfad Telnet:** /Setup/WAN/Backup-Gegenstellen

**Mögliche Werte:**

- Liste der Backup-Gegenstellen.

**Default:** Leer

### 2.2.24.3 Anf

Geben Sie an, ob der nächste Verbindungsaufbau mit der zuletzt erfolgreich erreichten Nummer oder immer mit der ersten Nummer durchgeführt werden soll.

**SNMP-ID:** 2.2.24.3

**Pfad Telnet:** /Setup/WAN/Backup-Gegenstellen

**Mögliche Werte:**

- letzter
- erster

**Default:** letzter

## 2.2.25 Aktions-Tabelle

In der Aktions-Tabelle können Sie Aktionen definieren, die ausgeführt werden, wenn sich am Zustand einer WAN-Verbindung etwas ändert.

**SNMP-ID:** 2.2.25

**Pfad Telnet:** /Setup/WAN

### 2.2.25.1 Index

Der Index gibt die Position des Eintrags in der Tabelle an und muss daher eindeutig sein. Die Einträge der Aktions-Tabelle werden der Reihe nach ausgeführt, sobald der entsprechende Zustandswechsel der WAN-Verbindung eintritt. Mit dem Eintrag im Feld "Pruefen-auf" kann das Überspringen von Zeilen je nach Auswertung der Aktion ausgelöst werden. Der Index legt die Position der Einträge in der Tabelle fest (in aufsteigender Reihenfolge) und beeinflusst somit maßgeblich das Verhalten der Aktionen, wenn die Option "Pruefen-auf" verwendet wird. Über den Index kann außerdem ein Eintrag aus der Aktions-Tabelle über einen Cron-Job angesprochen werden, z. B. um einen Eintrag zu bestimmten Zeiten zu aktivieren oder zu deaktivieren.

**Pfad Telnet**: /Setup/WAN/Aktions-Tabelle

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

### 2.2.25.2 Hostname

Name der Aktion. Dieser Name kann mit dem Platzhalter %h (Hostname) in den Feldern "Aktion" und "Pruefen-auf" referenziert werden.

**Pfad Telnet**: /Setup/WAN/Aktions-Tabelle

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** leer

### 2.2.25.3 Gegenstelle

Name der Gegenstelle, deren Zustandswechsel die in diesem Eintrag definierte Aktion auslösen soll.

**Pfad Telnet**: /Setup/WAN/Aktions-Tabelle

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen

**Default:** leer

### 2.2.25.4 Sperrzeit

Unterbricht die wiederholte Ausführung der in diesem Eintrag definierten Aktion für die eingestellte Zeit in Sekunden.

**Pfad Telnet**: /Setup/WAN/Aktions-Tabelle

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

### 2.2.25.5 Bedingung

Die Aktion wird ausgeführt, wenn der hier eingestellte Zustandswechsel der WAN-Verbindung eintritt.

**Pfad Telnet**: /Setup/WAN/Aktions-Tabelle

**Mögliche Werte:**

- Aufbau: Die Aktion wird ausgeführt, wenn die Verbindung erfolgreich aufgebaut wurde.
- Abbau: Die Aktion wird ausgeführt, wenn die Verbindung durch das Gerät selbst beendet wurde (z. B. durch eine manuelle Trennung oder den Ablauf einer Haltezeit).
- Ende: Die Aktion wird ausgeführt, wenn die Verbindung beendet wurde (unabhängig vom Grund für den Abbau).
- Fehler: Die Aktion wird ausgeführt, wenn die Verbindung beendet wurde, das Gerät selbst aber diesen Abbau nicht ausgelöst oder erwartet hat.
- Aufbaufehler: Die Aktion wird ausgeführt, wenn ein Verbindungsaufbau gestartet wurde, die Verbindung aber nicht erfolgreich aufgebaut werden konnte.

**Default:** Aufbau

### 2.2.25.6 Aktion

Hier beschreiben Sie die Aktion, die beim Zustandswechsel der WAN-Verbindung ausgeführt werden soll. In jedem Eintrag darf nur eine Aktionen ausgeführt werden.

**Pfad Telnet**: /Setup/WAN/Aktions-Tabelle

**Mögliche Werte:**

- exec: – Mit diesem Prefix leiten Sie alle Befehle ein, wie sie an der Telnet-Konsole eingegeben würden. Sie können z. B. mit der Aktion "exec:do /o/m/d" alle bestehenden Verbindungen beenden.
- dnscheck: – Mit diesem Prefix leiten Sie eine DNS-Namensauflösung ein. Sie können z. B. mit der Aktion "dnscheck:myserver.dyndns.org" die IP-Adresse des angegebenen Servers ermitteln.
- http: – Mit diesem Prefix lösen Sie eine HTTP-Get-Anfrage aus. Sie können z. B. mit der folgenden Aktion eine DynDNS-Aktualisierung bei dyndns.org durchführen:
- http://username:password@members.dyndns.org/nic/update?system=dyndns&hostname=%h&myip=%a
- Die Bedeutung der Platzhalter %h und %a wird in den folgenden Absätzen beschrieben.

- https: – Wie "http:", nur über eine verschlüsselte Verbindung.
- gnudip: – Mit diesem Prefix lösen Sie eine Anfrage über das GnuDIP-Protokoll an einen entsprechenden DynDNS-Server aus. Sie können z. B. mit der folgenden Aktion eine DynDNS-Aktualisierung bei einem DynDNS-Anbieter über das GnuDIP-Protokoll durchführen:
- gnudip://gnudipsrv?method=tcp&user=myserver&domn=mydomain.org
- &pass=password&reqc=0&addr=%a
- Der Zeilenumbruch dient nur der Lesbarkeit und wird nicht in die Aktion eingetragen. Die Bedeutung des Platzhalters %a wird in den folgenden Absätzen beschrieben.
- repeat: – Mit diesem Prefix und der Angabe einer Zeit in Sekunden werden alle Aktionen mit der Bedingung "Aufbau" wiederholt ausgeführt, sobald die Verbindung aufgebaut ist. Mit der Aktion "repeat:300" werden z. B. alle Aufbau-Aktionen alle fünf Minuten wiederholt.
- mailto: – Mit diesem Prefix lösen Sie den Versand einer E-Mail aus. Sie können z. B. mit der folgenden Aktion eine E-Mail an den Systemadministrator versenden, wenn eine Verbindung beendet wurde:
- mailto:admin@mycompany.de?subject=VPN-Verbindung abgebrochen um %t?body=VPN-Verbindung zu Filiale 1 wurde unterbrochen.
- Mögliche Variablen zur Erweiterung der Aktionen:
- %a – WAN-IP-Adresse der WAN-Verbindung, in deren Kontext diese Aktion ausgeführt wird.
- %H – Hostname der WAN-Verbindung, in deren Kontext diese Aktion ausgeführt wird.
- %h – wie %h, nur Hostname in Kleinbuchstaben
- %c – Verbindungsname der WAN-Verbindung, in deren Kontext diese Aktion ausgeführt wird.
- %n – Gerätename
- %s – Seriennummer des Gerätes
- %m – MAC-Adresse des Gerätes (wie im Sysinfo)
- %t – Uhrzeit und Datum, im Format YYYY-MM-DD hh:mm:ss
- %e – Bezeichnung des Fehlers, der bei einem nicht erfolgreichen Verbindungsaufbau gemeldet wurde.
- Das Ergebnis der Aktionen kann im Feld "Pruefen-auf" ausgewertet werden.

**Default:** leer

### 2.2.25.7 Pruefen-Auf

Das Ergebnis der Aktion kann hier ausgewertet werden, um je nach Ergebnis eine bestimmte Anzahl von Einträge beim Abarbeiten der Aktions-Tabelle zu überspringen.

**Pfad Telnet**: /Setup/WAN/Aktions-Tabelle

**Mögliche Werte:**

- contains= – Dieses Prefix prüft, ob das Ergebnis der Aktion die definierte Zeichenkette enthält.
- isequal= – Dieses Prefix prüft, ob das Ergebnis der Aktion der definierten Zeichenkette genau entspricht.
- ?skipiftrue= – Dieses Suffix überspringt die definierte Anzahl von Zeilen in der Liste der Aktionen, wenn das Ergebnis der Abfrage mit "contains" oder "isequal" das Ergebnis WAHR liefert.
- ?skipiffalse= – Dieses Suffix überspringt die definierte Anzahl von Zeilen in der Liste der Aktionen, wenn das Ergebnis der Abfrage mit "contains" oder "isequal" das Ergebnis FALSCH liefert.
- Mögliche Variablen zur Erweiterung der Aktionen:
- Wie bei der Definition der Aktion.

**Default:** leer

### 2.2.25.8 Aktiv

Aktiviert oder deaktiviert diesen Eintrag.

**Pfad Telnet**: /Setup/WAN/Aktions-Tabelle

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

### 2.2.25.9 Besitzer

Besitzer der Aktion. Mit den Rechten dieses Besitzers werden die exec-Aktionen ausgeführt. Verfügt der Besitzer nicht über die notwendigen Rechte (z. B. Administratoren mit Leserechten), so kann die Aktion nicht ausgeführt werden.

**Pfad Telnet**: /Setup/WAN/Aktions-Tabelle

**Mögliche Werte:**

- Auswahl aus den im Gerät definierten Administratoren. max. 16 Zeichen

**Default:** root

## 2.2.26 MTU-Liste

In dieser Tabelle können Sie für bestimmte Gegenstellen eine andere MTU (Maximum Transfer Unit) als die üblicherweise automatisch ausgehandelte definieren.

**SNMP-ID:** 2.2.26

**Pfad Telnet:** /Setup/WAN

### 2.2.26.1 Gegenstelle

Geben Sie hier den Namen der Gegenstelle ein. Dieser Name muss mit einem Eintrag in der Liste der Gegenstellen übereinstimmen.

Sie können auch direkt einen Namen aus der Liste der Gegenstellen auswählen.

**SNMP-ID:** 2.2.26.1

**Pfad Telnet:** /Setup/WAN/MTU-Liste

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen.

**Default:** Leer

### 2.2.26.2 MTU

Hier können Sie zusätzlich zu den automatischen Bestimmungen der verbindungsspezifischen MTU eine manuell konfigurierbare maximale MTU pro Verbindung definieren.

Geben Sie die maximale IP-Paketlänge/-größe in Byte an. Je kleiner der Wert ist, je größer ist die Fragmentierung der Nutzdaten.

**SNMP-ID:** 2.2.26.2

**Pfad Telnet:** /Setup/WAN/MTU-Liste

**Mögliche Werte:**

- max. 4 Zeichen

**Default:** 0

## 2.2.30 Zusaetzliche-PPTP-Gateways

Definieren Sie hier bis zu 32 zusätzliche Gateways um die Verfügbarkeit von PPTP-Gegenstellen sicherzustellen. Jede der PPTP-Gegenstellen hat die Möglichkeit bis zu 33 Gateways zu benutzen. Die zusätzlichen Gateways definieren Sie in einer zusätzlichen Liste.

**SNMP-ID:** 2.2.30

**Pfad Telnet:** /Setup/WAN

### 2.2.30.1 Gegenstelle

Wählen Sie hier aus, für welche PPTP-Gegenstelle dieser Eintrag gelten soll.

**SNMP-ID:** 2.2.30.1

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- Auswahl aus der Liste der definierten PPTP-Gegenstellen

**Default:**

- leer

### 2.2.30.3 Gateway-1

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.3

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:**

- leer

### 2.2.30.4 Rtg-Tag-1

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.4

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:**

0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.5 Gateway-2

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.5

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:**

- leer

### 2.2.30.6 Rtg-Tag-2

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.6

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:**

0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.7 Gateway-3

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.7

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.8 Rtg-Tag-3

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.8

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default: 0**

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.9 Gateway-4

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.9

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.10 Rtg-Tag-4

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.10

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.11 Gateway-5

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.11

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.12 Rtg-Tag-5

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.12

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.13 Gateway-6

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.13

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.14 Rtg-Tag-6

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.14

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.15 Gateway-7

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.15

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.16 Rtg-Tag-7

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.16

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.17 Gateway-8

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.17

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.18 Rtg-Tag-8

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.18

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.19 Gateway-9

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.19

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.20 Rtg-Tag-9

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.20

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.21 Gateway-10

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.21

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.22 Rtg-Tag-10

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.22

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.23 Gateway-11

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.23

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.24 Rtg-Tag-11

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.24

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.25 Gateway-12

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.25

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.26 Rtg-Tag-12

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.26

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.27 Gateway-13

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.27

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.28 Rtg-Tag-13

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.28

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.29 Gateway-14

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.29

**Pfad Telnet:** /Setup/WAN/RADIUS/Zusaetzliche-PPTP-Gateways/Gateway-14

**Mögliche Werte:**

- IP-Adresse oder 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.30 Rtg-Tag-14

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.30

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.31 Gateway-15

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.31

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.32 Rtg-Tag-15

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.32

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.33 Gateway-16

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.33

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.34 Rtg-Tag-16

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.34

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.35 Gateway-17

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.35

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.36 Rtg-Tag-17

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.36

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.37 Gateway-18

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.37

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.38 Rtg-Tag-18

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.38

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.39 Gateway-19

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.39

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.40 Rtg-Tag-19

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.40

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.41 Gateway-20

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.41

**Pfad Telnet:** /Setup/WAN/RADIUS/Zusaetzliche-PPTP-Gateways/Gateway-20

**Mögliche Werte:**

- IP-Adresse oder 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.42 Rtg-Tag-20

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.42

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.43 Gateway-21

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.43

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.44 Rtg-Tag-21

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.44

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.45 Gateway-22

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.45

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.46 Rtg-Tag.22

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.46

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.47 Gateway-23

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.47

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.48 Rtg-Tag-23

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.48

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.49 Gateway-24

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.49

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.50 Rtg-Tag-24

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.50

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.51 Gateway-25

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.51

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.52 Rtg-Tag-25

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.52

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.53 Gateway-26

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.53

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.54 Rtg-Tag-26

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.54

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.55 Gateway-27

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.55

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.56 Rtg-Tag-27

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.56

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.57 Gateway-28

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.57

**Pfad Telnet:** /Setup/WAN/RADIUS/Zusaetzliche-PPTP-Gateways/Gateway-28

**Mögliche Werte:**

- IP-Adresse oder 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.58 Rtg-Tag-28

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.58

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.59 Gateway-29

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.59

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.60 Rtg-Tag-29

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.60

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.61 Gateway-30

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.61

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.62 Rtg-Tag-30

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.62

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.63 Gateway-31

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.63

**Pfad Telnet:** /Setup/WAN/RADIUS/Zusaetzliche-PPTP-Gateways/Gateway-31

**Mögliche Werte:** IP-Adresse oder 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.64 Rtg-Tag-31

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.64

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.65 Gateway-32

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

**SNMP-ID:** 2.2.30.65

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- IP-Adresse
- maximal 63 alphanumerische Zeichen.

**Default:** leer

### 2.2.30.66 Rtg-Tag-32

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

**SNMP-ID:** 2.2.30.66

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- maximal 5 Ziffern

**Default:** 0

Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

### 2.2.30.2 Anfangen-mit

Wählen Sie hier aus, in welcher Reihenfolge die Einträge versucht werden sollen.

**SNMP-ID:** 2.2.30.2

**Pfad Telnet:** /Setup/WAN/Zusaetzliche-PPTP-Gateways

**Mögliche Werte:**

- Zuletzt-verwendetem: Wählt den Eintrag, zu dem zuletzt erfolgreich eine Verbindung hergestellt werden konnte.
- Erstem: Wählt den ersten Eintrag aus allen konfigurierten Gegenstellen aus.
- zufaelligem: Wählt zufällig eine der konfigurierten Gegenstellen aus. Mit dieser Einstellung erreichen Sie ein effektives Load Balancing für die Gateways in der Zentrale.

**Default:**

- Zuletzt-verwendetem

## 2.3 Gebuehren

Dieses Menü enthält die Einstellungen für die Gebühren-Verwaltung.

**SNMP-ID:** 2.3

**Pfad Telnet:** /Setup

## 2.3.12 Budgets-Zuruecksetzen

Wenn Sie für einmalige Aktionen das Online-Budget verlängern wollen, z. B. um eine sehr große Datei aus dem Internet zu laden, müssen Sie nicht unbedingt das Zeit-Limit verändern. Sie können für solche Fälle manuell das Limit zurücksetzen.

**SNMP-ID:** 2.3.12

**Pfad Telnet:** /Setup/Gebuehren

**Default:** leer

## 2.3.1 Budget-Einheiten

Geben Sie hier ein, wie viele Gebühreneinheiten maximal im oben angegebenen Zeitraum verbraucht werden dürfen. Sobald dieses Limit erreicht wird, baut der Router keine weiteren Verbindungen mehr auf.

**SNMP-ID:** 2.3.1

**Pfad Telnet:** /Setup/Gebuehren

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 830

## 2.3.16 Aktivieren-Reserve

Bei Aktivierung des zusätzlichen Zeit-Limits wird dieses für die aktuelle Periode freigeschaltet. In der nächsten Periode gilt wieder das normale Zeit-Limit.

**SNMP-ID:** 2.3.16

**Pfad Telnet:** /Setup/Gebuehren

## 2.3.8 DSL-Breitband-Minuten-Budget

Geben Sie hier ein, wie viele Online-Minuten maximal im oben angegebenen Zeitraum verbraucht werden dürfen. Sobald dieses Limit erreicht wird, baut der Router keine weiteren Verbindungen mehr auf.

**SNMP-ID:** 2.3.8

**Pfad Telnet:** /Setup/Gebuehren

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 600

## 2.3.13 Einwahl-Minuten-Budget

Geben Sie hier ein, wie viele Online-Minuten maximal im oben angegebenen Zeitraum verbraucht werden dürfen. Sobald dieses Limit erreicht wird, baut der Router keine weiteren Verbindungen mehr auf.

**SNMP-ID:** 2.3.13

**Pfad Telnet:** /Setup/Gebuehren

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 210

## 2.3.6 Gesamt-Einheiten

Anzeige der gesamten Einheiten, die auf allen Schnittstellen bisher verbraucht wurden.

**SNMP-ID:** 2.3.6

**Pfad Telnet:** /Setup/Gebuehren

**Default:** 10

## 2.3.11 Reserve-DSL-Breitband-Budget

Geben Sie hier ein, wie viele Online-Minuten zusätzlich im oben angegebenen Zeitraum verbraucht werden dürfen, wenn die Reserve aktiviert wird.

**SNMP-ID:** 2.3.11

**Pfad Telnet:** /Setup/Gebuehren

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 300

## 2.3.3 Rest-Budget

Anzeige der Gebühreneinheiten, die im angegebenen Zeitraum noch für Router-Verbindungen zur Verfügung stehen.

**SNMP-ID:** 2.3.3

**Pfad Telnet:** /Setup/Gebuehren

## 2.3.9 Rest-DSL-Breitband-Minuten-Aktiv

Anzeige der Minuten, die im angegebenen Zeitraum noch für DSL-Breitband-Verbindungen zur Verfügung stehen.

**SNMP-ID:** 2.3.9

**Pfad Telnet:** /Setup/Gebuehren

## 2.3.14 Rest-Einwahl-Minuten

Anzeige der Minuten, die im angegebenen Zeitraum noch für Einwahl-Verbindungen zur Verfügung stehen.

**SNMP-ID:** 2.3.14

**Pfad Telnet:** /Setup/Gebuehren

## 2.3.10 Router-DSL-Breitband-Budget

Anzeige der Minuten, die im aktuellen Zeitraum schon für DSL-Breitband-Verbindungen verbraucht wurden.

**SNMP-ID:** 2.3.10

**Pfad Telnet:** /Setup/Gebuehren

## 2.3.4 Router-Einheiten

Anzeige der Minuten, die im aktuellen Zeitraum schon für Router-Verbindungen verbraucht wurden.

**SNMP-ID:** 2.3.4

**Pfad Telnet:** /Setup/Gebuehren

## 2.3.15 Router-ISDN-Seriell-Minuten-Aktiv

Anzeige der Minuten, die im aktuellen Zeitraum schon für Einwahl-Verbindungen verbraucht wurden.

**SNMP-ID:** 2.3.15

**Pfad Telnet:** /Setup/Gebuehren

## 2.3.2 Tage-pro-Periode

Geben Sie einen Zeitraum in Tagen an, der als Basis für die Kontrolle der Gebühren- und Zeit-Limits dienen soll.

**SNMP-ID:** 2.3.2

**Pfad Telnet:** /Setup/Gebuehren

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 1

## 2.3.5 Tabelle-Budget

Diese Tabelle zeigt Ihnen eine Übersicht der konfigurierten Budgets nach Budget-Einheiten sortiert für ihre Schnittstellen an.

**SNMP-ID:** 2.3.5

**Pfad Telnet:** /Setup/Gebuehren

### 2.3.5.1 lfc.

Schnittstelle, auf die sich der Eintrag bezieht.

**SNMP-ID:** 2.3.5.1

**Pfad Telnet:** /Setup/Gebuehren/Tabelle-Budget

### 2.3.5.2 Budget-Einheiten

Anzeige der Budget-Einheiten, die für diese Schnittstelle schon verbraucht wurden.

**SNMP-ID:** 2.3.5.2

**Pfad Telnet:** /Setup/Gebuehren/Tabelle-Budget

### 2.3.5.3 Rest-Budget

Anzeige der Budget-Einheiten die für diese Schnittstelle noch zur Verfügung stehen.

**SNMP-ID:** 2.3.5.3

**Pfad Telnet:** /Setup/Gebuehren/Tabelle-Budget

### 2.3.5.4 Einheiten

Anzeige der Budget-Einheiten, die bisher auf dieser Schnittstelle verbraucht wurden.

**SNMP-ID:** 2.3.5.4

**Pfad Telnet:** /Setup/Gebuehren/Tabelle-Budget

## 2.3.7 Zeit-Tabelle

Diese Tabelle zeigt Ihnen eine Übersicht der konfigurierten Budgets nach Budget-Minuten sortiert für ihre Schnittstellen an.

**SNMP-ID:** 2.3.7

**Pfad Telnet:** /Setup/Gebuehren

### 2.3.7.1 lfc.

Schnittstelle, auf die sich der Eintrag bezieht.

**SNMP-ID:** 2.3.7.1

**Pfad Telnet:** /Setup/Gebuehren/Zeit-Tabelle

### 2.3.7.2 Budget-Minuten

Anzeige der Budget-Minuten, die für diese Schnittstelle schon verbraucht wurden.

**SNMP-ID:** 2.3.7.2

**Pfad Telnet:** /Setup/Gebuehren/Zeit-Tabelle

### 2.3.7.3 Rest-Minuten

Anzeige der Budget-Minuten, die für diese Schnittstelle noch zur Verfügung stehen.

**SNMP-ID:** 2.3.7.3

**Pfad Telnet:** /Setup/Gebuehren/Zeit-Tabelle

### 2.3.7.4 Minuten-aktiv

Anzeige der Budget-Minuten, in der auf dieser Schnittstelle Datenverbindungen aktiv waren.

**SNMP-ID:** 2.3.7.4

**Pfad Telnet:** /Setup/Gebuehren/Zeit-Tabelle

### 2.3.7.5 Minuten-passiv

Anzeige der Budget-Minuten, in der diese Schnittstelle passiv verbunden war.

**SNMP-ID:** 2.3.7.5

**Pfad Telnet:** /Setup/Gebuehren/Zeit-Tabelle

## 2.4 LAN

Hier finden Sie die Einstellungen zum LAN.

**SNMP-ID:** 2.4

**Pfad Telnet:** /Setup/LAN

## 2.4.3 Heap-Reserve

Die Heap-Reserve gibt an, wie viele Blöcke des LAN-Heaps für die Kommunikation mit dem Gerät über HTTP(S)/Telnet(S)/SSH reserviert sind. Sie dient dazu, das Gerät auch im Hochlastfall (oder wenn Queueblöcke verlorengehen) noch erreichen zu können. Wenn die Anzahl der Blöcke im Heap unter den angegebenen Wert fällt, dann werden empfangene Pakete sofort verworfen (außer bei TCP-Paketen, die direkt an das Gerät gerichtet sind).

**SNMP-ID:** 2.4.3

**Pfad Telnet:** /Setup/LAN/Heap-Reserve

**Mögliche Werte**:

- maximal 3 numerische Zeichen im Bereich von 0 bis 999

**Default**: 10

## 2.4.2 MAC-Adresse

Dies ist die Hardware-Adresse des Netzwerk-Adapters in Ihrem Gerät.

**SNMP-ID:** 2.4.2

**Pfad Telnet:** /Setup/LAN/MAC-Adresse

## 2.4.9 Trace-Level

Für den LAN-Data-Trace kann die Ausgabe von Tracemeldungen auf einen bestimmten Inhalt beschränkt werden.

**SNMP-ID:** 2.4.9

**Pfad Telnet:** /Setup/LAN/Trace-Level

**Mögliche Werte**:

- Numerische Zeichen von 0 bis 255

**Default**: 255

**Besondere Werte:**

- 0: nur die Meldung, dass ein Paket überhaupt empfangen/gesendet wurde
- 1: zusätzlich die physikalischen Parameter der Pakete (Datenrate, Signalstärke, ...)
- 2: zusätzlich der MAC-Header
- 3: zusätzlich der Layer3-Header (z. B. IP/IPX)
- 4: zusätzlich der Layer4-Header (TCP, UDP, ...)
- 5: zusätzlich der TCP/UDP-Payload
- 255: die Ausgabe ist nicht beschränkt

## 2.4.8 Trace-MAC

Mit diesem Wert beschränken Sie den Ethernet-Trace auf Pakete, welche die angegebene MAC-Adresse als Ziel- oder Quelladresse haben.

**SNMP-ID:** 2.4.8

**Pfad Telnet:** /Setup/LAN/Trace-MAC

**Mögliche Werte**:

- 12 hexadezimale Zeichen

**Default**: 000000000000

**Besondere Werte:** Bei einer Einstellung von 000000000000 gibt der Ethernet-Trace alle Pakete uneingeschränkt aus.

## 2.4.10 IEEE802.1x

Dieses Menü enthält die Einstellungen für den eingebauten 802.1x-Supplicant. Das Gerät benötigt diese Einstellungen z. B. dann, wenn es an einem Ethernet-Switch mit aktivierter 802.1x-Authentifizierung angeschlossen ist.

**SNMP-ID:** 2.4.10

**Pfad Telnet:** /Setup/LAN/IEEE802.1x

## 2.4.10.1 Supplicant-Ifc-Setup

Diese Tabelle steuert die Funktion des eingebauten 802.1x-Supplicant für die verfügbaren LAN-Interfaces.

**SNMP-ID:** 2.4.10.1

**Pfad Telnet:** /Setup/LAN/IEEE802.1x/Supplicant-Ifc-Setup

### 2.4.10.1.1 Ifc

Wählen Sie hier aus, für welches LAN-Interface die 802.1x-Supplicant-Einstellungen gelten.

**SNMP-ID:** 2.4.10.1.1

**Pfad Telnet:** /Setup/LAN/IEEE802.1x/Supplicant-Ifc-Setup/Ifc

**Mögliche Werte**:

- Auswahl aus den im Gerät verfügbaren LAN-Interfaces, z. B. LAN-1 oder LAN-2.

**Default**: LAN-1

### 2.4.10.1.2 Methode

Wählen Sie hier die Methode aus, mit der sich der 802.1x-Supplicant authentisieren soll.

**SNMP-ID:** 2.4.10.1.2

**Pfad Telnet:** /Setup/LAN/IEEE802.1x/Supplicant-Ifc-Setup/Methode

**Mögliche Werte**:

- Keine
- MD5
- TLS
- TTLS/PAP
- TTLS/CHAP
- TTLS/MSCHAP
- TTLS/MSCHAPv2
- TTLS/MD5
- PEAP/MSCHAPv2
- PEAP/GTC

**Default**: Keine

**Besondere Werte:** Der Wert "Keine" deaktiviert den 802.1x Supplicant auf dem jeweiligen Interface.

### 2.4.10.1.3 Zugangsdaten

Je nach verwendeter EAP/802.1x-Methode tragen Sie hier die zur Anmeldung erforderlichen Zugangsdaten ein. Für TLS ist hier nichts einzutragen. Die Authentisierung erfolgt dann mit dem im Dateisystem hinterlegen EAP/TLS-Zertifikat). Für alle anderen Methoden tragen Sie hier Benutzernamen und Paßwort in der Schreibweise 'user:password' ein.

**SNMP-ID:** 2.4.10.1.3

**Pfad Telnet:** /Setup/LAN/IEEE802.1x/Supplicant-Ifc-Setup/Zugangsdaten

**Mögliche Zeichen**:

- Max. 64 Alphanumerische Zeichen

**Default**: Leer

# 2.5 Bridge

In diesem Menü finden sie die Einstellungen für die Bridge.

**SNMP-ID:** 2.5

**Pfad Telnet:** /Setup/Bridge

Die Einstellungen der Bridge sind nur aus Gründen der Kompatibilität zu älteren Firmware-Versionen enthalten. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

## 2.5.4 Aging-Minuten

Hier können Sie einen Zeitraum in Minuten angeben, nach dem die Bridge-Tabelle automatisch aktualisiert wird, d.h. alle nicht angesprochenen MAC-Adressen aus der Liste entfernt werden.

**SNMP-ID:** 2.5.4

**Pfad Telnet:** /Setup/Bridge/Aging-Minuten

**Mögliche Werte:**

- maximal 63 numerische Zeichen

**Default:** 30

## 2.5.1 Aktiv

Hier können Sie die Remote-Bridge aktivieren bzw. deaktivieren. Über die Remote-Bridge können Sie zwei Netzwerke so miteinander koppeln, als wären sie physikalisch miteinander verbunden. So sind Sie völlig unabhängig von den eingesetzten Netzwerkprotokollen.

**SNMP-ID:** 2.5.1

**Pfad Telnet:** /Setup/Bridge/Aktiv

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

## 2.5.2 Gegenstelle

Wählen Sie hier den Namen der Gegenstelle aus. Wenn die Gegenstelle aktiv angewählt werden soll, muss dies ein Eintrag aus der Liste der Gegenstellen sein.

**SNMP-ID:** 2.5.2

**Pfad Telnet:** /Setup/Bridge/Gegenstelle

**Mögliche Werte:**

- Eintrag aus der Liste der Gegenstellen

**Default:** leer

## 2.5.7 LAN-Interface

Wählen Sie hier die Schnittstelle aus, für die die Bridge-Einstellungen gelten.

**SNMP-ID:** 2.5.7

**Pfad Telnet:** /Setup/Bridge/LAN-Interface

**Mögliche Werte:**

- LAN-1
- LAN-2
- LAN-3
- LAN-4

**Default:** LAN-1

## 2.5.8 VLAN-ID

Tragen Sie hier die VLAN-ID des VLANs ein, auf dem die Bridge aktiv sein soll.

**SNMP-ID:** 2.5.8

**Pfad Telnet:** /Setup/Bridge/VLAN-ID

**Mögliche Werte:**

- numerische Werte im Bereich von 0 bis 4096

**Default:** 0

## 2.5.3 Bridge-Tabelle

Diese Status-Tabelle zeigt Informationen über die Bridge bekannten MAC-Adressen mit den folgenden Werten:

- MAC-Adresse eines lokalen oder entfernten Rechners
- Zeitpunkt, an dem das latzte Mal ein Paket von der MAC-Adresse empfanfgen wurde (in Millisekunden Betriebszeit)
- Flags, die angeben, woher die MAC-Adresse gelernt wurde (local/remote) und was mit einem Paket geschehen soll, das von der MAC-Adresse empfangen wird
- - LAN-Dest.-Filter: Filtern, wenn es in Richtung LAN gesendet wird
  - LAN-Src.-Filter: Filtern, wenn es vom LAN empfangen wird
  - WAN-Dest.-Filter Filtern, wenn es in Richtung WAN gesendet wird WAN-Src.-Filter: Filtern, wenn es vom LAN empfangen wird

**SNMP-ID:** 2.5.3

**Pfad Telnet:** /Setup/Bridge/Bridge-Tabelle

## 2.5.5 LAN-Einstellung

Hier finden Sie die Filteroptionen für lokale Netzwerke.

**SNMP-ID:** 2.5.5

**Pfad Telnet:** /Setup/Bridge/LAN-Einstellung

### 2.5.5.1 Broadcast

Geben Sie ein, ob Broadcast-Pakete vom LAN übertragen werden sollen oder nicht.

**SNMP-ID:** 2.5.5.1

**Pfad Telnet:** /Setup/Bridge/LAN-Einstellung/Broadcast

**Mögliche Werte:**

- nie übertragen
- immer übertragen
- nur wenn verbunden

**Default:** immer übertragen

### 2.5.5.2 Multicast

Geben Sie ein, ob Multicast-Pakete vom lokalen Netz immer, nie oder nur bei bestehender Verbindung übertragen werden sollen.

**SNMP-ID:** 2.5.5.2

**Pfad Telnet:** /Setup/Bridge/LAN-Einstellung/Multicast

**Mögliche Werte:**

- nie übertragen
- immer übertragen
- nur wenn verbunden

**Default:** immer übertragen

### 2.5.5.3 Ziel-Adresse

Hier können Sie die Einstellungen für das Filtern der eintreffenden Pakete nach Zieladressen vornehmen.

**Pfad Telnet:** /Setup/Bridge/LAN-Einstellung/Ziel-Adresse

#### 2.5.5.3.1 Filter-Typ

Geben Sie hier an, nach welchen Kriterien die Ziel-Adressen gefiltert werden.

**Pfad Telnet:** /Setup/Bridge/LAN-Einstellung/Ziel-Adresse/Filter-Typ

**Mögliche Werte:**

- positiv: nur die in der Filtertabelle enthaltenen Adressen werden gefiltert, alle anderen werden durchgelassen
- negativ: nur die in der Filtertabelle enthaltenen Adressen werden durchgelassen, alle anderen werden gefiltert

**Default:** positiv

#### 2.5.5.3.2 Filter-Tabelle

Pakete aus dem lokalen Netz an die Adressen in dieser Tabelle werden, abhängig vom Filter-Typ, gefiltert oder durchgelassen.

**Pfad Telnet:** /Setup/Bridge/LAN-Einstellung/Ziel-Adresse/Filter-Tabelle

##### 2.5.5.3.2.1 Zieladresse

Geben Sie hier die zu filternde Adresse ein.

**Pfad Telnet:** /Setup/Bridge/LAN-Einstellung/Ziel-Adresse/Filter-Tabelle/Zieladresse

**Mögliche Werte:**

- maximal 12 aphanumerische Zeichen

**Default:** leer

### 2.5.5.4 Quell-Adresse

Nehmen Sie hier die Einstellungen zum Filtern der Quelladressen vor.

**SNMP-ID:** 2.5.5.4

**Pfad Telnet:** /Setup/Bridge/LAN-Einstellung/Quell-Adresse

#### 2.5.5.4.1 Filter-Typ

Geben Sie hier an, nach welchen Kriterien die Quell-Adressen gefiltert werden.

**Pfad Telnet**:/Setup/Bridge/LAN-Einstellung/Quell-Adresse/Filter-Typ

**Mögliche Werte**:

- positiv: nur die in der Filtertabelle enthaltenen Adressen werden gefiltert, alle anderen werden durchgelassen
- negativ: nur die in der Filtertabelle enthaltenen Adressen werden durchgelassen, alle anderen werden gefiltert

**Default:** positiv

#### 2.5.5.4.2 Filter-Tabelle

Pakete aus dem lokalen Netz von diesen Adressen in dieser Tabelle werden, abhängig vom Filter-Typ, gefiltert oder durchgelassen.

**Pfad Telnet:** /Setup/Bridge/LAN-Einstellung/Quell-Adresse/Filter-Tabelle

##### 2.5.5.4.2.1 Quelladresse

Geben Sie hier die zu filternde Adresse ein.

**Pfad Telnet:** /Setup/Bridge/LAN-Einstellung/Quell-Adresse/Filter-Tabelle/Quelladresse

**Mögliche Werte:**

- maximal 12 aphanumerische Zeichen

**Default:** leer

## 2.5.6 WAN-Einstellung

Hier finden Sie die Filteroptionen für entfernte Netzwerke.

**SNMP-ID:** 2.5.6

**Pfad Telnet:** /Setup/Bridge/WAN-Einstellung

### 2.5.6.1 Broadcast

Geben Sie ein, ob Broadcast-Pakete vom WAN übertragen werden sollen oder nicht.

**SNMP-ID:** 2.5.6.1

**Pfad Telnet:** /Setup/Bridge/WAN-Einstellung/Broadcast

**Mögliche Werte:**

- nie übertragen
- immer übertragen
- nur wenn verbunden

**Default:** immer übertragen

### 2.5.6.2 Multicast

Geben Sie ein, ob Multicast-Pakete vom WAN immer, nie oder nur bei bestehender Verbindung übertragen werden sollen.

**SNMP-ID:** 2.5.6.2

**Pfad Telnet:** /Setup/Bridge/WAN-Einstellung/Multicast

**Mögliche Werte:**

- nie übertragen
- immer übertragen
- nur wenn verbunden

**Default:** immer übertragen

### 2.5.6.3 Ziel-Adresse

Hier können Sie die Einstellungen für das Filtern der eintreffenden Pakete nach Zieladressen vornehmen.

**SNMP-ID:** 2.5.6.3

**Pfad Telnet:** /Setup/Bridge/WAN-Einstellung/Ziel-Adresse

#### 2.5.6.3.1 Filter-Typ

Geben Sie hier an, nach welchen Kriterien die Ziel-Adressen gefiltert werden.

**Pfad Telnet:** /Setup/Bridge/WAN-Einstellung/Ziel-Adresse/Filter-Typ

**Mögliche Werte:**

- positiv: nur die in der Filtertabelle enthaltenen Adressen werden gefiltert, alle anderen werden durchgelassen
- negativ: nur die in der Filtertabelle enthaltenen Adressen werden durchgelassen, alle anderen werden gefiltert

**Default:** positiv

#### 2.5.6.3.2 Filter-Tabelle

Pakete aus dem WAN an die Adressen in dieser Tabelle werden, abhängig vom Filter-Typ, gefiltert oder durchgelassen.

**Pfad Telnet:** /Setup/Bridge/WAN-Einstellung/Ziel-Adresse/Filter-Tabelle

##### 2.5.6.3.2.1 Zieladresse

Geben Sie hier die zu filternde Adresse ein.

**Pfad Telnet:** /Setup/Bridge/WAN-Einstellung/Ziel-Adresse/Filter-Tabelle/Zieladresse

**Mögliche Werte:**

- maximal 12 aphanumerische Zeichen

**Default:** leer

### 2.5.6.4 Quell-Adresse

Nehmen Sie hier die Einstellungen zum Filtern der Quelladressen vor.

**SNMP-ID:** 2.5.6.4

**Pfad Telnet:** /Setup/Bridge/WAN-Einstellung/Quell-Adresse

#### 2.5.6.4.1 Filter-Typ

Geben Sie hier an, nach welchen Kriterien die Quell-Adressen gefiltert werden.

**Pfad Telnet:** /Setup/Bridge/WAN-Einstellung/Quell-Adresse/Filter-Typ

**Mögliche Werte**:

- positiv: nur die in der Filtertabelle enthaltenen Adressen werden gefiltert, alle anderen werden durchgelassen
- negativ: nur die in der Filtertabelle enthaltenen Adressen werden durchgelassen, alle anderen werden gefiltert

**Default:** positiv

#### 2.5.6.4.2 Filter-Tabelle

Pakete aus dem WAN von diesen Adressen in dieser Tabelle werden, abhängig vom Filter-Typ, gefiltert oder durchgelassen.

**Pfad Telnet:** /Setup/Bridge/WAN-Einstellung/Quell-Adresse/Filter-Tabelle

##### 2.5.6.4.2.1 Zieladresse

Geben Sie hier die zu filternde Adresse ein.

**Pfad Telnet:** /Setup/Bridge/WAN-Einstellung/Quell-Adresse/Filter-Tabelle/Zieladresse

**Mögliche Werte:**

- maximal 12 aphanumerische Zeichen

**Default:** leer

## 2.7 TCP-IP

Dieses Menü enthält die TCP/IP Einstellungen.

**SNMP-ID:** 2.7

**Pfad Telnet:** /Setup

### 2.7.1 Aktiv

Aktiviert oder deaktiviert das TCP-IP-Modul.

**SNMP-ID:** 2.7.1

**Pfad Telnet:** /Setup/TCP-IP

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

### 2.7.11 ARP-Aging-Minuten

Hier können Sie eine Zeit in Minuten angeben, nach der die ARP-Tabelle automatisch aktualisiert wird, d.h. alle seit der letzten Aktualisierung nicht mehr angesprochenen Adressen entfernt werden.

**SNMP-ID:** 2.7.11

**Pfad Telnet:** /Setup/TCP-IP

**Mögliche Werte:**

- 1 bis 60 Minuten

**Default:** 15 Minuten

## 2.7.8 DNS-Backup

Geben Sie hier einen Nameserver an, der bei Ausfall des ersten DNS verwendet werden soll.

**SNMP-ID:** 2.7.8

**Pfad Telnet:** /Setup/TCP-IP

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

## 2.7.7 DNS-Default

Geben Sie hier die Adresse eines Nameservers ein, an den DNS-Anfragen weitergeleitet werden sollen. Wenn Sie einen Internetprovider oder eine andere Gegenstelle haben, die dem Router beim Einloggen automatisch einen Nameserver zuweist, dann können Sie dieses Feld leer lassen.

**SNMP-ID:** 2.7.7

**Pfad Telnet:** /Setup/TCP-IP

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

## 2.7.22 ICMP-bei-ARP-Timeout

Wenn das LANCOM ein Paket empfängt, das es aufs LAN senden soll, dann löst es den Empfänger mittels eines ARP-requests auf. Wenn dieser nicht beantwortet wird, dann schicht das Gerät ein "ICMP host unreachable" an den Absender des Pakets zurück.

**SNMP-ID:** 2.7.22

**Pfad Telnet:** /Setup/TCP-IP

## 2.7.10 NBNS-Backup

Geben Sie hier einen Netbios-Nameserver an, der bei Ausfall des ersten NBNS verwendet werden soll.

**SNMP-ID:** 2.7.10

**Pfad Telnet:** /Setup/TCP-IP

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

## 2.7.9 NBNS-Default

Geben Sie hier die Adresse eines Netbios-Nameservers ein, an den NBNS-Anfragen weitergeleitet werden sollen. Wenn Sie einen Internetprovider oder eine andere Gegenstelle haben, die dem Router beim Einloggen automatisch einen Netbios-Nameserver zuweist, dann können Sie dieses Feld leer lassen.

**SNMP-ID:** 2.7.9

**Pfad Telnet:** /Setup/TCP-IP

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

## 2.7.20 Nichtlok.-ARP-Replies

Wenn diese Option aktiviert ist, dann beantwortet das Gerät auch ARP-Requests für seine Adresse, wenn die Absenderadresse nicht im eigenen lokalen Netz steht.

**SNMP-ID:** 2.7.20

**Pfad Telnet:** /Setup/TCP-IP

## 2.7.6 Zugangs-Liste

In der Zugangs-Liste werden alle Stationen eingetragen, die Zugang zur Konfiguration des Geräts haben sollen. Wenn die Tabelle keinen Eintrag enthält, können alle Stationen auf das Gerät zugreifen.

**SNMP-ID:** 2.7.6

**Pfad Telnet:** /Setup/TCP-IP

### 2.7.6.1 IP-Adresse

IP-Adresse der Station, die Zugriff auf die Konfiguration des Geräts haben soll.

**SNMP-ID:** 2.7.6.1

**Pfad Telnet:** /Setup/TCP-IP/Zugangs-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

### 2.7.6.2 IP-Netzmaske

IP-Netzmaske der Station, die Zugriff auf die Konfiguration des Geräts haben soll.

**SNMP-ID:** 2.7.6.2

**Pfad Telnet:** /Setup/TCP-IP/Zugangs-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

### 2.7.6.3 Rtg-Tag

Routing-Tag zur Auswahl einer bestimmten Route.

**SNMP-ID:** 2.7.6.3

**Pfad Telnet:** /Setup/TCP-IP/Zugangs-Liste

**Mögliche Werte:** max. 5 Zeichen

## 2.7.16 ARP-Tabelle

Das Address Resolution Protocol (ARP) ermittelt zu einer IP-Adresse die MAC-Adresse und speichert diese Information in der ARP-Tabelle.

**SNMP-ID:** 2.7.16

**Pfad Telnet:** /Setup/TCP-IP

### 2.7.16.1 IP-Adresse

IP-Adresse, zu der eine MAC-Adresse ermittelt wurde.

**SNMP-ID:** 2.7.16.1

**Pfad Telnet:** /Setup/TCP-IP/ARP-Tabelle

**Mögliche Werte:**

- Gültige IP-Adresse.

### 2.7.16.2 MAC-Adresse

MAC-Adresse, zu der IP-Adresse aus diesem Eintrag ermittelt wurde.

**SNMP-ID:** 2.7.16.2

**Pfad Telnet:** /Setup/TCP-IP/ARP-Tabelle

### 2.7.16.3 Letzter-Zugriff

Zeitpunkt des letzten Netzwerkzugriffs dieser Station.

**SNMP-ID:** 2.7.16.3

**Pfad Telnet:** /Setup/TCP-IP/ARP-Tabelle

### 2.7.16.5 Ethernet-Port

Physikalische Schnittstelle, über welche die Station mit dem Gerät verbunden ist.

**SNMP-ID:** 2.7.16.5

**Pfad Telnet:** /Setup/TCP-IP/ARP-Tabelle

### 2.7.16.6 Gegenstelle

Gegenstelle, über welche die Station erreicht werden kann.

**SNMP-ID:** 2.7.16.6

**Pfad Telnet:** /Setup/TCP-IP/ARP-Tabelle

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen.

### 2.7.16.7 VLAN-ID

VLAN-ID des Netzwerks, in dem sich die Station befindet

**SNMP-ID:** 2.7.16.7

**Pfad Telnet:** /Setup/TCP-IP/ARP-Tabelle

### 2.7.16.8 Anschluss

Logische Schnittstelle, mit der das gerät verbunden ist.

**SNMP-ID:** 2.7.16.8

**Pfad Telnet:** /Setup/TCP-IP/ARP-Tabelle/Anschluss

**Mögliche Werte:**

- Ein Parameter aus der Liste der logischen Schnittstellen.

## 2.7.17 Loopback-Liste

In dieser Tabelle können Sie alternative Adressen konfigurieren.

**SNMP-ID:** 2.7.17

**Pfad Telnet:** /Setup/TCP-IP

### 2.7.17.1 Loopback-Addr.

Hier können Sie optional bis zu 16 Lopback-Adressen konfigurieren. Das Gerät sieht jede dieser Adressen als eigene Adresse an und verhält sich, als hätte es das Paket auf dem LAN empfangen. Dies gilt insbesondere auf maskierten Verbindungen. Antworten auf Pakete an eine Loopback-Adresse werden nicht maskiert.

**SNMP-ID:** 2.7.17.1

**Pfad Telnet:** /Setup/TCP-IP/Loopback-Liste

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

**Default:** 0.0.0.0

### 2.7.17.2 Name

Hier können Sie einen Namen eingeben mit max. 16 Zeichen

**SNMP-ID:** 2.7.17.2

**Pfad Telnet:** /Setup/TCP-IP/Loopback-Liste

**Mögliche Werte:**

- max. 16 Zeichen

**Default:** leer

### 2.7.17.3 Rtg-tag

Geben Sie hier das Routing-Tag an, mit dem die Routen zu allen entfernten Gateways ermittelt werden, welche kein eigenes Routing-Tag konfiguriert haben (d.h. das Routing-Tag ist 0).

**SNMP-ID:** 2.7.17.3

**Pfad Telnet:** /Setup/TCP-IP/Loopback-Liste

**Mögliche Werte:**

- 0 bis max 65.535

**Default:** 0

## 2.7.21 Alive-Test

Dieses Menü enthält die Einstellungen des Alive-Tests. Der Alive-Test sendet in konfigurierbaren Abständen einen Ping an eine bestimmte Ziel-Adresse. Wenn die Zieladresse nicht erreichbar ist, führt das Gerät nach definierten Kriterien einen Neustart oder eine andere Aktion durch.

Neben der Definition der Ziel-Adresse und der auszuführenden Aktion besteht die Konfiguration des Alive-Test vor allem aus der Gestaltung der Wiederholungsserien für den Ping und dem Grenzwert für das Auslösen der definierten Aktion. Die dazu erforderlichen Parameter haben folgende Default-Werte:

- Fehler-Limit: 10
- Test-Intervall: 10
- Wiederhol-Intervall: 1
- Wiederhol-Zahl: 1

Mit diesen Einstellungen sendet das Gerät alle 10 Sekunden (Test-Intervall) einen Ping. Wird dieser Ping nicht erfolgreich beantwortet, wiederholt das Gerät den Ping nach 1 Sekunde (Wiederhol-Intervall) genau 1 Mal (Wiederhol-Zahl). Bleibt auch die Antwort auf diesen Ping aus, betrachtet das Gerät die Serie als fehlgeschlagen. Wenn 10 Serien in Folge (Fehler-Limit) fehlschlagen, löst das Gerät die definierte Aktion aus, in diesem Fall also nach 10 x 10 Sekunden = 100 Sekunden.

**SNMP-ID:** 2.7.21

**Pfad Telnet:** /Setup/TCP-IP

### 2.7.21.7 Aktion

Tragen Sie hier die Aktion ein, die das Gerät ausführt, wenn die Ziel-Adresse nicht erreichbar ist. Sie können alle Aktionen eintragen, die auch in der Cron-Tabelle gültig sind, d.h. neben CLI-Kommandos können Sie auch HTTP-Zugriffe ausführen oder Mails verschicken.

Die hier eingestellte Aktion wird nur ausgeführt, wenn der Boot-Typ auf den Wert **Aktion** eingestellt ist. Den Boot-Typ konfigurieren Sie unter `/Setup/TCP-IP/Alive-Test/Boot-Typ` (siehe auch *Boot-Typ*).

**SNMP-ID:** 2.7.21.7

**Pfad Telnet:** /Setup/TCP-IP/Alive-Test

**Mögliche Werte:**

- 251 Zeichen

**Default:** leer

### 2.7.21.6 Boot-Typ

Diese Aktion führt das Gerät aus, wenn der Ping an die Ziel-Gegenstelle nicht erfolgreich war.

**SNMP-ID:** 2.7.21.6

**Pfad Telnet:** /Setup/TCP-IP/Alive-Test

**Mögliche Werte:**

- Kaltstart: Das Gerät führt einen Kaltstart durch.
- Warmstart: Das Gerät führt einen Warmstart durch.
- Aktion: Das Gerät führt eine konfigurierbare Aktion aus. Konfigurieren Sie die gewünschte Aktion unter `/Setup/TCP-IP/Alive-Test` (siehe auch *Aktion*).

**Default:** Warmstart

### 2.7.21.5 Fehler-Limit

Dieser Parameter definiert die Anzahl der aufeinander folgenden fehlerhaften Test-Serien, bevor das Gerät neu startet bzw. bevor die konfigurierte Aktion ausgeführt wird.

Das Produkt aus Fehler-Limit und Test-Intervall definiert die gesamte Dauer, die bis zum Neustart bzw. zur Ausführung der Aktion vergeht.

**SNMP-ID:** 2.7.21.5

**Pfad Telnet:** /Setup/TCP-IP/Alive-Test

**Mögliche Werte:**

- 0 bis 4294967295

**Default:** 10

### 2.7.21.2 Test-Intervall

Das zeitliche Intervall in Sekunden, in welchem das Gerät einen Ping an die Ziel-Adresse sendet. Wenn der Ping nicht beantwortet wird, sendet das Gerät optional in definierten Abständen eine gewünschte Anzahl von Wiederholungen. Mit dieser Konfiguration bildet das Gerät "Serien" von Ping-Versuchen. Nur wenn alle diese Pings nicht beantwortet werden, wird die komplette Serie als nicht erfolgreich gewertet.

Das Produkt aus Fehler-Limit und Test-Intervall definiert die gesamte Dauer, die bis zum Neustart bzw. zur Ausführung der Aktion vergeht.

**SNMP-ID:** 2.7.21.2

**Pfad Telnet:** /Setup/TCP-IP/Alive-Test

**Mögliche Werte:**

- 0 bis 4294967295 Sekunden

  Wählen Sie das Test-Intervall größer als das Produkt aus Wiederhol-Intervall und Wiederhol-Zahl, damit die gewünschten Wiederholungen innerhalb des Test-Intervalls ausgeführt werden können.

**Default:** 10

### 2.7.21.4 Wiederhol-Intervall

Dieser Wert gibt an, in welchem zeitlichen Intervall das Gerät einen nicht beantworteter Ping an die Ziel-Adresse wiederholt.

**SNMP-ID:** 2.7.21.4

**Pfad Telnet:** /Setup/TCP-IP/Alive-Test

**Mögliche Werte:**

- 0 bis 4294967295

Wählen Sie das Wiederhol-Intervall so, dass das Produkt aus Wiederhol-Intervall und Wiederhol-Zahl kleiner als das gewählte Test-Intervall ist, damit die gewünschten Wiederholungen innerhalb des Test-Intervalls ausgeführt werden können.

**Default:** 1

**Besondere Werte:** Bei einem Wiederhol-Intervall von 0 sendet das Gerät keine erneuten Versuche.

### 2.7.21.3 Wiederhol-Zahl

Dieser Wert gibt an, wie oft das Gerät einen nicht beantworteten Ping an die Ziel-Adresse wiederholt.

**SNMP-ID:** 2.7.21.3

**Pfad Telnet:** /Setup/TCP-IP/Alive-Test

**Mögliche Werte:**

- 0 bis 4294967295

Wählen Sie die Wiederhol-Zahl so, dass das Produkt aus Wiederhol-Intervall und Wiederhol-Zahl kleiner als das gewählte Test-Intervall ist, damit die gewünschten Wiederholungen innerhalb des Test-Intervalls ausgeführt werden können.

**Default:** 1

**Besondere Werte:** Bei einer Wiederhol-Zahl von 0 sendet das Gerät keine erneuten Versuche.

### 2.7.21.1 Ziel-Adresse

Die Ziel-Adresse, an welche das Gerät einen Ping sendet.

**SNMP-ID:** 2.7.21.1

**Pfad Telnet:** /Setup/TCP-IP/Alive-Test

**Mögliche Werte:**

- Gültige IP-Adresse.

## 2.7.30 Netzliste

In dieser Tabelle können Sie die IP-Netzwerke definieren. Diese werden von anderen Modulen (DHCP-Server, RIP, NetBIOS etc.) über den Netzwerknamen referenziert.

**SNMP-ID:** 2.7.30

**Pfad Telnet:** /Setup/TCP-IP

### 2.7.30.1 Netzwerkname

Tragen Sie hier einen eindeutigen Namen ein mit max. 16 Zeichen, über den das Netzwerk von anderen Modulen (DHCP-Server, RIP, NetBIOS etc.) referenziert werden kann.

**SNMP-ID:** 2.7.30.1

**Pfad Telnet:** /Setup/TCP-IP/Netzliste

**Mögliche Werte:**

- max. 16 Zeichen

**Default:** leer

### 2.7.30.2 IP-Adresse

Wenn Sie in Ihrem lokalen Netz einen privaten Adress-Bereich verwenden, dann tragen Sie hier eine freie Adresse aus diesem Bereich ein. Bei Verwendung von IP-Masquerading sind diese Adressen für entfernte Netze nicht sichtbar, sondern werden durch die für die jeweiligen Gegenstelle gültige Internet IP-Adresse ersetzt.

**SNMP-ID:** 2.7.30.2

**Pfad Telnet:** /Setup/TCP-IP/Netzliste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.7.30.3 IP-Netzmaske

Wenn Sie unter Intranet IP-Adresse eine Adresse aus einem privaten Adress-Bereich eingegeben haben, dann geben Sie hier die zugehörige Netzmaske ein.

**SNMP-ID:** 2.7.30.3

**Pfad Telnet:** /Setup/TCP-IP/Netzliste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 255.255.255.0

### 2.7.30.4 VLAN-ID

An einer physikalischen Schnittstelle können auch mehrere voneinander getrennte VLANs (die "davor" von einem Switch separiert wurden) gebunden werden. Dazu muss dem Router in jedem dieser VLANs eine eigene Adresse bzw. ein eigenes Netz gegeben werden. Hierzu kann jedem Netzwerk neben den Schnittstellen auch ein VLAN zugewiesen werden, für das es gelten soll. Wenn nun auf einer Schnittstelle ein Paket mit dieser VLAN-ID empfangen wird, so wird dieses Paket dem jeweiligen Netzwerk zugeordnet, d.h. das Netzwerk kann nur von Paketen erreicht werden, die dem selben VLAN entstammen. Pakete die dem Netzwerk selbst entstammen, werden beim Versand mit dieser VLAN-ID markiert. Eine "0" steht für ein ungetaggtes netz (kein VLAN). Achtung: Es ist sehr gefährlich diese ID zu verändern. Man kann sich hier sehr leicht vom Zugriff auf das Gerät aussperren, wenn man keinen Zugang zum zugewiesenen VLAN hat. Beachten Sie außerdem, dass sich diese Einstellung auf den gesamten von diesem Netzwerk verwalteten Verkehr auswirkt. Dies schließt alle Pakete ein, welche durch dieses Netzwerk geleitet werden.

**SNMP-ID:** 2.7.30.4

**Pfad Telnet:** /Setup/TCP-IP/Netzliste

**Mögliche Werte:**

- max 4.094

**Default:** 0

### 2.7.30.5 Interface

Wählen Sie hier die Schnittstelle aus, die dem Netzwerk zugeordnet sein soll. Wird hier "beliebig" gewählt, so gilt dieses Netzwerk auf allen Schnittstellen, an die nicht anderweitig ein Netzwerk gebunden ist.

**SNMP-ID:** 2.7.30.5

**Pfad Telnet:** /Setup/TCP-IP/Netzliste

**Mögliche Werte:**

- Beliebig
- LAN-1
- LAN-2
- LAN-3
- LAN-4
- WLAN-1
- WLAN-1-2
- WLAN-1-3
- WLAN-1-4
- WLAN-1-5
- WLAN-1-6
- WLAN-1-7
- WLAN-1-8
- P2P-1-1
- P2P-1-2
- P2P-1-3
- P2P-1-4
- P2P-1-5
- P2P-1-6
- BRG-1
- BRG-2
- BRG-3
- BRG-4
- BRG-5
- BRG-6
- BRG-7
- BRG-8

**Default:** beliebig

### 2.7.30.6 Quellpruefung

Der Schalter beeinflusst die Adressprüfung der Firewall. "Flexibel" ewartet keine Rückroute, d.h. jede Quelladresse wird akzeptiert, wenn das Gerät selbst angesprochen wurde. Das Gerät kann dadurch wie bisher direkt erreicht werden. "Streng" erwartet dagegen eine explizite Rückroute, damit kein IDS-Alarm ausgelöst wird.

**SNMP-ID:** 2.7.30.6

**Pfad Telnet:** /Setup/TCP-IP/Netzliste

**Mögliche Werte:**

- flexibel
- streng

**Default:** flexibel

### 2.7.30.7 Typ

Wählen Sie hier den Typ des Netzwerkes aus (Intranet oder DMZ) oder deaktivieren Sie es.

**SNMP-ID:** 2.7.30.7

**Pfad Telnet:** /Setup/TCP-IP/Netzliste

**Mögliche Werte:**

- Deaktiviert
- Intranet
- DMZ

**Default:** Intranet

### 2.7.30.8 Rtg-Tag

Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, die auf diesem Netzwerk empfangen werden, werden intern mit diesem Tag markiert. Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen auch ohne explizite Firewall-Regel. Zudem hat dieses Tag Einfluss auf die über IP propagierten Routen und auf die vom NetBIOS-Proxy sichtbaren Hosts und Gruppen.

**SNMP-ID:** 2.7.30.8

**Pfad Telnet:** /Setup/TCP-IP/Netzliste

**Mögliche Werte:**

- max. 65.535

**Default:** 0

### 2.7.30.9 Kommentar

Hier können Sie einen Kommentar eintragen.

**SNMP-ID:** 2.7.30.9

**Pfad Telnet:** /Setup/TCP-IP/Netzliste

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** leer

## 2.8 IP-Router

Dieses Menü enthält die Einstellungen des IP-Routers.

**SNMP-ID:** 2.8

**Pfad Telnet:** /Setup

## 2.8.1 Aktiv

Schaltet den IP-Router ein oder aus.

**SNMP-ID:** 2.8.1

**Pfad Telnet:** /Setup/IP-Router

**Mögliche Werte:**

- aktiv
- inaktiv

**Default:** inaktiv

## 2.8.12 Ende-WAN-Pool

Geben Sie hier einen Bereich von IP-Adressen ein, der Benutzern zugewiesen werden soll, die sich auf dem Gerät einwählen.

Das Gerät verwendet automatisch für jeden Benutzer eine freie Adresse aus diesem Bereich. Sobald ein Benutzer die Verbindung zum Gerät wieder trennt, wird die ihm zugewiesene Adresse wieder frei und steht anderen Benutzern zur Verfügung.

**SNMP-ID:** 2.8.12

**Pfad Telnet:** /Setup/IP-Router

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

## 2.8.6 ICMP-Redirect-Senden

Hier können Sie wählen, ob ICMP-Redirects gesendet werden sollen.

**SNMP-ID:** 2.8.6

**Pfad Telnet:** /Setup/IP-Router

**Mögliche Werte:**

- aktiv
- inaktiv

**Default:** Aktiv

## 2.8.14 Nutzung-Default-Listen

Aktivieren Sie hier die zeitabhängige Steuerung der Default-Route. Über die Default-Route wird üblicherweise die Verbindung zu einem Internet-Anbieter herestellt. Mit der Zeitsteuerung können Sie zeitabhängig verschiedene Internet-Anbieter auswählen, z. B. um den zu der jeweiligen Uhrzeit preisgünstigsten Anbieter zu verwenden.

**SNMP-ID:** 2.8.14

**Pfad Telnet:** /Setup/IP-Router

**Mögliche Werte:**

- aktiv
- inaktiv

**Default:** inaktiv

Um diesen Mechanismus zu nutzen, müssen Sie in der Routing-Tabelle eine Default-Route angegeben haben. Der in der Default-Route angegebene Router wird nur in den Zeiten verwendet, welche nicht von der Zeitsteuerungs-Tabelle abgedeckt werden.

## 2.8.5 Proxy-ARP

Hier können Sie den Proxy-ARP-Mechanismus aktivieren bzw. deaktivieren. Mit Proxy-ARP können Sie entfernte Rechner in Ihr lokales Netz einbinden, so als ständen Sie direkt in Ihrem lokalen Netz.

**SNMP-ID:** 2.8.5

**Pfad Telnet:** /Setup/IP-Router

**Mögliche Werte:**

- aktiv
- inaktiv

**Default:** inaktiv

## 2.8.11 Start-WAN-Pool

Geben Sie hier einen Bereich von IP-Adressen ein, der Benutzern zugewiesen werden soll, die sich auf dem Gerät einwählen.

Das Gerät verwendet automatisch für jeden Benutzer eine freie Adresse aus diesem Bereich. Sobald ein Benutzer die Verbindung zum Gerät wieder trennt, wird die ihm zugewiesene Adresse wieder frei und steht anderen Benutzern zur Verfügung.

**SNMP-ID:** 2.8.11

**Pfad Telnet:** /Setup/IP-Router

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

## 2.8.22 WAN-Tag-Erzeugung

Mit der WAN-Tag-Erzeugung wird die Quelle für die Zuordnung von Schnittstellen-Tags definiert. Neben der Zuordnung über die Firewall oder direkte Zuordnung über die Tag-Tabelle kann das Schnittstellen-Tag auch anhand der effektiven Routing-Tabelle gewählt werden (statische Routing-Einträge plus Routen, die über RIP gelernt wurden). Aus dieser Routing-Tabelle wird das Tag derjenigen Route gewählt, die sowohl auf die Gegenstelle als auch auf das zugehörige Netzwerk passt. Enthält die effektive Routing-Tabelle mehrere Einträge für eine Gegenstelle mit gleichem Netzwerk, so wird das kleinste Tag verwendet.

**SNMP-ID:** 2.8.22

**Pfad Telnet:** /Setup/IP-Router

**Mögliche Werte:**

- Manual: In dieser Einstellung werden die Schnittstellen-Tags ausschließlich über einen Eintrag in der Tag-Tabelle bestimmt. Die Routing-Tabelle hat keine Bedeutung für die Zuordnung der Schnittstellen-Tags.
- Auto: In dieser Einstellung werden die Schnittstellen-Tags zunächst über einen Eintrag in der Tag-Tabelle bestimmt. Wird dort kein passender Eintrag gefunden, so wird das Tag anhand der Routing-Tabelle ermittelt .

**Default:** Manual

Sowohl die über die Tag-Tabelle, als auch die anhand der Routing-Tabelle ermittelten Schnittstellen-Tags können durch einen passenden Eintrag in der Firewall überschrieben werden.

## 2.8.2 IP-Routing-Tabelle

In dieser Tabelle geben Sie ein, über welche Gegenstellen bestimmte Netzwerke oder Stationen erreicht werden können.

**SNMP-ID:** 2.8.2

**Pfad Telnet:** /Setup/IP-Router

### 2.8.2.1 IP-Adresse

Geben Sie hier die Zieladresse für diese Route ein. Dies kann eine einzelne Station sein, die Sie in Ihr Netz einbinden möchten oder ein ganzes Netzwerk, welches Sie mit Ihrem eigenen koppeln wollen.

**SNMP-ID:** 2.8.2.1

**Pfad Telnet:** /Setup/IP-Router/IP-Routing-Tabelle

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.8.2.2 IP-Netzmaske

Geben Sie hier die zu der eingetragenen IP-Adresse gehörige Netzmaske ein. Wenn Sie nur eine einzelne Station adressieren wollen, geben Sie als Netzmaske 255.255.255.255 ein.

**SNMP-ID:** 2.8.2.2

**Pfad Telnet:** /Setup/IP-Router/IP-Routing-Tabelle

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.8.2.3 Peer-oder-IP

Wählen Sie hier den Router, an den die Pakete für diese Route weitergeleitet werden sollen.

Wählen Sie dazu den Namen einer Gegenstelle aus der Liste der Gegenstellen aus.

Wenn diese Route zu einer anderen Station im lokalen Netz führen soll, geben Sie einfach die IP-Adresse dieser Station ein.

**SNMP-ID:** 2.8.2.3

**Pfad Telnet:** /Setup/IP-Router/IP-Routing-Tabelle

### 2.8.2.4 Distanz

Geben Sie hier die Anzahl der Hops zu diesem Router an. Normalerweise brauchen Sie diesen Wert nicht zu setzen, er wird automatisch vom Router kontrolliert.

**SNMP-ID:** 2.8.2.4

**Pfad Telnet:** /Setup/IP-Router/IP-Routing-Tabelle

**Mögliche Werte:**

- 0 bis 16

**Default:** 0

### 2.8.2.5 Maskierung

Mit der IP-Maskierung können Sie ein logisches Netzwerk hinter einer einzelnen Adresse (der des Routers) verbergen. Wenn Sie beispielsweise einen Internet-Zugang haben, können Sie so Ihr komplettes Netzwerk an das Internet anbinden. Bei fast allen Internet-Providern ist es üblich, dass die Gegenstelle Ihrem Gerät bei der Einwahl eine dynamische IP-Adresse zuteilt. Sollte Ihnen Ihr Internet-Provider feste IP-Adressen zugeteilt haben, so können Sie diese in der IP-Parameter-Liste

der jeweiligen Verbindung zuweisen. Wählen Sie "Intranet und DMZ maskieren" aus, wenn Sie die IP-Maskierung für alle LAN-Interfaces aktivieren wollen. Wenn Sie feste IP-Adressen für die Rechner in der demilitarisierten Zone (DMZ) zuweisen und dennoch die IP-Maskierung für die Rechner an den übrigen LAN-Interfaces (Intranet) aktivieren wollen, so wählen Sie "Nur Intranet maskieren" aus.

**SNMP-ID:** 2.8.2.5

**Pfad Telnet:** /Setup/IP-Router/IP-Routing-Tabelle

**Mögliche Werte:**

- IP-Maskierung abgeschaltet
- Intranet und DMZ maskieren (Standard)
- Nur Intranet maskieren

**Default:** IP-Maskierung abgeschaltet

### 2.8.2.6 Aktiv

Bestimmen Sie hier den Schaltzustand. Die Route kann aktiviert werden und entweder immer via RIP propagiert oder nur dann via RIP propagiert werden, wenn das Zielnetzwerk erreichbar ist.

**SNMP-ID:** 2.8.2.6

**Pfad Telnet:** /Setup/IP-Router/IP-Routing-Tabelle

**Mögliche Werte:**

- Die Route ist aktiviert und wird immer via RIP propagiert (sticky).
- Die Route ist aktiviert und wird via RIP propagiert, wenn das Zielnetzwerk erreichbar ist (konditional).
- Die Route ist aus.

**Default:** Die Route ist aktiviert und wird immer via RIP propagiert (sticky)

### 2.8.2.7 Kommentar

Dieses Feld steht für einen Kommentar zur Verfügung.

**SNMP-ID:** 2.8.2.7

**Pfad Telnet:** /Setup/IP-Router/IP-Routing-Tabelle

**Mögliche Werte:**

- max. 64 Zeichen

### 2.8.2.8 Rtg-Tag

Wenn Sie ein Routing-Tag für diese Route angeben, so wird die Route nur für solche Pakete verwendet, die entweder in der Firewall mit dem gleichen Tag markiert oder über ein Netzwerk mit passendem Schnittstellen-Tag empfangen wurden.

**SNMP-ID:** 2.8.2.8

**Pfad Telnet:** /Setup/IP-Router/IP-Routing-Tabelle

**Mögliche Werte:**

- max. 65535

**Default:** 0

Die Verwendung von Routing-Tags macht folglich nur in Kombination mit entsprechenden, dekorierenden Regeln in der Firewall oder getaggten Netzwerken Sinn.

## 2.8.7 Routing-Methode

Dieses Menü enthält die Konfiguration der Routing-Methode für ihren IP-Router.

**SNMP-ID:** 2.8.7

**Pfad Telnet:** /Setup/IP-Router

### 2.8.7.2 ICMP-Routing-Methode

Geben Sie an, ob der Router ICMP-Pakete gesichert übertragen soll.

**SNMP-ID:** 2.8.7.2

**Pfad Telnet:** /Setup/IP-Router

**Mögliche Werte:**

- Normal
- gesichert

**Default:** Normal

### 2.8.7.6 Interne-Dienste-routen

Wählen Sie hier aus, ob die internen Dienste über den Router geleitet werden sollen.

**SNMP-ID:** 2.8.7.6

**Pfad Telnet:** /Setup/IP-Router/Routing-Methode

**Mögliche Werte:**

- Ja: Die Pakete für die internen Dienste werden über den Router geleitet.
- Nein: Die Pakete werden direkt an den Absender zurückgeschickt.

**Default:** Nein

Behandeln Sie die internen Services VPN und PPTP speziell, denn das Routing aller Pakete ohne Ausnahme führt zu einem Performance-Verlust. Das Gerät leitet nur die ersten Pakete weiter, die von diesen Services während der Verbindungsherstellung zum Router geschickt werden, wenn Sie diese Option aktivieren. Weitere Pakete werden an den nächsten Port weitergleitet.

### 2.8.7.4 L2-L3-Tagging

Geben Sie an, was mit den DiffServ-Tags aus Layer-2 passieren soll.

**SNMP-ID:** 2.8.7.4

**Pfad Telnet:** /Setup/IP-Router/Routing-Methode

**Mögliche Werte:**

- Ignorieren
- nach Layer-3 kopieren
- automatisch kopieren

**Default:** ignorieren

### 2.8.7.5 L3-L2-Tagging

Geben Sie an, ob die DiffServ-Tags aus Layer-3 nach Layer-2 kopiert werden sollen .

**SNMP-ID:** 2.8.7.5

**Pfad Telnet:** /Setup/IP-Router

**Mögliche Werte:**

- aktiv
- inaktiv

**Default:** inaktiv

### 2.8.7.1 Routing-Methode

Auswertung der ToS- oder DiffServ-Felder.

**SNMP-ID:** 2.8.7.1

**Pfad Telnet:** /Setup/IP-Router

**Mögliche Werte:**

- Normal: Das ToS/DiffServ-Feld wird ignoriert.
- TOS: Das ToS/DiffServ-Feld wird als ToS-Feld betrachtet, es werden die Bits "Low-Delay" und "High-Reliability"
- ausgewertet.
- DiffServ: Das ToS/DiffServ-Feld wird als DiffServ-Feld betrachtet und wie folgt ausgewertet:
- CSx (inklusive CS0 = BE): normal übertragen
- AFxx: gesichert übertragen
- EF: bevorzugt übertragen

### 2.8.7.3 SYN/ACK-Speedup

Geben Sie an, ob TCP SYN- und ACK-Pakete bevorzugt weitergeleitet werden sollen.

**SNMP-ID:** 2.8.7.3

**Pfad Telnet:** /Setup/IP-Router/Routing-Methode

**Mögliche Werte:**

- aktiv
- inaktiv

**Default:** Aktiv

## 2.8.8 RIP

Dieses Menü enthält die Konfiguration des RIP für ihren IP-Router.

**SNMP-ID:** 2.8.8

**Pfad Telnet:** /Setup/IP-Router

### 2.8.8.2 R1-Maske

Diese Einstellung ist nur nötig, wenn Sie als RIP-Unterstützung RIP-1 ausgewählt haben. Sie beeinflusst die Bildung von Netzwerkmasken für über RIP gelernte Routen.

**SNMP-ID:** 2.8.8.2

**Pfad Telnet:** /Setup/IP-Router/RIP

**Mögliche Werte:**

- Klasse
- Adresse
- Klasse + Adresse

**Default:** Klasse

### 2.8.8.4 WAN-Tabelle

Konfigurieren Sie hier für jede Gegenstelle getrennt die WAN-seitige RIP-Unterstützung

**SNMP-ID:** 2.8.8.4

**Pfad Telnet:** /Setup/IP-Router/RIP

#### 2.8.8.4.1 Gegenstelle

Name der Gegenstelle, von der WAN-RIP-Pakete gelernt werden sollen.

**SNMP-ID:** 2.8.8.4.1

**Pfad Telnet:** /Setup/IP-Router/RIP/WAN-Tabelle

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen

**Default:** Leer

**Besondere Werte:** Mit dem * als Platzhalter können in einem Eintrag mehrere Gegenstellen konfiguriert werden. Sollen z. B. mehrere Gegenstellen per WAN-RIP ihre Netze bekannt geben, während für alle anderen User und Filialen eine statische Netzvergabe existiert, können alle entsprechenden Gegenstellen einen Namen mit dem Prefix "RIP_" bekommen. In der WAN-RIP-Tabelle wird dann nur noch ein Eintrag mit der Gegenstelle "RIP_*" aufgenommen, um alle Gegenstellen zu konfigurieren.

#### 2.8.8.4.10 Rx-Filter

Geben Sie hier den Filter an, der beim Empfang von RIP-Paketen verwendet werden soll.

**SNMP-ID:** 2.8.8.4.10

**Pfad Telnet:** /Setup/IP-Router/RIP/WAN-Tabelle

**Mögliche Werte:**

- Auswahl aus der Liste der definierten RIP-Filter (max. 16 Zeichen).

**Default:** Leer

#### 2.8.8.4.11 Tx-Filter

Geben Sie hier den Filter an, der beim Versand von RIP-Paketen verwendet werden soll.

**SNMP-ID:** 2.8.8.4.11

**Pfad Telnet:** /Setup/IP-Router/RIP/WAN-Tabelle

**Mögliche Werte:**

- Auswahl aus der Liste der definierten RIP-Filter (max. 16 Zeichen).

**Default:** Leer

#### 2.8.8.4.12 RIP-senden

Stellen Sie ein, ob RIP auf dem WAN Routen propagiert. Dazu muss gleichzeitig der RIP-Typ gesetzt sein.

**SNMP-ID:** 2.8.8.4.12

**Pfad Telnet:** /Setup/IP-Router/RIP/WAN-Tabelle/RIP-senden

**Mögliche Werte**:

- Nein
- Ja

**Default**: Nein/Aus

#### 2.8.8.4.2 RIP-Typ

Der RIP-Typ gibt an, mit welcher RIP-Version die lokalen Routen propagiert werden.

**SNMP-ID:** 2.8.8.4.2

**Pfad Telnet:** /Setup/IP-Router/RIP/WAN-Tabelle

**Mögliche Werte:**

- Aus
- RIP-1
- RIP-1 kompatibel
- RIP 2

**Default:** Aus

#### 2.8.8.4.3 RIP-lernen

In der Spalte RIP-Accept wird angegeben, ob RIP aus dem WAN akzeptiert wird. Dazu muss gleichzeitig der RIP-Typ gesetzt sein.

**SNMP-ID:** 2.8.8.4.3

**Pfad Telnet:** /Setup/IP-Router/RIP/WAN-Tabelle

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

#### 2.8.8.4.4 Maskierung

In der Spalte Masquerade wird angegeben ob und wie auf der Strecke maskiert wird. Durch diesen Eintrag ist es möglich, das WAN-RIP auch mit einer leeren Routing-Tabelle zu starten.

**SNMP-ID:** 2.8.8.4.4

**Pfad Telnet:** /Setup/IP-Router/RIP/WAN-Tabelle

**Mögliche Werte:**

- Auto: Der Maskierungstyp wird aus der Routing-Tabelle entnommen. Existiert für die Gegenstelle kein Routing-Eintrag, so wird nicht maskiert.
- An: Alle Verbindungen werden maskiert.
- Intranet: Verbindungen aus dem Intranet werden maskiert, Verbindungen aus der DMZ gehen transparent hindurch.

**Default:** Ein

#### 2.8.8.4.5 Dft-Rtg-Tag

In der Spalte Dft-Rtg-Tag steht das für die WAN-Verbindung geltende „Default-Routing-Tag". Alle ungetaggten Routen werden beim Versenden im WAN mit diesem Tag getaggt.

**SNMP-ID:** 2.8.8.4.5

**Pfad Telnet:** /Setup/IP-Router/RIP/WAN-Tabelle

**Mögliche Werte:**

- max. 65.535

**Default:** 0

#### 2.8.8.4.6 Rtg-Tag-Liste

In der Spalte Rtg-Tag-List steht eine kommaseparierte Liste der Tags, die auf dem Interface akzeptiert werden. Wenn diese Liste leer ist, dann werden alle Tags akzeptiert. Steht mindestens ein Tag in der Liste, dann werden nur die Tags in dieser Liste akzeptiert. Ebenso werden beim Senden von getaggten Routen auf das WAN nur Routen mit erlaubten Tags propagiert.

Alle vom WAN gelernten Routen werden intern als ungetaggte Routen behandelt und auf das LAN mit dem Default-Tag (0) propagiert. Auf das WAN hingegen werden sie mit dem Tag propagiert, mit dem sie auch gelernt wurden.

**SNMP-ID:** 2.8.8.4.6

**Pfad Telnet:** /Setup/IP-Router/RIP/WAN-Tabelle

**Mögliche Werte:**

- Komma-separierte Liste mit max. 33 Zeichen

**Default:** leer

#### 2.8.8.4.7 Poisoned-Reverse

Poisoned Reverse dient dazu, Routing-Schleifen zu verhindern. Dazu wird an den Router, der die beste Route zu einem Netz propagiert hat, dieses Netz auf dem zugehörigen Interface als unerreichbar zurückpropagiert.

Gerade auf WAN-Strecken hat dies aber einen entscheidenden Nachteil: Hier werden von der Zentrale sehr viele Routen gesendet, die dann als nicht erreichbar zurückpropagiert werden und so gegebenenfalls die verfügbare Bandbreite belasten. Daher kann die Verwendung von Poisoned Reverse auf jedem Interface (LAN/WAN) manuell aktiviert werden.

**SNMP-ID:** 2.8.8.4.7

**Pfad Telnet:** /Setup/IP-Router/RIP/WAN-Tabelle

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

#### 2.8.8.4.8 RFC2091

Anders als im LAN sind auf WAN-Strecken regelmäßige Updates alle 30 Sekunden ggf. unerwünscht, weil die Bandbreite beschränkt ist. Daher können nach RFC 2091 alle Routen im WAN nur noch einmal beim Verbindungsaufbau übertragen werden, danach nur noch Updates (triggered Updates).

Da in diesem Fall die Updates explizit angefragt werden, können keine Broadcasts oder Multicasts für die Zustellung der RIP-Nachrichten verwendet werden. Stattdessen muss im Filialgerät die IP-Adresse des nächsten erreichbaren Routers in der Zentrale statisch konfiguriert werden. Der Zentralrouter kann sich aufgrund der Anfragen merken, von welchen Filialroutern er Update-Requests empfangen hat, um etwaige Routenänderungen über passende Messages direkt an das Filialgerät zu senden.

**SNMP-ID:** 2.8.8.4.8

**Pfad Telnet:** /Setup/IP-Router/RIP/WAN-Tabelle

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

In einem Zentral-Gateway kann die Einstellung "RFC 2091" immer aus und der Eintrag "Gateway" immer auf 0.0.0.0 stehen, da das Zentral-Gateway immer die Vorgabe des Filial-Gateway berücksichtigt.

#### 2.8.8.4.9 Gateway

IP-Adresse des nächsten erreichbaren Routers im Zusammenhang mit RFC 2091.

**SNMP-ID:** 2.8.8.4.9

**Pfad Telnet:** /Setup/IP-Router/RIP/WAN-Tabelle

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

**Besondere Werte:** Bei Eingabe von 0.0.0.0 wird die Gateway-Adresse aus der PPP-Verhandlung bestimmt.

In einem Router in der Zentrale kann die RFC 2091 ausgeschaltet werden und die Gateway-Adresse auf 0.0.0.0 bleiben, da sich die Zentrale immer an die Anfragen der Filialen hält.

Das LANCOM fällt automatisch auf Standard-RIP zurück, wenn das angegebene Gateway RFC 2091 nicht unterstützt.

In einem Zentral-Gateway kann die Einstellung "RFC 2091" immer aus und der Eintrag "Gateway" immer auf 0.0.0.0 stehen, da das Zentral-Gateway immer die Vorgabe des Filial-Gateway berücksichtigt.

### 2.8.8.5 LAN-Tabelle

In dieser Tabelle können Sie RIP Einstellungen vornehmen und auswählen für welches Netzwerk diese gelten sollen.

**SNMP-ID:** 2.8.8.5

**Pfad Telnet:** /Setup/IP-Router/RIP

#### 2.8.8.5.1 Netzwerkname

Wählen Sie hier den Netzwerknamen des Netzes aus, für das die Einstellungen gelten sollen.

**SNMP-ID:** 2.8.8.5.1

**Pfad Telnet:** /Setup/IP-Router/RIP/LAN-Tabelle

**Mögliche Werte:**

- Intranet
- DMZ

**Default:** leer

#### 2.8.8.5.10 Rx-Filter

Geben Sie hier den beim Empfang (RX) von RIP-Paketen anzuwendende Filter an.

**Pfad Telnet:** /Setup/IP-Router/RIP/LAN-Tabelle/Rx-Filter

**Mögliche Werte**:

- Max. 16 Alphanumerische Zeichen

**Default**: Leer

Definieren Sie die Filter zuerst in der RIP-Filterliste, um sie hier verwenden zu können.

#### 2.8.8.5.11 Tx-Filter

Geben Sie hier den beim Senden (TX) von RIP-Paketen anzuwendende Filter an.

**Pfad Telnet:** /Setup/IP-Router/RIP/LAN-Tabelle/Tx-Filter

**Mögliche Werte**:

- Max. 16 Alphanumerische Zeichen

**Default**: Leer

Definieren Sie die Filter zuerst in der RIP-Filterliste, um sie hier verwenden zu können.

#### 2.8.8.5.12 RIP-senden

Wählen Sie hier, ob Routen auf diesem Netzwerk propagiert werden sollen. Dazu muss gleichzeitig der RIP-Typ gesetzt sein

**Pfad Telnet:** /Setup/IP-Router/RIP/LAN-Tabelle/RIP-senden

**Mögliche Werte**:

- Nein
- Ja

**Default**: Nein

#### 2.8.8.5.2 RIP-Typ

Wählen Sie aus, ob der Router IP-RIP unterstützen soll. Mit IP-RIP können automatisch Routing-Informationen zwischen einzelnen Stationen ausgetauscht werden.

**SNMP-ID:** 2.8.8.5.2

**Pfad Telnet:** /Setup/IP-Router/RIP/LAN-Tabelle

**Mögliche Werte:**

- Aus
- RIP-1
- RIP-1 kompatibel
- RIP-2

**Default:** Aus

#### 2.8.8.5.3 RIP-lernen

Wählen Sie hier, ob Routen von diesem Netzwerk gelernt werden sollen oder nicht.

**SNMP-ID:** 2.8.8.5.3

**Pfad Telnet:** /Setup/IP-Router/RIP/LAN-Tabelle

**Mögliche Werte:**

- aktiv
- inaktiv

**Default:** inaktiv

#### 2.8.8.5.4 Propagieren

Wählen Sie hier, ob das zugehörige Netzwerk auf anderen Netzwerken propagiert wird.

**SNMP-ID:** 2.8.8.5.4

**Pfad Telnet:** /Setup/IP-Router/RIP/LAN-Tabelle

**Mögliche Werte:**

- aktiv
- inaktiv

**Default:** inaktiv

#### 2.8.8.5.5 Dft-Rtg-Tag

Tragen Sie hier einen Wert für das Standard-Routing-Tag ein, der für die gewählte Schnittstelle gilt. Routen die das Tag der Schnittstelle gesetzt haben, werden auf dieser Schnittstelle mit dem Standard-Routing-Tag propagiert. Von der Schnittstelle gelernte Routen, die das hier konfigurierte Standard-Routing-Tag gesetzt haben, werden mit dem Schnittstellen-Tag in die RIP-Tabelle aufgenommen. Desweiteren werden unmarkierte Routen (also Routen mit dem Tag 0) auf dieser Schnittstelle nicht propagiert, es sei denn, die Schnittstelle besitzt selbst das Tag 0.

**SNMP-ID:** 2.8.8.5.5

**Pfad Telnet:** /Setup/IP-Router/RIP/LAN-Tabelle

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

#### 2.8.8.5.6 Rtg-Tag-Liste

Hier steht eine Komma-separierte Liste der Routing-Tags, die auf dieser Schnittstelle akzeptiert werden. Wenn diese Liste leer ist, dann werden alle Routen ungeachtet ihrer Routing-Tags akzeptiert. Steht mindestens ein Tag in dieser Liste, dann werden nur Routen mit den Tags in dieser Liste akzeptiert. Ebenso werden beim Senden von markierten Routen nur Routen mit erlaubten (d.h. hier aufgezählte) Tags weitergeleitet. Die Routing-Tag-Liste entspricht insoweit der WAN-RIP-Liste, mit dem Unterschied, dass etwaige Umsetzungen über das Standard-Routing-Tag berücksichtigt werden. D.h. wenn z. B. das Schnittstellen-Tag 1 und das Standard-Routing-Tag 0 ist, muss das Tag 0 in der Routing-Tag-Liste erscheinen, da es beim Empfang intern in das Tag 1 umgewandelt wird. Beim Senden wird entspechend das interne Tag 1 in das externe Tag 0 umgewandelt. Diese Maßnahme ist nötig, damit ein virtualisierter Router mit weiteren Routern im LAN, die keine getaggten Routen unterstützen, zusammenarbeiten kann.

**SNMP-ID:** 2.8.8.5.6

**Pfad Telnet:** /Setup/IP-Router/RIP/LAN-Tabelle

**Mögliche Werte:**

- max. 33 Zeichen

**Default:** leer

#### 2.8.8.5.7 Poisoned-Reverse

Poisoned Reverse dient dazu, Routing-Schleifen zu verhindern. Dazu wird an den Router, der die beste Route zu einem Netz propagiert hat, dieses Netz auf dem zugehörigen Interface als unerreichbar zurückpropagiert.

Gerade auf WAN-Strecken hat dies aber einen entscheidenden Nachteil: Hier werden von der Zentrale sehr viele Routen gesendet, die dann als nicht erreichbar zurückpropagiert werden und so gegebenenfalls die verfügbare Bandbreite belasten. Daher kann die Verwendung von Poisoned Reverse auf jedem Interface (LAN/WAN) manuell aktiviert werden.

**SNMP-ID:** 2.8.8.5.7

**Pfad Telnet:** /Setup/IP-Router/RIP/LAN-Tabelle

**Mögliche Werte:**

- aktiv
- inaktiv

**Default:** inaktiv

## 2.8.8.6 Einstellungen

Das Routing Information Protocol (RIP) versendet regelmäßige Update-Nachrichten an die benachbarten Router mit Informationen über die erreichbaren Netzwerke und die zugehörigen Metriken (Hops). RIP verwendet verschiedene Timer, um den Austausch der Routing-Informationen zeitlich zu steuern.

**SNMP-ID:** 2.8.8.6

**Pfad Telnet:** /Setup/IP-Router/RIP

### 2.8.8.6.4 Flush

Erhält ein Router während des Flush-Intervalls keine Update-Information über eine Route, wird diese Route endgültig aus der dynamischen Routingtabelle gelöscht.

**SNMP-ID:** 2.8.8.6.4

**Pfad Telnet:** /Setup/IP-Router/RIP/Einstellungen

**Mögliche Werte:**

- 0 bis 99 in Vielfachen des Update-Intervalls

**Default:** 10

### 2.8.8.6.2 Holddown

Das Holddown-Intervall gibt an, nach wie vielen Update-Intervallen eine von einem Router A gelernte Route durch eine schlechtere eines anderen Routers B ersetzt werden darf, wenn Router A diese Route nicht mehr propagiert.

Bis zum Ablauf der Holddown-Intervalls nimmt das LANCOM eine Route nur an, wenn sie von dem gleichen Router propagiert wurden, von dem sie ursprünglich gelernt wurde. Von anderen Routern nimmt das LANCOM innarhalb dieser Zeit eine Route nur dann an, wenn sie besser als die bisher bekannt Route ist.

**SNMP-ID:** 2.8.8.6.2

**Pfad Telnet:** /Setup/IP-Router/RIP/Einstellungen

**Mögliche Werte:**

- 0 bis 99 in Vielfachen des Update-Intervalls

**Default:** 4

### 2.8.8.6.3 Invalidate

Das Invalidate-Intervall gibt an nach wie vielen Update-Intervallen eine Route als nicht erreichbar (invalid) markiert wird, wenn der Router, von dem sie ursprünglich gelernt wurde, diese nicht mehr propagiert.

Lernt das LANCOM in dieser Zeit eine gleich gute oder bessere Route von einem anderen Router, so wird diese übernommen

**SNMP-ID:** 2.8.8.6.3

**Pfad Telnet:** /Setup/IP-Router/RIP/Einstellungen

**Mögliche Werte:**

- 0 bis 99 in Vielfachen des Update-Intervalls

**Default:** 6

#### 2.8.8.6.6 Max-Hopcount

In manchen Szenarien ist es erwünscht, einen größeren maximalen Hopcount als den von RIP vorgesehenen Wert von 16 zu verwenden. Mit dem Parameter Max-Hopcount kann der Wert angepasst werden.

**SNMP-ID:** 2.8.8.6.6

**Pfad Telnet:** /Setup/IP-Router/RIP/Einstellungen

**Mögliche Werte:**

- 16 bis 99

**Default:** 16

#### 2.8.8.6.7 Routes-pro-Frame

Anzahl der Routen, die in einem Paket gemeinsam propagiert werden dürfen.

**SNMP-ID:** 2.8.8.6.7

**Pfad Telnet:** /Setup/IP-Router/RIP/Einstellungen

**Mögliche Werte:**

- 1 bis 90

**Default:** 25

#### 2.8.8.6.1 Update

Zeit zwischen zwei regelmäßigen Updates. Zu diesem Wert wird immer noch ein Zufallswert von +/- 5 Sekunden addiert.

**SNMP-ID:** 2.8.8.6.1

**Pfad Telnet:** /Setup/IP-Router/RIP/Einstellungen

**Mögliche Werte:**

- 0 bis 99 Sekunden

**Default:** 30 Sekunden

#### 2.8.8.6.5 Upd-Delay

Bei einem Triggered Update werden Änderungen in den Metriken sofort an die benachbarten Router gemeldet, nicht erst beim nächsten regelmäßigen Update. Damit es bei Fehlkonfigurationen im Netzwerk nicht zu massenhaften Update-Nachrichten kommt, wird eine so genannte Update-Verzögerung (Update-Delay) definiert.

Die Update-Verzögerung startet, sobald die Routing-Tabelle bzw. Teile davon propagiert wurden. Solange dieses Verzögerung läuft, werden neue Routing-Informationen zwar angenommen und in die Tabelle eingetragen, aber nicht sofort weitergeleitet. Der Router meldet die aktuellen Einträge erst nach Ablauf der Verzögerung aktiv weiter.

Der hier konfigurierte Wert gibt die Obergrenze der Verzögerung an – die tatsächliche Verzögerung wird immer zufällig ermittelt und liegt zwischen einer Sekunde und dem hier angegebenen Wert.

**SNMP-ID:** 2.8.8.6.5

**Pfad Telnet:** /Setup/IP-Router/RIP/Einstellungen

**Mögliche Werte:**

- 0 bis 99 Sekunden

**Default:** 5

### 2.8.8.7 Filter

Über RIP gelernte Routen können durch die Einstellungen bei LAN- und WAN-RIP nach dem Routing-Tag gefiltert werden. Um die Routen zusätzlich über die Angabe von Netzadressen zu filtern (z. B. „Lerne nur Routen, die im Netz 192.168.0.0/255.255.0.0 liegen“), werden in einer zentralen Tabelle zunächst die Filter definiert, die dann von Einträgen in der LAN- und WAN-RIP-Tabelle genutzt werden können.

Die in der Filtertabelle definierten Filter können in der LAN-RIP- und WAN-RIP-Tabelle in den Spalten RX- und TX-Filter referenziert werden. Dabei werden mit RX die Filter angesprochen, die das Lernen der Routen von diesen Netzwerken erlauben oder sperren – mit TX werden die Netzwerke definiert, zu denen das Propagieren der Routen erlaubt oder gesperrt werden soll.

**SNMP-ID:** 2.8.8.7

**Pfad Telnet:** /Setup/IP-Router/RIP

#### 2.8.8.7.1 Name

Name des Filtereintrags.

**SNMP-ID:** 2.8.8.7.1

**Pfad Telnet:** /Setup/IP-Router/RIP/Filter

**Mögliche Werte:**

- 18 Zeichen

Mit dem Rautezeichen # können mehrere Einträge zu einem einzigen Filter verbunden werden. Die Einträge LAN#1 und LAN#2 bilden zusammen also einen Filter „LAN“, der in der RIP-Tabelle aufgerufen werden kann.

#### 2.8.8.7.2 Filter

Kommaseparierte Liste von Netzwerken, die akzeptiert (+) oder abgelehnt (-) werden sollen.

**SNMP-ID:** 2.8.8.7.2

**Pfad Telnet:** /Setup/IP-Router/RIP/Filter

**Mögliche Werte:**

- 64 Zeichen aus ‚+-/0123456789.

Die Angabe des Pluszeichens für akzeptierte Netzwerke ist optional.

Die Filterung über Routing-Tags bleibt davon unberührt, d. h., wenn eine Route schon aufgrund ihres Tags nicht gelernt bzw. propagiert werden darf, dann kann das nicht über die Filtertabellen erzwungen werden.

### 2.8.8.8 Beste-Routen

In größeren Netzen kann ein Zielnetz auch über mehrere Gateways erreichbar sein. Wenn alle diese Gateways ihre Routen über RIP propagieren, dann lernt das Gerät mehrere Routen zum gleichen Ziel. Die bevorzugten Routen werden in der Tabelle "Beste Routen" abgelegt. Die Einträge der Tabelle beinhalten folgende Einträge:

- IP-Adresse
- IP-Netzmaske
- Rtg-Tag
- Gateway
- Distanz
- Zeit

- Gegenstelle
- Port
- VLAN-ID
- Netzwerkname

**Pfad Telnet:** /Setup/IP-Router/RIP/Einstellungen/Beste-Routen

### 2.8.8.9 Alle-Routen

In größeren Netzen kann ein Zielnetz auch über mehrere Gateways erreichbar sein. Wenn alle diese Gateways ihre Routen über RIP propagieren, dann lernt das Gerät mehrere Routen zum gleichen Ziel. Diese Routen werden in der Tabelle "Alle Routen" abgelegt. Die Einträge der Tabelle beinhalten folgende Einträge:

- IP-Adresse
- IP-Netzmaske
- Rtg-Tag
- Gateway
- Distanz
- Zeit
- Gegenstelle
- Port
- VLAN-ID
- Netzwerkname

**Pfad Telnet:** /Setup/IP-Router/RIP/Einstellungen/Alle-Routen

## 2.8.9 1-N-NAT

Dieses Menü enthält die Konfiguration des 1-N-NAT für ihren IP-Router.

**SNMP-ID:** 2.8.9

**Pfad Telnet:** /Setup/IP-Router

### 2.8.9.7 Fragment-Aging-Sekunden

Wenn ein IP-Paket nicht vollständig demaskiert werden kann, weil nicht alle Fragmente empfangen wurden, dann werden die unvollständigen Fragmente nach der hier eingestellten Zeit in Sekunden verworfen.

**SNMP-ID:** 2.8.9.7

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT

**Mögliche Werte:**

- 1 bis 255

**Default:** 5

### 2.8.9.6 Fragmente

Diese Einstellung kontrolliert das Verhalten der Firewall bei fragmentierten IP-Paketen.

**SNMP-ID:** 2.8.9.6

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT

**Mögliche Werte:**

- Filtern: Die Fragmente werden immer verworfen (gefiltert).

- Routen: Die Fragmente werden demaskiert. Dazu müssen die Fragmente allerdings in der ursprünglichen Reihenfolge empfangen werden. Ausserdem werden in dieser Einstellung nur die einzelnen Fragmente von der Firewall überprüft, nicht aber das gesamte IP-Paket.
- Reassemblieren: Die einzelnen Fragmente werden so lange zwischengespeichert, bis das IP-Paket komplett reassembliert ist. Die Fragmente können dabei in beliebiger Reihenfolge empfangen werden. Ausserdem überprüft die Firewall den Inhalt des reassemblierten IP-Pakets.

**Default:** Reassemblieren

### 2.8.9.3 ICMP-Aging-Sekunden

Geben Sie hier an, nach welcher Zeit der Inaktivität einer ICMP-Verbindung der entsprechende Eintrag in der Masquerading-Tabelle entfernt werden soll.

**SNMP-ID:** 2.8.9.3

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT

**Mögliche Werte:**

- 0 bis 65.535

**Default:** 10 Sek.

### 2.8.9.10 ID-Spoofing

Bei der Verwendung von NAT werden in den abgehenden Paketen die Paket-IDs ersetzt (ID-Spoofing), um einerseits auch fragmentierte Pakete übertragen zu können und andererseits ein Ausspähen des internen Netzes über die Paket-IDs zu verhindern. Bei der Nutzung von AH ist dieser Vorgang unerwünscht, da die Pakete-ID von AH genutzt wird. Für die korrekte Funktion von AH kann das ID-Spoofing hier deaktiviert werden.

**SNMP-ID:** 2.8.9.10

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

### 2.8.9.8 IPSec-Aging-Sekunden

Geben Sie hier an, nach welcher Zeit der Inaktivität einer IPSec-Verbindung der entsprechende Eintrag in der Masquerading-Tabelle entfernt werden soll.

**SNMP-ID:** 2.8.9.8

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT

**Mögliche Werte:**

- 0 bis 65.535

**Default:** 2000

### 2.8.9.1 TCP-Aging-Sekunden

Geben Sie hier an, nach welcher Zeit der Inaktivität einer TCP-Verbindung der entsprechende Eintrag in der Masquerading-Tabelle entfernt werden soll.

**SNMP-ID:** 2.8.9.1

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT

**Mögliche Werte:**

- 0 bis 65.535

**Default:** 300 Sek.

### 2.8.9.2 UDP-Aging-Sekunden

Geben Sie hier an, nach welcher Zeit der Inaktivität einer UDP-Verbindung der entsprechende Eintrag in der Masquerading-Tabelle entfernt werden soll.

**SNMP-ID:** 2.8.9.2

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT

**Mögliche Werte:**

- 0 bis 65.535

**Default:** 20 Sek.

### 2.8.9.4 Service-Tabelle

Wenn Sie einzelne Dienste auf bestimmten Stationen auch ausserhalb Ihres Netzes verfügbar machen wollen (z. B. einen WebServer), dann tragen Sie die Stationen und die Dienste in diese Tabelle ein.

**SNMP-ID:** 2.8.9.4

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT

#### 2.8.9.4.1 D-Port-von

Geben Sie hier den Port des gewünschten Services an.

**SNMP-ID:** 2.8.9.4.1

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/Service-Tabelle

**Mögliche Werte:**

- max. 65.535

**Default:** 0

#### 2.8.9.4.2 Intranet-Adresse

Geben Sie hier die Adresse des Rechners im Intranet an, der den Service zur Verfügung stellt.

**SNMP-ID:** 2.8.9.4.2

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/Service-Tabelle

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

#### 2.8.9.4.3 D-Port-bis

Geben Sie hier den Port des gewünschten Services an.

**SNMP-ID:** 2.8.9.4.3

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/Service-Tabelle

**Mögliche Werte:**

- max. 65.535

**Default:** 0

#### 2.8.9.4.4 Map-Port

Port mit dem das Paket weitergeleitet wird.

**SNMP-ID:** 2.8.9.4.4

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/Service-Tabelle

**Mögliche Werte:**

- max. 65.535

**Default:** 0

#### 2.8.9.4.5 Aktiv

Sie können diesen Eintrag vorübergehend inaktiv schalten, ohne ihn löschen zu müssen.

**SNMP-ID:** 2.8.9.4.5

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/Service-Tabelle

**Mögliche Werte:**

- aktiv
- inaktiv

**Default:** Aktiv

#### 2.8.9.4.6 Kommentar

Dieses Feld steht für einen Kommentar zur Verfügung.

**SNMP-ID:** 2.8.9.4.6

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/Service-Tabelle

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** /

#### 2.8.9.4.7 Gegenstelle

Wählen Sie hier die Gegenstelle, für die dieser Eintrag gültig ist.

**SNMP-ID:** 2.8.9.4.7

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/Service-Tabelle

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen.

#### 2.8.9.4.8 Protokoll

Stellen Sie hier ein für welches Protokoll der Datensatz gelten soll.

**SNMP-ID:** 2.8.9.4.8

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/Service-Tabelle

**Mögliche Werte:**

- TCP
- UDP
- TCP + UDP

**Default:** TCP + UDP

#### 2.8.9.4.9 WAN-Adresse

Stellen Sie hier ein, für welche WAN-Adresse der Datensatz gelten soll. Hat man mehr als eine statische IP-Adresse, kann man durch Angabe dieser Adresse ein gezieltes Portforwarding für diese Adresse erzielen. Bei Angabe der Adresse 0.0.0.0 wird weiterhin die der Verbindung zugewiesene Adresse verwendet.

**SNMP-ID:** 2.8.9.4.9

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/Service-Tabelle

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.8.9.5 Tabelle-1-N-NAT

Die 1-N-NAT-Tabelle zeigt die maskierten Verbindungen.

**SNMP-ID:** 2.8.9.5

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT

#### 2.8.9.5.1 Intranet-Adresse

Zeigt die interne IP-Adresse der Station, zu der eine maskierte Verbindung gespeichert wurde.

**SNMP-ID:** 2.8.9.5.1

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/Tabelle-1-N-NAT

**Mögliche Werte:**

- Gültige IP-Adresse.

#### 2.8.9.5.2 S-Port

Quell-Port der maskierten Verbindung.

**SNMP-ID:** 2.8.9.5.2

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/Tabelle-1-N-NAT

#### 2.8.9.5.3 Protokoll

Protokoll (UDP/TCP), das auf der maskierten Verbindung verwendet wird.

**SNMP-ID:** 2.8.9.5.3

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/Tabelle-1-N-NAT

#### 2.8.9.5.4 Timeout

Gültigkeitsdauer der maskierten Verbindung in Sekunden (Einstellbar unter TCP-Aging, UDP-Aging oder ICMP-Aging).

**SNMP-ID:** 2.8.9.5.4

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/Tabelle-1-N-NAT

#### 2.8.9.5.5 Handler

Handler, der zur Maskierung benötigt wird, z. B. FTP

**SNMP-ID:** 2.8.9.5.5

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/Tabelle-1-N-NAT

#### 2.8.9.5.6 Remote-Adresse

Entfernte IP-Adresse, zu der die maskierte Verbindung aufgebaut wurde.

**SNMP-ID:** 2.8.9.5.6

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/Tabelle-1-N-NAT

**Mögliche Werte:**

- Gültige IP-Adresse.

### 2.8.9.9 IPSec-Table

Die IPSec-Tabelle zeigt die maskierten IPSec-Verbindungen an inkl. einiger Parameter der Verbindung.

**SNMP-ID:** 2.8.9.9

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT

#### 2.8.9.9.1 Remote-Adresse

Adresse des entfernten VPN-Gateways

**SNMP-ID:** 2.8.9.9.1

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/IPSec-Table

**Mögliche Werte:**

- Gültige IP-Adresse.

#### 2.8.9.9.10 Flags

Flags, die den Zustand der Verbindung beschreiben:

0x01 Verbindung ist invers maskiert

0x02 Verbindung wartet auf SPI

0x04 andere Verbindungen warten auf SPI

0x08 Aggressive-Mode Verbindung

0x10 NAT-Traversal-Verbindung

0x20 Session-Recovery

**SNMP-ID:** 2.8.9.9.10

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/IPSec-Table

#### 2.8.9.9.11 CO

Connect-Timeout - läuft direkt nachdem der Eintrag angelegt wurde. Wenn innerhalb von 30 Sekunden keine SA ausgehandelt wurde (d.h.es wurde kein ESP Paket gesendet oder empfangen) wird der Eintrag wieder gelöscht

**SNMP-ID:** 2.8.9.9.11

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/IPSec-Table

#### 2.8.9.9.12 NL

Lokaler Notification Timeout: wenn vom lokalen VON-Gateway eine IKE Notification empfangen wurde wird dieser Timer gestartet. Wird innerhalb von 30 Sekunden kein IKE oder ESP-Paket von der remoten Seite empfangen, so wird der Eintrag gelöscht

**SNMP-ID:** 2.8.9.9.12

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/IPSec-Table

#### 2.8.9.9.13 NR

Remoter Notification Timeout: entspricht dem lokalen Notification Timeout, nur dass hier die Notification vom remoten VPN-Gateway empfangen wurde.

**SNMP-ID:** 2.8.9.9.13

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/IPSec-Table

#### 2.8.9.9.14 DP

DPD-Timeout: wenn von einer Seite ein DPD-Paket empfangen wurde, wird dieser Timer gestartet. Wenn innerhalb von 30 Sekunden kein DPD-Paket von der anderen Seite empfangen wird, dann wird der Eintrag entfernt.

**SNMP-ID:** 2.8.9.9.14

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/IPSec-Table

#### 2.8.9.9.2 Lokale-Adresse

Adresse des lokalen VPN-Gateways (i.A. ist das ein VPN-Client im lokalen Netz)

**SNMP-ID:** 2.8.9.9.2

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/IPSec-Table

**Mögliche Werte:**

- Gültige IP-Adresse.

#### 2.8.9.9.3 rc-hi

Höchstwertige 32 Bit des IKE Cookies des entfernten VPN-Gateways

**SNMP-ID:** 2.8.9.9.3

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/IPSec-Table

#### 2.8.9.9.4 rc-lo

Niederwertige 32 Bit des IKE Cookies des entfernten VPN-Gateways.

**SNMP-ID:** 2.8.9.9.4

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/IPSec-Table

#### 2.8.9.9.5 lc-hi

Höchstwertige 32 Bit des IKE Cookies des lokalen VPN-Gateways.

**SNMP-ID:** 2.8.9.9.5

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/IPSec-Table

#### 2.8.9.9.6 lc-lo

Niederwertige 32 Bit des IKE Cookies des lokalen VPN-Gateways.

**SNMP-ID:** 2.8.9.9.6

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/IPSec-Table

#### 2.8.9.9.7 remoter-SPI

Vom entfernten VPN Gateway verwendeter SPI.

**SNMP-ID:** 2.8.9.9.7

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/IPSec-Table

#### 2.8.9.9.8 lokaler-SPI

Vom lokalen VPN Gateway verwendeter SPI.

**SNMP-ID:** 2.8.9.9.8

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/IPSec-Table

#### 2.8.9.9.9 Timeout

Timeout in Sekunden bis der Eintrag gelöscht wird. Der Wert ist unter IPSec-Aging-Seconds einstellbar und der Default beträgt 2000 Sekunden.

**SNMP-ID:** 2.8.9.9.9

**Pfad Telnet:** /Setup/IP-Router/1-N-NAT/IPSec-Table

## 2.8.10 Firewall

Dieses Menü enthält die Konfiguration der Firewall.

**SNMP-ID:** 2.8.10

**Pfad Telnet:** /Setup/IP-Router

### 2.8.10.10 Admin-Email

Wenn sie über definierte Ereignisse (DoS. IDS oder das Überschreiten von Limitierungen) benachrichtigt werden wollen, müssen Sie hier eine gültige E-Mail-Adresse angeben.

**SNMP-ID:** 2.8.10.10

**Pfad Telnet:** /Setup/IP-Router/Firewall

**Mögliche Werte:**

- max. 255 Zeichen

Für E-Mail-Benachrichtigung müssen Sie außerdem die notwendigen Einstellungen in der Hauptgruppe 'Meldungen' in der Untersektion 'SMTP' vornehmen.

### 2.8.10.11 Aktiv

Hier können Sie die gesamte Firewall an- oder abschalten. Die Firewall überprüft und zählt alle ein- und ausgehenden Pakete. Sie öffnet in Abhängigkeit vom jeweiligen Protokoll vorübergehend nur jene Kanäle, die von einer lokalen Station zur Abwicklung einer Anfrage erforderlich sind. Außerdem können bestimmte Netze oder Stationen, Dienste oder Protokolle bevorzugt, limitiert oder verboten werden.

**SNMP-ID:** 2.8.10.11

**Pfad Telnet:** /Setup/IP-Router/Firewall

**Mögliche Werte:**

- aktiv
- inaktiv

**Default:** Aktiv

Bei abgeschalteter Firewall werden definierte VPN-Regeln weiterhin beachtet.

### 2.8.10.16 Auth-Port

Werden TCP- oder UDP-Ports versteckt, so entsteht auf maskierten Verbindungen das Problem, dass die sogenannten "Authenticate"- bzw. "Idenf-Anfragen", welche von einigen Mail- oder News-Servern dazu benutzt werden etwaige zusätzliche Informationen vom User anzufordern, nicht mehr korrekt abgelehnt werden. Diese Server laufen dann in einen Timeout, was dazu führt, dass die Mailzustellung erheblich verzögert wird. Um dieses Problem bei eingeschaltetem Stealth-Modus zu umgehen, wird für den betroffenen Port vorübergehend der Stealth-Modus aufgehoben. Die Firewall erkennt die Absicht einer internen Station zu einem Mail- (SMTP, POP3, IMAP2) oder News-Server (NNTP) Kontakt aufzunehmen und öffnet den Port für 20 Sekunden. Sie können hier die kurzfristige Aufhebung des Stealth-Modus für den Authentifizierungs-Port unterdrücken.

**SNMP-ID:** 2.8.10.16

**Pfad Telnet:** /Setup/IP-Router/Firewall

**Mögliche Werte:**

- aktiv
- inaktiv

**Default:** inaktiv

### 2.8.10.9 DoS-Aktion

Hier bestimmen Sie, wie mit den Paketen verfahren werden soll, welche den Trigger ausgelöst oder überschritten haben. Sie können die Pakete übertragen, unkommentiert verwerfen oder mittels ICMP-Reject (der Absender wird informiert) zurückweisen.

**SNMP-ID:** 2.8.10.9

**Pfad Telnet:** /Setup/IP-Router/Firewall

**Mögliche Werte:**

- Übertragen
- Verwerfen
- Zurückweisen

**Default:** Verwerfen

### 2.8.10.13 IDS-Aktion

Hier bestimmen Sie, wie mit den Paketen verfahren werden soll, welche den Trigger ausgelöst oder überschritten haben. Sie können die Pakete übertragen, unkommentiert verwerfen oder mittels ICMP-Reject (der Absender wird informiert) zurückweisen.

**SNMP-ID:** 2.8.10.13

**Pfad Telnet:** /Setup/IP-Router/Firewall

**Mögliche Werte:**

- Übertragen
- Verwerfen
- Zurückweisen

**Default:** Verwerfen

### 2.8.10.8 Max.-Halb-Offene-Verb.

Denial-Of-Service Angriffe nutzen prinzipielle Schwächen der TCP/IP-Protokolle sowie fehlerhafte Implementationen aus. Zu den Angriffen, die prinzipielle Schwächen ausnutzen, gehören z. B. SYN-Flood und Smurf. Zu den Angriffen, die fehlerhafte Implementationen zum Ziel haben, gehören alle Angriffe, die mit fehlerhaft fragmentierten Paketen operieren (z. B. Teardrop) oder mit gefälschten Absenderadressen arbeiten (z. B. Land). Ihr Gerät erkennt die meisten dieser Angriffe und kann mit einer hier konfigurierbaren gezielten Gegenmaßnahme reagieren.

**SNMP-ID:** 2.8.10.8

**Pfad Telnet:** /Setup/IP-Router/Firewall

**Mögliche Werte:**

- 100 bis 9999

**Default:** 100

### 2.8.10.14 Ping-Block

Eine umstrittene Methode, die Sicherheit zu erhöhen, ist das Verstecken des Routers. indem Ping- und Traceroute-Anfragen nicht mehr beantwortet werden (Ping-Blocking). Dies ist insofern umstritten, als auch ein Nichtantworten auf die Existenz eines Gerätes schließen lässt. Ist nämlich wirklich kein Gerät vorhanden, so beantwortet der jeweils vorherige Router die entsprechenden Pakete mit "nicht zustellbar", da er sie wirklich nicht zustellen kann. Antwortet hingegen der jeweils vorherige Router nicht mit einer entsprechenden Ablehnung, so war das Paket für ihn zustellbar und unabhängig vom darauf folgenden Verhalten des Empfängers ist dieser auf jeden Fall vorhanden. Das Verhalten des jeweils vorherigen Routers kann nicht simuliert werden, ohne Ihr Gerät wirklich offline (und damit auch für selbst angeforderte Dienste unerreichbar) zu halten oder abzuschalten.

**SNMP-ID:** 2.8.10.14

**Pfad Telnet:** /Setup/IP-Router/Firewall

**Mögliche Werte:**

- Aus
- Immer
- Nur WAN
- Nur für Default-Route

**Default:** Aus

### 2.8.10.12 Port-Scan-Schwelle

Intrusion-Detection-System (IDS). Ihr Gerät erkennt die meisten unberechtigten Eindringversuche und kann mit einer hier konfigurierbaren gezielten Gegenmaßnahme reagieren.

**SNMP-ID:** 2.8.10.12

**Pfad Telnet:** /Setup/IP-Router/Firewall

**Mögliche Werte:**

- 50 bis 9999

**Default:** 50

### 2.8.10.17 Sitzungswiederherst.-Verb.

Die Firewall öffnet für jede begonnene Sitzung und deren Verbindungen (z. B. FTP mit Kontroll- und Datenverbindung) für eine bestimmte Zeit für jede Verbindung einen entsprechenden Kanal. Findet über einen definierten Zeitraum hinaus (Einstellung in IP-Router-Maskierung) auf den Verbindungen keine Kommunikation statt, so wird die Sitzung als beendet betrachtet und die den Verbindungen zugehörigen Kanäle geschlossen. Die Auswahl 'Sitzungs-Wiederherstellung' bestimmt das Verhalten der Firewall beim Empfang von Paketen, die auf eine ehemalige Sitzung schließen lassen. Die Pakete werden entweder verworfen oder es wird davon ausgegangen, dass eine Sitzung bestand, auf dieser aber zu lange keine Kommunikation stattfand. Dann kann eine gleichwertige Sitzung wiederhergestellt werden. Letzteres Verhalten kann generell erlaubt oder verboten werden. Ein Verbot kann auf die Default-Route oder auf WAN-Sitzungen eingeschränkt werden.

**SNMP-ID:** 2.8.10.17

**Pfad Telnet:** /Setup/IP-Router/Firewall

**Mögliche Werte:**

- Immer erlaubt
- Immer verboten
- Nicht über WAN
- Nicht über Default-Route

**Default:** Nicht über Default-Route

### 2.8.10.15 Stealth-Mode

Eine umstrittene Methode, die Sicherheit zu erhöhen, ist das Verstecken des Routers. indem TCP- und UDP-Anfragen nicht mehr normgerecht abgelehnt, sondern ignoriert werden (Stealth-Modus). Dies ist insofern umstritten, als auch ein Nichtantworten auf die Existenz eines Gerätes schließen lässt. Ist nämlich wirklich kein Gerät vorhanden, so beantwortet der jeweils vorherige Router die entsprechenden Pakete mit "nicht zustellbar", da er sie wirklich nicht zustellen kann. Antwortet hingegen der jeweils vorherige Router nicht mit einer entsprechenden Ablehnung, so war das Paket für ihn zustellbar und unabhängig vom darauf folgenden Verhalten des Empfängers ist dieser auf jeden Fall vorhanden. Das Verhalten des jeweils vorherigen Routers kann nicht simuliert werden, ohne Ihr Gerät wirklich offline (und damit auch für selbst angeforderte Dienste unerreichbar) zu halten oder abzuschalten.

**SNMP-ID:** 2.8.10.15

**Pfad Telnet:** /Setup/IP-Router/Firewall

**Mögliche Werte:**

- Aus
- Immer
- Nur WAN
- Nur für Default-Route

**Default:** Aus

### 2.8.10.1 Objekt-Tabelle

In der Objekttabelle werden diejenigen Elemente bzw. Objekte definiert, die in der Regeltabelle der Firewall verwendet werden sollen. Objekte können sein:

- einzelne Rechner (MAC- oder IP-Adresse, Host-Name)
- ganze Netze
- Protokolle
- Dienste (Ports oder Port-Bereiche, z. B. HTTP, Mail&News, FTP, ...)

Diese Elemente lassen sich beliebig kombinieren und hierarchisch strukturieren. So können z. B. zunächst Objekte für die Protokolle TCP und UDP definiert werden. Später kann man darauf aufbauend Objekte z. B. für FTP (= TCP + Ports 20 und 21), HTTP (= TCP + Port 80) und DNS (= TCP, UDP + Port 53) anlegen. Diese können dann wiederum zu einem Objekt zusammengefasst werden, das alle Definitionen der Einzelobjekte enthält.

**SNMP-ID:** 2.8.10.1

**Pfad Telnet:** /Setup/IP-Router/Firewall

#### 2.8.10.1.1 Name

Geben Sie hier einen eindeutigen Namen für dieses Objekt an.

**SNMP-ID:** 2.8.10.1.1

**Pfad Telnet:** /Setup/IP-Router/Firewall/Objekt-Tabelle

**Mögliche Werte:**

- max. 32 Zeichen

**Default:** Leer

#### 2.8.10.1.2 Beschreibung

In der Objekttabelle können die Stationen und Dienste beschrieben werden.

**SNMP-ID:** 2.8.10.1.2

**Pfad Telnet:** /Setup/IP-Router/Firewall/Objekt-Tabelle

**Mögliche Werte:**

- %L: lokales Netz
- %H: Gegenstellen – Name muss in DSL-/ISDN-/PPTP- oder VPN-Gegenstellenliste stehen
- %D: Hostname – Hinweis zu Hostnamen beachten
- %E: MAC-Adresse – 00:A0:57:01:02:03
- %A: IP-Adresse – %A10.0.0.1, 10.0.0.2; %A0 (alle Adressen)
- %M: Netzmaske – %M255.255.255.0
- %P: Protokoll (TCP/UDP/ICMP etc.) – %P6 (für TCP)
- %S: Dienst (Port) – %S20-25 (für Ports 20 bis 25)

**Default:** Leer

Bei der Konfiguration über die Konsole (Telnet oder Terminalprogramm) müssen die kombinierten Parameter (Port, Ziel, Quelle) jeweils in Anführungszeichen (Zollzeichen: ") eingeschlossen werden. Hostnamen können nur dann verwendet werden, wenn das LANCOM die Namen in IP-Adressen auflösen kann. Dafür muss das LANCOM die Namen über DHCP oder NetBIOS gelernt haben, oder die Zuordnung muss statisch in der DNS- oder IP-Routing-Tabelle eingetragen sein. Ein Eintrag in der IP-Routing-Tabelle kann dabei einem Hostnamen ein ganzes Netz zuordnen.

### 2.8.10.2 Regel-Tabelle

In der Regel-Tabelle werden verschiedene Informationen zu einer Firewall-Regel verknüpft. Die Regel enthält das zu filternde Protokoll, die Quelle, das Ziel sowie die auszuführende Firewall-Aktion. Zusätzlich gibt es für jede Firewall-Regel einen Ein-/Ausschalter, eine Priorität, die Option für eine Verknüpfung mit anderen Regeln und eine Aktivierung der Regel für VPN-Verbindungen.

Zur Beschreibung der Firewall-Regeln gibt es im LCOS eine spezielle Syntax. Diese Syntax erlaubt es, auch komplexe Zusammenhänge für die Prüfung und Behandlung von Datenpaketen in der Firewall mit wenigen Zeichen darzustellen. Die Regeln werden in der Regel-Tabelle definiert. Damit häufig verwendete Objekte nicht jedesmal wieder neu in der LCOS-Syntax eingetragen werden müssen, können in zwei weiteren Tabellen vordefinierte Objekte gespeichert werden:

In der Aktionstabelle sind die Firewall-Aktionen enthalten

In der Objekttabelle sind die Stationen und Dienste enthalten

Die Definition der Firewall-Regeln kann sowohl aus Einträgen der Objekttabelle für Protokolle, Dienste, Stationen und der Aktionstabelle für die Firewall-Aktionen bestehen, als auch direkte Beschreibungen in der entsprechenden LCOS-Syntax enthalten (z. B. %P6 für TCP).

**SNMP-ID:** 2.8.10.2

**Pfad Telnet:** /Setup/IP-Router/Firewall

Die Objekte aus diesen Tabellen können bei der Regeldefinition verwendet werden, müssen es aber nicht! Sie erleichtern lediglich die Verwendung von häufiger verwendeten Objekten. Bei der direkten Eingabe der Pegel-Parameter in der LCOS-Syntax gelten die gleichen Regeln, wie sie in den folgenden Abschnitten für Protokolle, Quelle und Ziel sowie die Firewall-Aktionen angegeben sind.

#### 2.8.10.2.1 Name

Geben Sie hier einen eindeutigen Namen für diese Firewall-Regel an.

**SNMP-ID:** 2.8.10.2.1

**Pfad Telnet:** /Setup/IP-Router/Firewall/Regel-Tabelle

**Mögliche Werte:**

- max. 32 Zeichen

**Default:** Leer

#### 2.8.10.2.10 Aktiv

Schaltet die Regel ein oder aus.

**SNMP-ID:** 2.8.10.2.10

**Pfad Telnet:** /Setup/IP-Router/Firewall/Regel-Tabelle

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

#### 2.8.10.2.11 VPN-Regel

Aktiviert die Regel für das Erstellen von VPN-Regeln.

**SNMP-ID:** 2.8.10.2.11

**Pfad Telnet:** /Setup/IP-Router/Firewall/Regel-Tabelle

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

#### 2.8.10.2.12 Stateful

Wenn diese Option aktiviert ist, wird geprüft, ob ein Verbindungaufbau korrekt abläuft. Fehlerhafte Pakete im Verbindungsaufbau werden verworfen. Ist diese Option nicht aktiviert, dann werden alle Pakete akzeptiert, auf die diese Regel zutrifft.

Desweiteren wird über diese Option die automatische Protokollerkennung für FTP, IRC und PPTP aktiviert, die benötigt wird, um für die jeweiligen Datenverbindungen einen Port in der Firewall öffnen zu können.

Auch die Prüfung auf Portscans/SYN-Floodings wird über diese Option aktiviert oder deaktiviert. Damit können bestimmte, stark frequentierte Server von der Prüfung ausgenommen werden, ohne die Limits für halboffene Verbindungen (DOS) oder Portanfragen (IDS) so hoch einzustellen, dass sie letztendlich unwirksam werden.

**SNMP-ID:** 2.8.10.2.12

**Pfad Telnet:** /Setup/IP-Router/Firewall/Regel-Tabelle

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

#### 2.8.10.2.13 Kommentar

Kommentar für diesen Eintrag.

**SNMP-ID:** 2.8.10.2.13

**Pfad Telnet:** /Setup/IP-Router/Firewall/Regel-Tabelle

**Mögliche Werte:**

- max. 64 Stellen

**Default:** Leer

#### 2.8.10.2.14 Rtg-Tag

Routing-Tag für die Regel.

**SNMP-ID:** 2.8.10.2.14

**Pfad Telnet:** /Setup/IP-Router/Firewall/Regel-Tabelle

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

#### 2.8.10.2.2 Prot.

Angabe der Protokolle, für welche dieser Eintrag gelten soll.

**SNMP-ID:** 2.8.10.2.2

**Pfad Telnet:** /Setup/IP-Router/Firewall/Regel-Tabelle

**Mögliche Werte:**

- Direkte Eingabe nach der LCOS-Syntax wie in der Objekttabelle beschrieben.
- Verweis auf einen Eintrag der Objekttabelle.

**Default:** Leer

#### 2.8.10.2.3 Quelle

Angabe der Quell-Stationen, für welche dieser Eintrag gelten soll.

**SNMP-ID:** 2.8.10.2.3

**Pfad Telnet:** /Setup/IP-Router/Firewall/Regel-Tabelle

**Mögliche Werte:**

- Direkte Eingabe nach der LCOS-Syntax wie in der Objekttabelle beschrieben.
- Verweis auf einen Eintrag der Objekttabelle.

**Default:** Leer

#### 2.8.10.2.4 Ziel

Angabe der Ziel-Stationen, für welche dieser Eintrag gelten soll.

**SNMP-ID:** 2.8.10.2.4

**Pfad Telnet:** /Setup/IP-Router/Firewall/Regel-Tabelle

**Mögliche Werte:**

- Direkte Eingabe nach der LCOS-Syntax wie in der Objekttabelle beschrieben.
- Verweis auf einen Eintrag der Objekttabelle.

**Default:** Leer

#### 2.8.10.2.7 Aktion

Aktion, die ausgeführt werden soll, wenn die Firewall-Regel auf ein Paket zutrifft.

**SNMP-ID:** 2.8.10.2.7

**Pfad Telnet:** /Setup/IP-Router/Firewall/Regel-Tabelle

**Mögliche Werte:**

- Direkte Eingabe nach der LCOS-Syntax wie in der Aktionstabelle beschrieben.
- Verweis auf einen Eintrag der Aktionstabelle.

**Default:** Leer

#### 2.8.10.2.8 verknuepft

Verbindet die Regel mit weiteren Regeln.

**SNMP-ID:** 2.8.10.2.8

**Pfad Telnet:** /Setup/IP-Router/Firewall/Regel-Tabelle

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

#### 2.8.10.2.9 Prio

Priorität der Regel.

**SNMP-ID:** 2.8.10.2.9

**Pfad Telnet:** /Setup/IP-Router/Firewall/Regel-Tabelle

**Mögliche Werte:**

- 0 bis 255

**Default:** Leer

### 2.8.10.3 Filter-Liste

Die Filterliste wird aus den Regeln der Firewall erzeugt. Die darin enthaltenen Filter sind statisch und ändern sich nur beim Hinzufügen, Bearbeiten oder Löschen von Firewall-Regeln.

**SNMP-ID:** 2.8.10.3

**Pfad Telnet:** /Setup/IP-Router/Firewall

#### 2.8.10.3.1 Idx.

Index zu diesem Eintrag in der Liste.

**SNMP-ID:** 2.8.10.3.1

**Pfad Telnet:** /Setup/IP-Router/Firewall/Filter-Liste

#### 2.8.10.3.10 Z-Bis

Endadresse eines Bereiches von Ziel-IP-Adressen, deren Datenpakete von diesem Eintrag erfasst werden.

**SNMP-ID:** 2.8.10.3.10

**Pfad Telnet:** /Setup/IP-Router/Firewall/Filter-Liste

#### 2.8.10.3.11 Aktion

Aktion, die für Datenpakete ausgeführt wird, die von diesem Eintrag erfasst werden.

**SNMP-ID:** 2.8.10.3.11

**Pfad Telnet:** /Setup/IP-Router/Firewall/Filter-Liste

#### 2.8.10.3.13 Quell-MAC

Quell-MAC-Adresse für Datenpakete, die von diesem Eintrag erfasst werden.

**SNMP-ID:** 2.8.10.3.13

**Pfad Telnet:** /Setup/IP-Router/Firewall/Filter-Liste

#### 2.8.10.3.14 Ziel-MAC

Ziel-MAC-Adresse für Datenpakete, die von diesem Eintrag erfasst werden.

**SNMP-ID:** 2.8.10.3.14

**Pfad Telnet:** /Setup/IP-Router/Firewall/Filter-Liste

#### 2.8.10.3.15 verknuepft

Zeigt an, ob nach dieser Aktion noch weitere Firewall-Regeln angewendet werden.

**SNMP-ID:** 2.8.10.3.15

**Pfad Telnet:** /Setup/IP-Router/Firewall/Filter-Liste

#### 2.8.10.3.16 Prio

Priorität für diesen Eintrag.

**SNMP-ID:** 2.8.10.3.16

**Pfad Telnet:** /Setup/IP-Router/Firewall/Filter-Liste

#### 2.8.10.3.17 Rtg-tag

Dieses Routing-Tag wird Datenpaketen hinzugefügt, die von diesem Eintrag erfasst werden.

**SNMP-ID:** 2.8.10.3.17

**Pfad Telnet:** /Setup/IP-Router/Firewall/Filter-Liste

#### 2.8.10.3.2 Prot.

TCP-Protokoll für Datenpakete, die von diesem Eintrag erfasst werden.

**SNMP-ID:** 2.8.10.3.2

**Pfad Telnet:** /Setup/IP-Router/Firewall/Filter-Liste

#### 2.8.10.3.3 Quell-Adresse

Quell-IP-Adresse für Datenpakete, die von diesem Eintrag erfasst werden.

**SNMP-ID:** 2.8.10.3.3

**Pfad Telnet:** /Setup/IP-Router/Firewall/Filter-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

#### 2.8.10.3.4 Quell-Netz-Maske

Quell-IP-Netzmaske für Datenpakete, die von diesem Eintrag erfasst werden.

**SNMP-ID:** 2.8.10.3.4

**Pfad Telnet:** /Setup/IP-Router/Firewall/Filter-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

#### 2.8.10.3.5 Q-Von

Anfangsadresse eines Bereiches von Quell-IP-Adressen, deren Datenpakete von diesem Eintrag erfasst werden.

**SNMP-ID:** 2.8.10.3.5

**Pfad Telnet:** /Setup/IP-Router/Firewall/Filter-Liste

#### 2.8.10.3.6 Q-Bis

Endadresse eines Bereiches von Quell-IP-Adressen, deren Datenpakete von diesem Eintrag erfasst werden.

**SNMP-ID:** 2.8.10.3.6

**Pfad Telnet:** /Setup/IP-Router/Firewall/Filter-Liste

#### 2.8.10.3.7 Ziel-Adresse

Ziel-IP-Adresse für Datenpakete, die von diesem Eintrag erfasst werden.

**SNMP-ID:** 2.8.10.3.7

**Pfad Telnet:** /Setup/IP-Router/Firewall/Filter-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

#### 2.8.10.3.8 Ziel-Netz-Maske

Ziel-IP-Netzmaske für Datenpakete, die von diesem Eintrag erfasst werden.

**SNMP-ID:** 2.8.10.3.8

**Pfad Telnet:** /Setup/IP-Router/Firewall/Filter-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

#### 2.8.10.3.9 Z-Von

Anfangsadresse eines Bereiches von Ziel-IP-Adressen, deren Datenpakete von diesem Eintrag erfasst werden.

**SNMP-ID:** 2.8.10.3.9

**Pfad Telnet:** /Setup/IP-Router/Firewall/Filter-Liste

### 2.8.10.4 Aktions-Tabelle

Eine Firewall-Aktion besteht aus einer Bedingung, einem Limit, einer Paket-Aktion und sonstigen Maßnahmen.

Die Firewall-Aktionen können wie bereits die Elemente der Objekt-Tabelle mit einem Namen versehen und beliebig rekursiv miteinander kombiniert werden, wobei die maximale Rekursionstiefe auf 16 beschränkt ist. Sie können aber auch direkt in das Aktionsfeld der Regeltabelle eingetragen werden.

**SNMP-ID:** 2.8.10.4

**Pfad Telnet:** /Setup/IP-Router/Firewall

#### 2.8.10.4.1 Name

Geben Sie hier einen eindeutigen Namen für diese Aktion an.

**SNMP-ID:** 2.8.10.4.1

**Pfad Telnet:** /Setup/IP-Router/Firewall/Aktions-Tabelle

**Mögliche Werte:**

- max. 32 Zeichen

**Default:** Leer

#### 2.8.10.4.2 Beschreibung

In der Aktionstabelle werden die Firewall-Aktionen als beliebige Kombinationen aus Bedingungen, Limits, Paket-Aktionen und weiteren Maßnahmen zusammengestellt.

**SNMP-ID:** 2.8.10.4.2

**Pfad Telnet:** /Setup/IP-Router/Firewall/Aktions-Tabelle

**Mögliche Werte:**

- 0

### 2.8.10.5 Verbindungsliste

In der Verbindungsliste wird für jede aufgebaute Verbindung ein Eintrag vorgenommen, wenn das geprüfte Paket von der Filterliste akzeptiert wird. In der Verbindungsliste wird festgehalten, von welcher Quelle zu welchem Ziel, über welches Protokoll und welchen Port eine Verbindung aktuell erlaubt ist. Darüber hinaus wird in dieser Liste festgehalten, wie

lange der Eintrag noch in der Liste stehen bleibt und welche Firewall-Regel den Eintrag erzeugt hat. Diese Liste ist sehr dynamisch und permanent “in Bewegung”.

**SNMP-ID:** 2.8.10.5

**Pfad Telnet:** /Setup/IP-Router/Firewall

#### 2.8.10.5.1 Quell-Adresse

IP-Adresse der Station, die eine Verbindung aufgebaut hat.

**SNMP-ID:** 2.8.10.5.1

**Pfad Telnet:** /Setup/IP-Router/Firewall/Verbindungsliste

**Mögliche Werte:**

- Gültige IP-Adresse.

#### 2.8.10.5.10 Ziel-Route

Ziel-Route, zu der diese Verbindung aufgebaut wurde.

**SNMP-ID:** 2.8.10.5.10

**Pfad Telnet:** /Setup/IP-Router/Firewall/Verbindungsliste

#### 2.8.10.5.11 Rtg-tag

Routing-Tag der Verbindung.

**SNMP-ID:** 2.8.10.5.11

**Pfad Telnet:** /Setup/IP-Router/Firewall/Verbindungsliste

#### 2.8.10.5.2 Ziel-Adresse

Ziel-IP-Adresse, zu der eine Verbindung aufgebaut wurde.

**SNMP-ID:** 2.8.10.5.2

**Pfad Telnet:** /Setup/IP-Router/Firewall/Verbindungsliste

**Mögliche Werte:**

- Gültige IP-Adresse.

#### 2.8.10.5.3 Prot.

Protokoll, das auf dieser Verbindung zugelassen ist.

**SNMP-ID:** 2.8.10.5.3

**Pfad Telnet:** /Setup/IP-Router/Firewall/Verbindungsliste

#### 2.8.10.5.4 Quell-Port

Quell-Port der Station, die eine Verbindung aufgebaut hat.

**SNMP-ID:** 2.8.10.5.4

**Pfad Telnet:** /Setup/IP-Router/Firewall/Verbindungsliste

#### 2.8.10.5.5 Ziel-Port

Ziel-Port, zu der eine Verbindung aufgebaut wurde.

**SNMP-ID:** 2.8.10.5.5

**Pfad Telnet:** /Setup/IP-Router/Firewall/Verbindungsliste

#### 2.8.10.5.6 Timeout

Gültigkeitsdauer dieses Eintrags in der Tabelle.

**SNMP-ID:** 2.8.10.5.6

**Pfad Telnet:** /Setup/IP-Router/Firewall/Verbindungsliste

#### 2.8.10.5.7 Flags

In den Flags wird der Zustand der Verbindung und weitere (interne) Informationen in einem Bitfeld gespeichert.

Als Zustände sind folgende Werte möglich: new, establish, open, closing, closed, rejected (entsprechend der TCP-Flags: SYN, SYN ACK, ACK, FIN, FIN ACK und RST).

UDP-Verbindungen kennen nun die Zustände new, open und closing (letzteren nur, wenn die UDP-Verbindung mit einem zustandsbehafteten Steuerkanal verknüpft ist. Dies ist z. B. beim Protokoll H.323 der Fall).

**Pfad Telnet:** /Setup/IP-Router/Firewall/Verbindungsliste

**Mögliche Werte:**

- 00000001 TCP: SYN gesendet
- 00000002 TCP: SYN/ACK empfangen
- 00000004 TCP: warte auf ACK des Servers
- 00000008 alle: Verbindung offen
- 00000010 TCP: FIN empfangen
- 00000020 TCP: FIN gesendet
- 00000040 TCP: RST gesendet oder empfangen
- 00000080 TCP: Sitzung wird wiederhergestellt
- 00000100 FTP: passive FTP-Verbindung wird aufgebaut
- 00000400 H.323: zugehörige T.120-Verbindung
- 00000800: Verbindung über Loopback-Interface
- 00001000: prüfe verkettete Regeln
- 00002000: Regel ist verkettet
- 00010000: Ziel ist auf "lokaler Route"
- 00020000: Ziel ist auf Default-Route
- 00040000: Ziel ist auf VPN-Route
- 00080000: physikalische Verbindung ist nicht aufgebaut
- 00100000: Quelle ist auf Default-Route
- 00200000: Quelle ist auf VPN-Route
- 00800000: keine Route zum Ziel
- 01000000: enthält globale Aktion mit Bedingung

#### 2.8.10.5.8 Filterregel

Zeigt die Filterregel, die diesen Eintrag erzeugt hat.

**SNMP-ID:** 2.8.10.5.8

**Pfad Telnet:** /Setup/IP-Router/Firewall/Verbindungsliste

#### 2.8.10.5.9 Quell-Route

Quell-Route, über welche diese Verbindung aufgebaut wurde.

**SNMP-ID:** 2.8.10.5.9

**Pfad Telnet:** /Setup/IP-Router/Firewall/Verbindungsliste

## 2.8.10.6 Hostsperrliste

In der Hostsperrliste werden die Stationen aufgeführt, die aufgrund einer Firewall-Aktion für eine bestimmte Zeit gesperrt sind. Die Liste ist dynamisch, neue Einträge können fortlaufend durch entsprechende Aktionen der Firewall hinzugefügt werden, nach Ablauf der Sperrzeit verschwinden die Einträge automatisch.

**SNMP-ID:** 2.8.10.6

**Pfad Telnet:** /Setup/IP-Router/Firewall

### 2.8.10.6.1 Quell-Adresse

Quell-IP-Adresse, die durch diesen Eintrag gesperrt ist.

**SNMP-ID:** 2.8.10.6.1

**Pfad Telnet:** /Setup/IP-Router/Firewall/Hostsperrliste

**Mögliche Werte:**

- Gültige IP-Adresse.

### 2.8.10.6.2 Timeout

Gültigkeitsdauer dieses Eintrags in der Tabelle.

**SNMP-ID:** 2.8.10.6.2

**Pfad Telnet:** /Setup/IP-Router/Firewall/Hostsperrliste

### 2.8.10.6.3 Filterregel

Zeigt die Filterregel, die diesen Eintrag erzeugt hat.

**SNMP-ID:** 2.8.10.6.3

**Pfad Telnet:** /Setup/IP-Router/Firewall/Hostsperrliste

## 2.8.10.7 Portsperrliste

In der Portsperrliste werden die Protokolle und Dienste aufgeführt, die aufgrund einer Firewall-Aktion für eine bestimmte Zeit gesperrt sind. Diese Liste ist dynamisch, neue Einträge können fortlaufend durch entsprechende Aktionen der Firewall hinzugefügt werden, nach Ablauf der Sperrzeit verschwinden die Einträge automatisch.

**SNMP-ID:** 2.8.10.7

**Pfad Telnet:** /Setup/IP-Router/Firewall

### 2.8.10.7.1 Ziel-Adresse

Ziel-IP-Adresse, die durch diesen Eintrag gesperrt ist.

**SNMP-ID:** 2.8.10.7.1

**Pfad Telnet:** /Setup/IP-Router/Firewall/Portsperrliste

**Mögliche Werte:**

- Gültige IP-Adresse.

### 2.8.10.7.2 Prot.

Protokoll, das durch diesen Eintrag gesperrt ist.

**SNMP-ID:** 2.8.10.7.2

**Pfad Telnet:** /Setup/IP-Router/Firewall/Portsperrliste

#### 2.8.10.7.3 Ziel-Port

Ziel-Port, der durch diesen Eintrag gesperrt ist.

**SNMP-ID:** 2.8.10.7.3

**Pfad Telnet:** /Setup/IP-Router/Firewall/Portsperrliste

#### 2.8.10.7.4 Timeout

Gültigkeitsdauer dieses Eintrags in der Tabelle.

**SNMP-ID:** 2.8.10.7.4

**Pfad Telnet:** /Setup/IP-Router/Firewall/Portsperrliste

#### 2.8.10.7.5 Filterregel

Zeigt die Filterregel, die diesen Eintrag erzeugt hat.

**SNMP-ID:** 2.8.10.7.5

**Pfad Telnet:** /Setup/IP-Router/Firewall/Portsperrliste

### 2.8.10.19 Open-Port-Liste

In der Portsperrliste werden die Protokolle und Dienste aufgeführt, die aufgrund einer Firewall-Aktion für eine bestimmte Zeit geöffnet sind. Diese Liste ist dynamisch, neue Einträge können fortlaufend durch entsprechende Aktionen der Firewall hinzugefügt werden, nach Ablauf der Sperrzeit verschwinden die Einträge automatisch.

**SNMP-ID:** 2.8.10.19

**Pfad Telnet:** /Setup/IP-Router/Firewall

#### 2.8.10.19.1 Quell-Adresse

Quell-IP-Adresse, welche die geöffneten Ports und Protokolle aus diesem Eintrag nutzen kann.

**SNMP-ID:** 2.8.10.19.1

**Pfad Telnet:** /Setup/IP-Router/Firewall/Open-Port-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

#### 2.8.10.19.2 Ziel-Adresse

Ziel-IP-Adresse, zu der über die geöffneten Ports und Protokolle aus diesem Eintrag Verbindungen aufgebaut werden können.

**SNMP-ID:** 2.8.10.19.2

**Pfad Telnet:** /Setup/IP-Router/Firewall/Open-Port-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

#### 2.8.10.19.3 Prot.

Protokoll, das durch diesen Eintrag geöffnet ist.

**SNMP-ID:** 2.8.10.19.3

**Pfad Telnet:** /Setup/IP-Router/Firewall/Open-Port-Liste

#### 2.8.10.19.5 Ziel-Port

Ziel-Port, der durch diesen Eintrag geöffnet ist.

**SNMP-ID:** 2.8.10.19.5

**Pfad Telnet:** /Setup/IP-Router/Firewall/Open-Port-Liste

#### 2.8.10.19.6 Timeout

Gültigkeitsdauer dieses Eintrags in der Tabelle.

**SNMP-ID:** 2.8.10.19.6

**Pfad Telnet:** /Setup/IP-Router/Firewall/Open-Port-Liste

#### 2.8.10.19.8 Filterregel

Zeigt die Filterregel, die diesen Eintrag erzeugt hat.

**SNMP-ID:** 2.8.10.19.8

**Pfad Telnet:** /Setup/IP-Router/Firewall/Open-Port-Liste

#### 2.8.10.19.9 Quell-Route

Quell-Route, über welche diese Verbindung aufgebaut wurde.

**SNMP-ID:** 2.8.10.19.9

**Pfad Telnet:** /Setup/IP-Router/Firewall/Open-Port-Liste

### 2.8.10.20 Anwendungen

Dieses Menü enthält die Konfiguration einzelner Anwendungen für ihre Firewall.

**SNMP-ID:** 2.8.10.20

**Pfad Telnet:** /Setup/IP-Router/Firewall

#### 2.8.10.20.10 Anw.-Aktion

Wenn eine IRC-Session auf einem beliebigen Port erkannt wird, werden die konfigurierbaren Gegenmaßnahmen ergriffen.

**SNMP-ID:** 2.8.10.20.10

**Pfad Telnet:** /Setup/IP-Router/Firewall/Anwendungen

**Mögliche Werte:**

- Übertragen
- Verwerfen
- Zurückweisen

**Default:** Zurückweisen

#### 2.8.10.20.1 FTP

Dieses Menü enthält die Konfiguration von FTP für ihre Firewall.

**SNMP-ID:** 2.8.10.20.1

**Pfad Telnet:** /Setup/IP-Router/Firewall/Anwendungen

#### 2.8.10.20.1.2 Actives-FTP-Blockieren

Wenn eine FTP-Session auf einem beliebigen Port erkannt wird, werden die konfigurierbaren Gegenmaßnahmen ergriffen. 'Auf aktives FTP reagieren' gibt an, ob und auf welchen Routen aktives FTP sonderbehandelt werden soll.

**SNMP-ID:** 2.8.10.20.1.2

**Pfad Telnet:** /Setup/IP-Router/Firewall/Anwendungen/FTP

**Mögliche Werte:**

- Nein
- Immer
- Nur für WAN-Route
- Nur für Default-Route

**Default:** Nein

#### 2.8.10.20.1.1 FTP-Blockieren

Wenn eine FTP-Session auf einem beliebigen Port erkannt wird, werden die konfigurierbaren Gegenmaßnahmen ergriffen. 'Auf jede FTP-Session reagieren' gibt an, ob und auf welchen Routen jede Art von FTP sonderbehandelt werden soll.

**SNMP-ID:** 2.8.10.20.1.1

**Pfad Telnet:** /Setup/IP-Router/Firewall/Anwendungen/FTP

**Mögliche Werte:**

- Aus
- Immer
- WAN
- Default-Route

**Default:** Nein

#### 2.8.10.20.1.5 FXP-Blockieren

Wenn eine FTP-Session auf einem beliebigen Port erkannt wird, werden die konfigurierbaren Gegenmaßnahmen ergriffen. 'Auf FXP-Sessions reagieren' gibt an, ob Site-To-Site-Transfers (FXP) sonderbehandelt werden soll.

**SNMP-ID:** 2.8.10.20.1.5

**Pfad Telnet:** /Setup/IP-Router/Firewall/Anwendungen/FTP

**Mögliche Werte:**

- Nein
- Immer
- Nur für WAN-Route
- Nur für Default-Route

**Default:** Nur für Default-Route

#### 2.8.10.20.1.4 Host-IP-Pruefen

Wenn eine FTP-Session auf einem beliebigen Port erkannt wird, werden die konfigurierbaren Gegenmaßnahmen ergriffen. 'Stations-IP-Adresse prüfen' gibt an, ob und auf welchen Routen die im FTP-Kommando-Kanal übermittelte Adresse gegen die Quelladresse des FTP-Clients geprüft werden soll. Stimmt sie nicht, werden die unten konfigurierten Gegenmaßnahmen ergriffen. Wenn ein Site-To-Site-Transfers stattfinden soll und auch erlaubt ist, dann wird diese Überprüfung natürlich nicht durchgeführt.

**SNMP-ID:** 2.8.10.20.1.4

**Pfad Telnet:** /Setup/IP-Router/Firewall/Anwendungen/FTP

**Mögliche Werte:**

- Nein
- Immer
- Nur für WAN-Route
- Nur für Default-Route

**Default:** Nur für Default-Route

#### 2.8.10.20.1.3 Min-Port

Wenn eine FTP-Session auf einem beliebigen Port erkannt wird, werden die konfigurierbaren Gegenmaßnahmen ergriffen. "Die kleinste erlaubte Port-Nummer" gibt den kleinsten zulässigen Port beim aktiven FTP an.

**SNMP-ID:** 2.8.10.20.1.3

**Pfad Telnet:** /Setup/IP-Router/Firewall/Anwendungen/FTP

**Mögliche Werte:**

- 1024 bis 9999

**Default:** 1024

### 2.8.10.20.2 IRC

Dieses Menü enthält die Konfiguration von IRC für ihre Firewall.

**SNMP-ID:** 2.8.10.20.2

**Pfad Telnet:** /Setup/IP-Router/Firewall/Anwendungen

#### 2.8.10.20.2.2 DDC-Blockieren

Wenn eine IRC-Session auf einem beliebigen Port erkannt wird, werden die konfigurierbaren Gegenmaßnahmen ergriffen. 'Auf DDC reagieren' gibt an, ob und auf welchen Routen Direct-Data-Connect (private Chats und Filetransfers) sonderbehandelt werden sollen.

**SNMP-ID:** 2.8.10.20.2.2

**Pfad Telnet:** /Setup/IP-Router/Firewall/Anwendungen/IRC

**Mögliche Werte:**

- Nein
- Immer
- Nur für WAN-Route
- Nur für Default-Route

**Default:** Nein

#### 2.8.10.20.2.4 Host-IP-Pruefen

Wenn eine IRC-Session auf einem beliebigen Port erkannt wird, werden die konfigurierbaren Gegenmaßnahmen ergriffen. 'Stations-IP-Adresse prüfen' gibt an, ob und auf welchen Routen die im DDC-Kommando übermittelte Adresse gegen die Quelladresse des IRC-Clients geprüft werden soll.

**SNMP-ID:** 2.8.10.20.2.4

**Pfad Telnet:** /Setup/IP-Router/Firewall/Anwendungen/IRC

**Mögliche Werte:**

- Nein

- Immer
- Nur für WAN-Route
- Nur für Default-Route

**Default:** Nur für Default-Route

#### 2.8.10.20.2.1 IRC-Blockieren

Wenn eine IRC-Session auf einem beliebigen Port erkannt wird, werden die konfigurierbaren Gegenmaßnahmen ergriffen. 'Auf IRC reagieren' gibt an, ob und auf welchen Routen jede Art von IRC sonderbehandelt werden.

**SNMP-ID:** 2.8.10.20.2.1

**Pfad Telnet:** /Setup/IP-Router/Firewall/Anwendungen/IRC

**Mögliche Werte:**

- Nein
- Immer
- Nur für WAN-Route
- Nur für Default-Route

**Default:** Nein

#### 2.8.10.20.2.3 Min-Port

Wenn eine IRC-Session auf einem beliebigen Port erkannt wird, werden die konfigurierbaren Gegenmaßnahmen ergriffen. 'Kleinste erlaubte Port-Nummer" gibt den kleinsten zulässigen Port beim DDC an.

**SNMP-ID:** 2.8.10.20.2.3

**Pfad Telnet:** /Setup/IP-Router/Firewall/Anwendungen/IRC

**Mögliche Werte:**

- 1024 bis 9999

**Default:** 1024

## 2.8.13 Default-Zeit-Liste

Über die zeitabhängige Steuerung können Sie, abhängig vom Wochentag und von der Uhrzeit, verschiedene Ziele für die Default-Route angeben.

**SNMP-ID:** 2.8.13

**Pfad Telnet:** /Setup/IP-Router

### 2.8.13.1 Index

Index für diesen Eintrag in der Liste.

**SNMP-ID:** 2.8.13.1

**Pfad Telnet:** /Setup/IP-Router/Default-Zeit_Liste

### 2.8.13.2 Tage

Wählen Sie die Tage, wann dieser Eintrag verwendet werden soll.

**SNMP-ID:** 2.8.13.2

**Pfad Telnet:** /Setup/IP-Router/Default-Zeit_Liste

**Mögliche Werte:**

- Mo
- Di
- Mi
- Do
- Fr
- Sa
- So
- Feiertags

**Default:** Es sind keine Tage markiert

### 2.8.13.3 Start

Wählen Sie den Zeitraum, wann dieser Eintrag verwendet werden soll.

**SNMP-ID:** 2.8.13.3

**Pfad Telnet:** /Setup/IP-Router/Default-Zeit_Liste

**Mögliche Werte:**

- 00:00 bis 23:59

**Default:** 0

### 2.8.13.4 Stop

Wählen Sie den Zeitraum, wann dieser Eintrag verwendet werden soll.

**SNMP-ID:** 2.8.13.4

**Pfad Telnet:** /Setup/IP-Router/Default-Zeit_Liste

**Mögliche Werte:**

- 00:00 bis 23:59

**Default:** 0.999305556

### 2.8.13.5 Gegenstelle

Sobald dieser Eintrag gültig wird, weil der angegebene Zeitraum erreicht ist, wird die hier angegebene Gegenstelle als Ziel der Default-Route verwendet. Wählen Sie dazu den Namen einer Gegenstelle aus der Liste der Gegenstellen aus.

**SNMP-ID:** 2.8.13.5

**Pfad Telnet:** /Setup/IP-Router/Default-Zeit_Liste

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen

## 2.8.19 N-N-NAT

Die N:N-NAT-Tabelle enthält Regeln, auf welche IP-Adressen die Quell-Adressen einzelner Stationen oder ganzer IP-Netze umgesetzt werden sollen. Diese Regeln müssen für jede Gegenstelle gesondert spezifiziert werden, da die Umsetzung nach dem Routen erfolgt. Für die Gegenstelle sind die Stationen oder Netzwerke unter ihrer angegebenen umgesetzten IP-Adresse erreichbar.

**SNMP-ID:** 2.8.19

**Pfad Telnet:** /Setup/IP-Router

### 2.8.19.1 Idx.

Eindeutiger Index des Eintrags.

**SNMP-ID:** 2.8.19.1

**Pfad Telnet:** /Setup/IP-Router/N-N-NAT

**Mögliche Werte:**

- max. 4 Zeichen

**Default:** Leer

### 2.8.19.2 Quell-Adresse

IP-Adresse des Rechners oder Netzes, dass eine alternative IP-Adresse erhalten soll.

**SNMP-ID:** 2.8.19.2

**Pfad Telnet:** /Setup/IP-Router/N-N-NAT

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.8.19.3 Quell-Maske

Netzmaske des Quell-Bereiches.

**SNMP-ID:** 2.8.19.3

**Pfad Telnet:** /Setup/IP-Router/N-N-NAT

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.8.19.4 Ziel-Gegenstelle

Name der Gegenstelle, über die das entfernte Netzwerk erreicht werden kann.

**SNMP-ID:** 2.8.19.4

**Pfad Telnet:** /Setup/IP-Router/N-N-NAT

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen.

**Default:** Leer

### 2.8.19.5 Neue-Netz-Adr.

IP-Adresse oder -Adressebereich, der für die Umsetzung verwendet werden soll.

**SNMP-ID:** 2.8.19.5

**Pfad Telnet:** /Setup/IP-Router/N-N-NAT

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

Für die neue Netzadresse wird jeweils die gleiche Netzmaske verwendet, die auch schon die Quell-Adresse verwendet. Für die Zuordnung von Quell- und Mapping-Adresse gelten folgende Hinweise:

- Bei der Umsetzung von einzelnen Adressen können Quelle und Mapping beliebig zugeordnet werden.
- Bei der Umsetzung von ganzen Adressbereichen wird der rechnerbezogene Teil der IP-Adresse direkt übernommen und nur an den netzbezogenen Teil der Mapping-Adresse angehängt. Bei einer Zuweisung von 10.0.0.0/255.255.255.0 nach 192.168.1.0 wird also dem Server im LAN mit der IP-Adresse 10.1.1.99 zwangsweise die Mapping-Adresse 192.168.1.99 zugewiesen.

Der Adressbereich für die Umsetzung muss mindestens so groß sein wie der Quell-Adressbereich.

Bitte beachten Sie, dass die Funktionen des N:N-Mapping nur wirksam sind, wenn die Firewall eingeschaltet ist.

## 2.8.20 Load-Balancer

Dieses Menü enthält die Konfiguration von Load-Balancing für ihren IP-Router.

**SNMP-ID:** 2.8.20

**Pfad Telnet:** /Setup/IP-Router

### 2.8.20.1 Aktiv

Hier werden die Load-Balancing (Last-Verteilung) Parameter eingestellt. Load-Balancing kann genutzt werden, wenn Ihr Provider keine echte Kanal-Bündelung anbietet. Mindestens eine virtuelle Verbindung muss dafür in der Load-Balancing-Tabelle festgelegt werden. Wieviele Gegenstellen maximal gebündelt weden können hängt davon ab, wie viele DSL-Ports der verwendete Gerätetyp zur Verfügung stellt.

**SNMP-ID:** 2.8.20.1

**Pfad Telnet:** /Setup/IP-Router/Load-Balancer

**Mögliche Werte:**

- aktiv
- inaktiv

**Default:** inaktiv

### 2.8.20.2 Buendel-Gegenstellen

Wenn Ihr Internet-Anbieter keine echte Kanal-Bündelung zur Verfügung stellt, ist es möglich mehrere Verbindungen mit Hilfe des Load-Balancing zusammenzufassen.

**SNMP-ID:** 2.8.20.2

**Pfad Telnet:** /Setup/IP-Router/Load-Balancer

#### 2.8.20.2.1 Gegenstelle

Eindeutiger Name für eine virtuelle Load-Balancing-Gegenstelle. Diese Gegenstelle kann dann in der Routing-Tabelle verwendet werden.

**SNMP-ID:** 2.8.20.2.1

**Pfad Telnet:** /Setup/IP-Router/Load-Balancer/Buendel-Gegenstellen

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen

**Default:** leer

#### 2.8.20.2.2 Buendel-GgSt.-1

Name einer bereits konfigurierten Gegenstelle zu der weitere hinzugebündelt werden sollen.

**SNMP-ID:** 2.8.20.2.2

**Pfad Telnet:** /Setup/IP-Router/Load-Balancer/Buendel-Gegenstellen

**Mögliche Werte:**

- max. 16 Zeichen

**Default:** leer

#### 2.8.20.2.3 Buendel-GgSt.-2

Name einer bereits konfigurierten Gegenstelle zu der weitere hinzugebündelt werden sollen.

**SNMP-ID:** 2.8.20.2.3

**Pfad Telnet:** /Setup/IP-Router/Load-Balancer/Buendel-Gegenstellen

**Mögliche Werte:**

- max. 16 Zeichen

**Default:** leer

#### 2.8.20.2.4 Buendel-GgSt.-3

Name einer bereits konfigurierten Gegenstelle zu der weitere hinzugebündelt werden sollen.

**SNMP-ID:** 2.8.20.2.4

**Pfad Telnet:** /Setup/IP-Router/Load-Balancer/Buendel-Gegenstellen

**Mögliche Werte:**

- max. 16 Zeichen

**Default:** leer

#### 2.8.20.2.5 Buendel-GgSt.-4

Name einer bereits konfigurierten Gegenstelle zu der weitere hinzugebündelt werden sollen.

**SNMP-ID:** 2.8.20.2.5

**Pfad Telnet:** /Setup/IP-Router/Load-Balancer/Buendel-Gegenstellen

**Mögliche Werte:**

- max. 16 Zeichen

**Default:** leer

## 2.8.21 VRRP

Dieses Menü enthält die Konfiguration von VRRP für ihren IP-Router.

**SNMP-ID:** 2.8.21

**Pfad Telnet:** /Setup/IP-Router

### 2.8.21.1 Aktiv

Das Virtual-Router-Redundancy-Protocol dient dazu, mehrere physikalische Router wie einen einzigen "virtuellen" Router erscheinen zu lassen. Von den vorhandenen physikalischen Routern ist immer einer der sogenannte Master. Dieser Master ist der einzige, der wirklich eine Verbindung z. B. ins Internet hat und Daten überträgt. Erst wenn der Master ausfällt, weil z. B. die Spannungsversorgung unterbrochen oder seine Internetanbindung ausgefallen ist, werden die anderen Router aktiv. Über das Protokoll VRRP, handeln sie nun aus, wer als nächster die Rolle des Masters zu übernehmen hat. Der neue Master übernimmt vollständig die Aufgaben des bisherigen Masters.

**SNMP-ID:** 2.8.21.1

**Pfad Telnet:** /Setup/IP-Router/VRRP

**Mögliche Werte:**

- aktiv
- inaktiv

**Default:** inaktiv

### 2.8.21.4 Anz.-IntervallInterne-Dienste

Das Advertising-Intervall gibt an nach wie vielen Sekunden ein Router neu propagiert wird. Alle Router des Virtuellen-Router-Systems müssen den gleichen Wert konfiguriert haben

**SNMP-ID:** 2.8.21.4

**Pfad Telnet:** /Setup/IP-Router/VRRP

**Mögliche Werte:**

- 0 bis 999 Sekunden

**Default:** 1 Sek.

### 2.8.21.5 Interne-Dienste

Der Schalter "Interne Dienste" steuert das Verhalten des Routers, wenn er unter der Adresse eines virtuellen Routers angesprochen wird. In der Default-Einstellung "on" reagiert der Router bei den Diensten DNS und NETBIOS genau so, als wäre er unter seiner realen Adresse angesprochen worden. Dies funktioniert jedoch nur, wenn der Router selbst Master des virtuellen Routers ist. Die Einstellung "off" bewirkt RFC konformes Verhalten, d.h. entsprechende Pakete werden verworfen.

**SNMP-ID:** 2.8.21.5

**Pfad Telnet:** /Setup/IP-Router/VRRP

**Mögliche Werte:**

- ein
- aus

**Default:** ein

### 2.8.21.3 Reconnect-Verz.

Wenn die Backup-Verbindung eines Routers nicht aufgebaut werden konnte, wird der Router nicht mehr propagiert. Das Reconnect-Delay gibt an, nach wie vielen Minuten ein solcher Router in diesem Fall versucht, seine Haupt- oder Backup-Verbindung erneut aufzubauen. Während dieses Versuchs wird dieser Router weiterhin nicht propagiert.

**SNMP-ID:** 2.8.21.3

**Pfad Telnet:** /Setup/IP-Router/VRRP

**Mögliche Werte:**

- 0 bis 999 Minuten

**Default:** 30 Min.

## 2.8.21.2 VRRP-Liste

In der VRRP-Liste können Sie virtuelle Router definieren und konfigurieren.

**SNMP-ID:** 2.8.21.2

**Pfad Telnet:** /Setup/IP-Router/VRRP

### 2.8.21.2.1 Router-ID

Eindeutige ID des virtuellen Routers.

**SNMP-ID:** 2.8.21.2.1

**Pfad Telnet:** /Setup/IP-Router/VRRP/VRRP-Liste

**Mögliche Werte:**

- 0 bis 255

**Default:** 1

### 2.8.21.2.2 virt.-Adresse

IP-Adresse des virtuellen Routers. Alle Router auf denen der virtuelle Router eingerichtet ist, müssen diesem die gleiche IP-Adresse zuweisen.

**SNMP-ID:** 2.8.21.2.2

**Pfad Telnet:** /Setup/IP-Router/VRRP/VRRP-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.8.21.2.3 Prio

Haupt-Priorität des virtuellen Routers. Es sind Werte zwischen 0 und 255 zulässig. Die Priorität ist proportional zum eingetragenen Wert. Dabei haben die Werte 0 und 255 eine besondere Bedeutung. Der Wert 0 schaltet den virtuellen Router aus. Der Wert 255 wird nur akzeptiert, wenn die Adresse des virtuellen Routers gleich der Adresse des Interfaces ist, an das der Router gebunden ist. Ist das nicht der Fall, wird der Router von allen anderen Routern im Event-Log gemeldet.

**SNMP-ID:** 2.8.21.2.3

**Pfad Telnet:** /Setup/IP-Router/VRRP/VRRP-Liste

**Mögliche Werte:**

- 0 bis 255

**Default:** 0

### 2.8.21.2.4 B-Prio

Backup-Priorität des virtuellen Routers. Es sind Werte zwischen 0 und 255 zulässig. Die Priorität ist proportional zum eingetragenen Wert. Dabei haben die Werte 0 und 255 eine besondere Bedeutung. Der Wert 0 deaktiviert den virtuellen Router im Backup-Fall. Es wird in regelmäßigen Intervallen geprüft, ob die Hauptverbindung wieder aufgebaut werden

kann. Das Intervall legt der Reconnect-Delay-Parameter fest. Der Wert 255 wird nur akzeptiert, wenn die Adresse des virtuellen Routers gleich der Adresse des Interfaces ist, an das der Router gebunden ist. Ist das nicht der Fall, wird der Router von allen anderen Routern im Event-Log gemeldet. Wenn im Backup-Fall auch die Backup-Verbindung nicht aufgebaut werden kann, geht der virtuelle Router vollständig in den Stand-by-Modus und versucht in Intervallen entweder die Haupt- oder die Backup-Verbindung erneut aufzubauen.

**SNMP-ID:** 2.8.21.2.4

**Pfad Telnet:** /Setup/IP-Router/VRRP/VRRP-Liste

**Mögliche Werte:**

- 0 bis 255

**Default:** 0

#### 2.8.21.2.5 Gegenstelle

Der Eintrag des Gegenstellennamens ist optioal. Wird hier eine Gegenstelle eingetragen, so steuert diese das VRRP. Verliert diese Gegenstelle bspw. Ihre Internetanbindung, so tritt der Backup-Fall ein. Wird keine eingetragen, so kann man VRRP dazu nutzen einen Hardware-Ausfall abzudecken. Die Gegenstelle kann auch weiteren virtuellen Routern zugeordnet werden.

**SNMP-ID:** 2.8.21.2.5

**Pfad Telnet:** /Setup/IP-Router/VRRP/VRRP-Liste

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen.

**Default:** leer

#### 2.8.21.2.6 Kommentar

Hier können Sie einen Kommentar zur Beschreibung des virtuellen Routers einfügen.

**SNMP-ID:** 2.8.21.2.6

**Pfad Telnet:** /Setup/IP-Router/VRRP/VRRP-Liste

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** leer

## 2.8.23 Tag-Tabelle

Über die Tag-Tabelle kann den eingehenden Datenpaketen anhand der Gegenstelle direkt ein Schnittstellen-Tag zugewiesen werden.

**SNMP-ID:** 2.8.23

**Pfad Telnet:** /Setup/IP-Router

### 2.8.23.1 Gegenstelle

Name der Gegenstelle, zu deren Paketen beim Empfang Schnittstellen-Tags hinzugefügt werden sollen.

**SNMP-ID:** 2.8.23.1

**Pfad Telnet:** /Setup/IP-Router/Tag-Tabelle

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen

**Default:** Leer

**Besondere Werte:** Mit dem * als Platzhalter können in einem Eintrag mehrere Gegenstellen konfiguriert werden. Sollen z. B. mehrere Gegenstellen (RAS-Benutzer) einer Firma getaggt werden, können alle entsprechenden Gegenstellen einen Namen mit dem Prefix "Firma1_" bekommen. In der Tag-Tabelle wird dann nur noch ein Eintrag mit der Gegenstelle "Firma1_*" aufgenommen, um alle Gegenstellen zu konfigurieren.

### 2.8.23.2 Rtg-Tag

Dieses Schnittstellen-Tag wird den eingehenden Paketen der Gegenstelle zugewiesen.

**SNMP-ID:** 2.8.23.2

**Pfad Telnet:** /Setup/IP-Router/Tag-Tabelle

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.8.23.3 Start-WAN-Pool

Der Start-WAN-Pool stellt den Beginn des Adress-Pools für die Gegenstelle bzw. die Gruppe von Gegenstellen dar (bei Verwendung von Platzhaltern bei der Angabe der Gegenstelle). Bei der Einwahl von RAS-Benutzern wird der Gegenstelle eine Adresse aus dem hier definierten Adress-Pool zugewiesen.

**SNMP-ID:** 2.8.23.3

**Pfad Telnet:** /Setup/IP-Router/Tag-Tabelle

**Mögliche Werte:**

- Gültige IP-Adresse

**Default:** 0.0.0.0

### 2.8.23.4 Ende-WAN-Pool

Der End-WAN-Pool stellt das Ende des Adress-Pools für die Gegenstelle bzw. die Gruppe von Gegenstellen dar (bei Verwendung von Platzhaltern bei der Angabe der Gegenstelle). Bei der Einwahl von RAS-Benutzern wird der Gegenstelle eine Adresse aus dem hier definierten Adress-Pool zugewiesen.

**SNMP-ID:** 2.8.23.4

**Pfad Telnet:** /Setup/IP-Router/Tag-Tabelle

**Mögliche Werte:**

- Gültige IP-Adresse

**Default:** 0.0.0.0

**Besondere Werte:** Wenn der Pool leer ist (Start- und End-Adresse sind 0.0.0.0), dann wird der globale Pool verwendet.

## 2.9 SNMP

Dieses Menü enthält die Konfiguration von SNMP.

**SNMP-ID:** 2.9

**Pfad Telnet:** /Setup

## 2.9.3 Administrator

Name des Geräte-Administrators. Wird nur zu Anzeigezwecken verwendet.

**SNMP-ID:** 2.9.3

**Pfad Telnet:** /Setup/SNMP

**Mögliche Werte:**

- max. 255 Zeichen

**Default:** Leer

## 2.9.11 Kommentar-1

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

**SNMP-ID:** 2.9.11

**Pfad Telnet:** /Setup/SNMP

**Mögliche Werte:**

- max. 255 Zeichen

**Default:** Leer

## 2.9.12 Kommentar-2

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

**SNMP-ID:** 2.9.12

**Pfad Telnet:** /Setup/SNMP

**Mögliche Werte:**

- max. 255 Zeichen

**Default:** Leer

## 2.9.13 Kommentar-3

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

**SNMP-ID:** 2.9.13

**Pfad Telnet:** /Setup/SNMP

**Mögliche Werte:**

- max. 255 Zeichen

**Default:** Leer

## 2.9.14 Kommentar-4

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

**SNMP-ID:** 2.9.14

**Pfad Telnet:** /Setup/SNMP

**Mögliche Werte:**

- max. 255 Zeichen

**Default:** Leer

## 2.9.16 Kommentar-5

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

**SNMP-ID:** 2.9.16

**Pfad Telnet:** /Setup/SNMP

**Mögliche Werte:**

- max. 255 alphanumerische Zeichen

**Default:** Leer

## 2.9.17 Kommentar-6

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

**SNMP-ID:** 2.9.17

**Pfad Telnet:** /Setup/SNMP

**Mögliche Werte:**

- max. 255 alphanumerische Zeichen

**Default:** Leer

## 2.9.17 Kommentar-7

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

**SNMP-ID:** 2.9.17

**Pfad Telnet:** /Setup/SNMP

**Mögliche Werte:**

- max. 255 alphanumerische Zeichen

**Default:** Leer

## 2.9.17 Kommentar-8

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

**SNMP-ID:** 2.9.17

**Pfad Telnet:** /Setup/SNMP

**Mögliche Werte:**

- max. 255 alphanumerische Zeichen

**Default:** Leer

## 2.9.6 Loesche-Monitor

Mit dieser Aktion können angemeldete SNMP-Agenten aus der Monitor-Liste entfernt werden. Zu dem Kommando werden dazu die IP-Adresse und der Port des SNMP-Agenten angegeben. Alle drei Werte können durch den Platzhalter * ersetzt werden, in diesem Fall ermittelt das Gerät die Werte aus den vom SNMP-Agenten empfangenen Paketen.

**SNMP-ID:** 2.9.6

**Pfad Telnet:** /Setup/SNMP

**Mögliche Werte:**

- <IP-Adresse|*>:<Port|*>

**Default:** Leer

## 2.9.10 Passw.Zwang-fuer-SNMP-Lesezugriff

Mit dieser Option können Sie entscheiden, dass zum Lesen von SNMP-Meldungen über einen SNMP-Agenten (z. B.LANmonitor) ein Passwort benötigt wird. Ist diese Option aktiviert, so muss zwingend das Gerätepasswort (oder Username:Passwort) als Community verwendet werden.

**SNMP-ID:** 2.9.10

**Pfad Telnet:** /Setup/SNMP

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

## 2.9.15 Read-Only-Community

Mit dem Eintrag einer Read-Only-Community kann auch die Authentifizierung über TACACS+ für den LANmonitor deaktiviert werden. Die dort definierte Read-Only- Community wird dazu im LANmonitor als Benutzername eingetragen.

**SNMP-ID:** 2.9.15

**Pfad Telnet:** /Setup/SNMP

**Mögliche Werte:** max. 31 alphanumerische Zeichen

**Default:** leer

## 2.9.5 Register-Monitor

Mit dieser Aktion können sich SNMP-Agenten bei einem Gerät anmelden, um anschließend SNMP-Traps zu erhalten. Zu dem Kommando werden dazu die IP-Adresse, der Port und die MAC-Adresse des SNMP-Agenten angegeben. Alle drei Werte können durch den Platzhalter * ersetzt werden, in diesem Fall ermittelt das Gerät die Werte aus den vom SNMP-Agenten empfangenen Paketen.

**SNMP-ID:** 2.9.5

**Pfad Telnet:** /Setup/SNMP

**Mögliche Werte:**

- <IP-Adresse|*>:<Port|*> <MAC-Adresse|*> <W>

**Default:** Leer

**Besondere Werte:** <W> am Ende des Kommandos ist für eine Registrierung über eine WAN-Verbindung erforderlich.

Ein LANmonitor muss nicht explizit am Gerät angemeldet werden. Der LANmonitor überträgt bei der Suche nach neuen Geräten automatisch die Anmeldeinformationen an das Gerät.

## 2.9.4 Standort

Standortangabe zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

**SNMP-ID:** 2.9.4

**Pfad Telnet:** /Setup/SNMP

**Mögliche Werte:**

- max. 255 Zeichen

**Default:** Leer

## 2.9.1 Traps-senden

Bei schwerwiegenden Fehlern, zum Beispiel bei einem unberechtigten Zugriff, kann das Gerät automatisch eine Fehlermeldung an einen oder mehrere SNMP-Manager senden. Schalten Sie dazu diese Option ein und geben Sie in der IP-Trap-Tabelle die IP-Adressen der Computer ein, auf denen diese SNMP-Manager installiert sind.

**SNMP-ID:** 2.9.1

**Pfad Telnet:** /Setup/SNMP

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

## 2.9.20 Volle-Host-MIB

Wählen Sie hier aus, ob für das Gerät eine volle Host-MIB genutzt wird.

**SNMP-ID:** 2.9.20

**Pfad Telnet:** /Setup/SNMP/Volle-Host-MIB

**Mögliche Werte**:

- Nein
- Ja

**Default**: Nein

## 2.9.2 IP-Traps

Hier können Sie SNMP-Manager eintragen.

**SNMP-ID:** 2.9.2

**Pfad Telnet:** /Setup/SNMP

### 2.9.2.1 Trap-IP

Geben Sie hier die IP-Adresse des Computers ein, auf dem ein SNMP-Manager installiert ist.

**SNMP-ID:** 2.9.2.1

**Pfad Telnet:** /Setup/SNMP/IP-Traps

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** Leer

### 2.9.2.3 Loopback-Addr.

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

**SNMP-ID:** 2.9.2.3

**Pfad Telnet:** /Setup/SNMP/IP-Traps

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

**Default:** Leer

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, wird die zugehorige IP-Adresse verwendet.

### 2.9.2.4 Version

Gibt die SNMP-Version an, die für die Traps an diesen Empfänger verwendet werden soll.

**SNMP-ID:** 2.9.2.4

**Pfad Telnet:** /Setup/SNMP/IP-Traps

**Mögliche Werte:**

- SNMPv1
- SNMPv2

**Default:** SNMPv2

## 2.9.7 Monitor-Tabelle

Die Monitor-Tabelle zeigt alle am Gerät angemeldeten SNMP-Agenten.

**SNMP-ID:** 2.9.7

**Pfad Telnet:** /Setup/SNMP

### 2.9.7.1 IP-Adresse

IP-Adresse der Gegenstelle, von der ein SNMP-Agent auf das Gerät zugreift.

**SNMP-ID:** 2.9.7.1

**Pfad Telnet:** /Setup/SNMP/Monitor-Tabelle

**Mögliche Werte:**

- Gültige IP-Adresse.

### 2.9.7.2 Port

Port, über den die Gegenstelle mit einem SNMP-Agent auf das Gerät zugreift.

**SNMP-ID:** 2.9.7.2

**Pfad Telnet:** /Setup/SNMP/Monitor-Tabelle

### 2.9.7.3 Timeout

Timeout in Minuten, bis die Gegenstelle aus der Monitor-Tabelle entfernt wird.

**SNMP-ID:** 2.9.7.3

**Pfad Telnet:** /Setup/SNMP/Monitor-Tabelle

### 2.9.7.4 MAC-Adresse

MAC-Adresse der Gegenstelle, von der ein SNMP-Agent auf das Gerät zugreift.

**SNMP-ID:** 2.9.7.4

**Pfad Telnet:** /Setup/SNMP/Monitor-Tabelle

### 2.9.7.5 Gegenstelle

Name der Gegenstelle, von der ein SNMP-Agent auf das Gerät zugreift.

**SNMP-ID:** 2.9.7.5

**Pfad Telnet:** /Setup/SNMP/Monitor-Tabelle

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen.

### 2.9.7.6 Loopback-Addr.

Loopback-Adresse der Gegenstelle, von der ein SNMP-Agent auf das Gerät zugreift.

**SNMP-ID:** 2.9.7.6

**Pfad Telnet:** /Setup/SNMP/Monitor-Tabelle

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

### 2.9.7.7 VLAN-ID

VLAN-ID, über den die Gegenstelle mit einem SNMP-Agent auf das Gerät zugreift.

**SNMP-ID:** 2.9.7.7

**Pfad Telnet:** /Setup/SNMP/Monitor-Tabelle

### 2.9.7.8 LAN-Ifc

LAN-Ifc, über den die Gegenstelle mit einem SNMP-Agent auf das Gerät zugreift.

**SNMP-ID:** 2.9.7.8

**Pfad Telnet:** /Setup/SNMP/Monitor-Tabelle

### 2.9.7.9 Ethernet-Port

Ethernet-Port, über den die Gegenstelle mit einem SNMP-Agent auf das Gerät zugreift.

**SNMP-ID:** 2.9.7.9

**Pfad Telnet:** /Setup/SNMP/Monitor-Tabelle

## 2.10 DHCP

Dieses Menü enthält die Einstellungen für DHCP.

**SNMP-ID:** 2.10

**Pfad Telnet:** /Setup

## 2.10.7 Default-Gueltigkeit-Minuten

Wenn ein Client eine IP-Adresse anfordert, ohne eine Gültigkeitsdauer für diese Adresse zu fordern, wird dieser Adresse als Gültigkeitsdauer der hier eingestellte Wert zugewiesen.

**SNMP-ID:** 2.10.7

**Pfad Telnet:** /Setup/DHCP

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 500

## 2.10.6 Max.-Gueltigkeit-Minuten

Wenn ein Client eine IP-Adresse bei einem DHCP-Server anfordert, kann er eine Gültigkeitsdauer für diese Adresse anfordern. Dieser Wert kontrolliert die maximale Gültigkeitsdauer, die ein Client anfordern darf.

**SNMP-ID:** 2.10.6

**Pfad Telnet:** /Setup/DHCP

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 6000

## 2.10.19 User-Class-Identifier

Der DHCP-Client im Gerät kann in den versendeten DHCP-Requests zusätzliche Angaben einfügen, die eine Erkennung der Requests im Netzwerk erleichtern. Der Vendor-Class-Identifier (DHCP-Option 60) zeigt den Gerätetyp an, z. B. 'LANCOM

L-54ag'. Die Vendor-Class-ID wird immer übertragen. Der User-Class-Identifier (DHCP-Option 77) gibt einen benutzerdefinierten String an. Die User-Class-ID wird nur übertragen, wenn der Benutzer einen Wert konfiguriert hat.

**SNMP-ID:** 2.10.19

**Pfad Telnet:** /Setup/DHCP

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** leer

## 2.10.8 DHCP-Tabelle

Die DHCP-Tabelle gibt eine Übersicht über die in den IP-Netzwerken verwendeten IP-Adressen. Bei der DHCP-Tabelle handelt es sich um eine reine Status-Tabelle, in der keine Parameter konfiguriert werden können.

**SNMP-ID:** 2.10.8

**Pfad Telnet:** /Setup/DHCP

### 2.10.8.1 IP-Adresse

IP-Adresse, die von der Station verwendet wird.

**SNMP-ID:** 2.10.8.1

**Pfad Telnet:** /Setup/DHCP/DHCP-Tabelle

**Mögliche Werte:**

- Gültige IP-Adresse.

### 2.10.8.10 LAN-Ifc

Die LAN-Schnittstelle, auf die sich dieser Eintrag bezieht.

**SNMP-ID:** 2.10.8.10

**Pfad Telnet:** /Setup/DHCP/DHCP-Tabelle/LAN-Ifc

### 2.10.8.2 MAC-Adresse

MAC-Adresse der Station.

**SNMP-ID:** 2.10.8.2

**Pfad Telnet:** /Setup/DHCP/DHCP-Tabelle

### 2.10.8.3 Timeout

Gültigkeitsdauer der Adresszuweisung in Minuten.

**SNMP-ID:** 2.10.8.3

**Pfad Telnet:** /Setup/DHCP/DHCP-Tabelle

### 2.10.8.4 Rechnername

Name der Station, sofern dieser ermittelt werden konnte.

**SNMP-ID:** 2.10.8.4

**Pfad Telnet:** /Setup/DHCP/DHCP-Tabelle

### 2.10.8.5 Typ

Im Feld 'Typ' wird angegeben, wie die Adresse zugewiesen wurde. Das Feld kann die folgenden Werte annehmen:

neu: Der Rechner hat zum ersten Mal angefragt. Der DHCP-Server überprüft die Eindeutigkeit der Adresse, die dem Rechner zugewiesen werden soll.

unbek.: Bei der Überprüfung der Eindeutigkeit wurde festgestellt, dass die Adresse bereits an einen anderen Rechner vergeben wurde. Der DHCP-Server hat leider keine Möglichkeit, weitere Informationen über diesen Rechner zu erhalten.

stat.: Ein Rechner hat dem DHCP-Server mitgeteilt, dass er eine feste IP-Adresse besitzt. Diese Adresse darf nicht mehr für andere Stationen im Netz verwendet werden.

dyn.: Der DHCP-Server hat dem Rechner eine Adresse zugewiesen.

**SNMP-ID:** 2.10.8.5

**Pfad Telnet:** /Setup/DHCP/DHCP-Tabelle

### 2.10.8.7 Ethernet-Port

Physikalisches Interface, über das die Station mit dem Gerät verbunden ist.

**SNMP-ID:** 2.10.8.7

**Pfad Telnet:** /Setup/DHCP/DHCP-Tabelle

### 2.10.8.8 VLAN-ID

Die von dieser Station verwendete VLAN-ID.

**SNMP-ID:** 2.10.8.8

**Pfad Telnet:** /Setup/DHCP/DHCP-Tabelle

### 2.10.8.9 Netzwerkname

Name des IP-Netzwerks, in dem sich die Station befindet.

**SNMP-ID:** 2.10.8.9

**Pfad Telnet:** /Setup/DHCP/DHCP-Tabelle

## 2.10.9 Hosts

Über das Bootstrap-Protokoll (BOOTP) können einer Station beim Starten eine IP-Adresse und weitere Parameter übermittelt werden. Dazu wird die MAC-Adresse der Station in die Host-Tabelle eingetragen.

**SNMP-ID:** 2.10.9

**Pfad Telnet:** /Setup/DHCP

### 2.10.9.1 MAC-Adresse

Geben Sie hier die MAC-Adresse der Station ein, der eine IP-Adresse zugewiesen werden soll.

**SNMP-ID:** 2.10.9.1

**Pfad Telnet:** /Setup/DHCP/Hosts

**Mögliche Werte:**

- Gültige MAC-Adresse.

**Default:** 000000000000

### 2.10.9.2 IP-Adresse

Geben Sie hier die IP-Adresse der Station ein, die der Station zugewiesen werden soll.

**SNMP-ID:** 2.10.9.2

**Pfad Telnet:** /Setup/DHCP/Hosts

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.10.9.3 Rechnername

Geben Sie hier einen Namen ein, mit dem die Station identifiziert werden soll. Wenn eine Station ihren Namen nicht übermittelt, verwendet das Gerät den hier eingetragenen Namen.

**SNMP-ID:** 2.10.9.3

**Pfad Telnet:** /Setup/DHCP/Hosts

**Mögliche Werte:**

- max. 30 Zeichen

**Default:** Leer

### 2.10.9.4 Image-Alias

Wenn die Station das BOOTP-Protokoll verwendet, dann können Sie ein Boot-Image auswählen, über das die Station ihr Betriebssystem laden soll.

**SNMP-ID:** 2.10.9.4

**Pfad Telnet:** /Setup/DHCP/Hosts

**Mögliche Werte:**

- max. 16 Zeichen

**Default:** Leer

Den Server, der das Boot-Image zur Verfügung stellt, sowie den Namen der Datei auf dem Server müssen Sie in der Boot-Image-Tabelle eingeben.

### 2.10.9.5 Netzwerkname

Hier wird der Name eines konfigurierten IP-Netzwerks eingetragen. Nur wenn sich die anfragende Station in diesem IP-Netzwerk befindet, wird der Station die für die MAC-Adresse definierte IP-Adresse zugewiesen.

**SNMP-ID:** 2.10.9.5

**Pfad Telnet:** /Setup/DHCP/Hosts

**Mögliche Werte:**

- max. 16 Zeichen

**Default:** Leer

**Besondere Werte:** Leer: Passt die in diesem Eintrag definierte IP-Adresse zu dem Adresskreis des IP-Netzwerks, in dem sich die anfragende Station befindet, dann wird die IP-Adresse zugewiesen.

Befindet sich die anfragende Station in einem IP-Netzwerk, zu dem es keinen passenden Eintrag in der HostTabelle gibt, so wird der Station dynamisch eine IP-Adresse aus dem IP-Adress-Pool des jeweiligen IP-Netzwerks zugewiesen.

## 2.10.10 Alias-Liste

In der Alias-Liste werden die Bezeichnungen für die Boot-Images definiert, über welche die Images in der Host-Tabelle referenziert werden können.

**SNMP-ID:** 2.10.10

**Pfad Telnet:** /Setup/DHCP

### 2.10.10.1 Image-Alias

Geben Sie eine beliebige Bezeichnung für dieses Boot-Image ein. Diese Bezeichnung wird verwendet, wenn Sie in der Stations-Liste ein Boot-Image einer bestimmten Station zuordnen.

**SNMP-ID:** 2.10.10.1

**Pfad Telnet:** /Setup/DHCP/Alias-Liste

**Mögliche Werte:**

- max. 16 Zeichen

**Default:** leer

### 2.10.10.2 Image-File

Geben Sie den Namen der Datei auf dem Server an, die das Boot-Image enthält.

**SNMP-ID:** 2.10.10.2

**Pfad Telnet:** /Setup/DHCP/Alias-Liste

**Mögliche Werte:**

- max. 60 Zeichen

**Default:** leer

### 2.10.10.3 Image-Server

Geben Sie die IP-Adresse des Servers ein, der das Boot-Image zur Verfügung stellt.

**SNMP-ID:** 2.10.10.3

**Pfad Telnet:** /Setup/DHCP/Alias-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

## 2.10.18 Ports

In der Port-Tabelle wird der DHCP-Server für die jeweiligen logischen Interfaces des Geräts freigegeben.

**SNMP-ID:** 2.10.18

**Pfad Telnet:** /Setup/DHCP

### 2.10.18.2 Port

Auswahl des logischen Interfaces, für das der DHCP-Server aktiviert bzw. deaktiviert werden soll.

**SNMP-ID:** 2.10.18.2

**Pfad Telnet:** /Setup/DHCP/Ports

**Mögliche Werte:**

- Auswahl aus der Liste der logischen Interfaces in diesem Gerät, z. B. LAN-1, WLAN-1, P2P-1-1 etc.

### 2.10.18.3 DHCP-Freigeben

Aktiviert bzw. deaktiviert den DHCP-Server für das gewählte logische Interface.

**SNMP-ID:** 2.10.18.3

**Pfad Telnet:** /Setup/DHCP/Ports

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

## 2.10.20 Netzliste

Wenn mehrere DHCP-Server in einem Netz aktiv sind, dann "verteilen" sich die Stationen im Netz gleichmäßig auf diese Server. Der DNS-Server der Geräte löst allerdings nur die Namen der Stationen richtig auf, denen der eigene DHCP-Server die Adressinformationen zugewiesen hat. Damit der DNS-Server auch die Namen anderer DHCP-Server auflösen kann, können die DHCP-Server im Cluster betrieben werden. In dieser Betriebsart verfolgt der DHCP-Server alle im Netz laufenden DHCP-Verhandlungen mit und trägt auch Stationen in seine Tabelle ein, die sich nicht bei ihm, sondern bei anderen DHCP-Servern im Cluster angemeldet haben.

Der Betrieb eines DHCP-Servers im Cluster kann für jedes einzelne ARF-Netz in den zugehörigen DHCP-Einstellungen aktiviert bzw. deaktiviert werden.

**SNMP-ID:** 2.10.20

**Pfad Telnet:** /Setup/DHCP/Netzliste

### 2.10.20.1 Netzwerkname

Name des Netzwerks, für das die Einstellungen des DCHP-Servers gelten sollen.

**SNMP-ID:** 2.10.20.1

**Pfad Telnet:** /Setup/DHCP/Netzliste

**Mögliche Werte:**

- max. 16 Zeichen

**Default:** leer

### 2.10.20.10 NBNS-Backup

IP-Adresse des Backup-NBNS-Nameservers. Diesen NBNS-Nameserver verwendet die Arbeitsstation, wenn der erste NBNS-Nameserver ausfällt.

**SNMP-ID:** 2.10.20.10

**Pfad Telnet:** /Setup/DHCP/Netzliste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.10.20.11 Aktiv

Betriebsart des DHCP-Servers für dieses Netzwerk. Je nach Betriebsart kann sich der DHCP-Server selbst aktivieren bzw. deaktivieren. Ob der DHCP-Server aktiv ist, kann den DHCP-Statistiken entnommen werden.

**SNMP-ID:** 2.10.20.11

**Pfad Telnet:** /Setup/DHCP/Netzliste

**Mögliche Werte:**

- Nein: Der DHCP-Server ist dauerhaft abgeschaltet.
- Ja: Der DHCP-Server ist dauerhaft eingeschaltet. Bei der Eingabe dieses Wertes wird die Konfiguration des Servers (Gültigkeit des Adress-Pools) überprüft. Bei einer korrekten Konfiguration bietet das Gerät sich als DHCP-Server im Netz an. Bei einer fehlerhaften Konfiguration (z. B. ungültige Pool-Grenzen) wird der DHCP-Server für das Netzwerk deaktiviert. Verwenden Sie diese Einstellung nur dann, wenn sichergestellt ist, das kein anderer DHCP-Server im LAN aktiv ist.
- Automatisch: In diesem Zustand sucht das Gerät regelmäßig im lokalen Netz nach anderen DHCP-Servern. Diese Suche ist erkennbar durch ein kurzes Aufleuchten der LAN-Rx/Tx-LED. Wird mindestens ein anderer DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server aus. Ist für den LANCOM noch keine IP-Adresse konfiguriert, dann wechselt er in den DHCP-Client-Modus und bezieht eine IP-Adresse vom DHCP-Server. Damit wird u. a. verhindert, dass ein unkonfiguriertes Gerät nach dem Einschalten im Netz unerwünscht Adressen vergibt. Werden keine anderen DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server ein. Wird zu einem späteren Zeitpunkt ein anderer DHCP-Server im LAN eingeschaltet, wird der DHCP-Server im LANCOM deaktiviert.
- 'Anfragen Weiterleiten': Der DHCP-Server ist eingeschaltet, das Gerät nimmt die Anfragen der DHCP-Clients im lokalen Netz entgegen. Das Gerät beantwortet diese Anfragen jedoch nicht selbst, sondern leitet sie an einen zentralen DHCP-Server in einem anderen Netzwerkabschnitt weiter (Betriebsart DHCP-Relay-Agent).
- 'Client-Modus': Der DHCP-Server ist ausgeschaltet, das Gerät verhält sich als DHCP-Client und bezieht seine Adress-Informationen von einem anderen DHCP-Server im LAN. Verwenden Sie diese Einstellung nur dann, wenn sichergestellt ist, das ein anderer DHCP-Server im LAN aktiv ist und die Zuweisung der IP-Adress-Informationen übernimmt.

**Default:** Nein

Verwenden Sie die Einstellung “Ja” nur dann, wenn sichergestellt ist, dass kein anderer DHCP-Server im LAN aktiv ist. Verwenden Sie die Einstellung “Client-Modus” nur dann, wenn sichergestellt ist, das ein anderer DHCP-Server im LAN aktiv ist und die Zuweisung der IP-Adress-Informationen übernimmt.

### 2.10.20.12 Broadcast-Bit

Wählen Sie hier, ob das von den Clients gemeldete Broadcast-Bit ausgewertet wird oder nicht. Wenn das Bit nicht ausgewertet wird, werden alle DHCP-Nachrichten als Broadcast versendet.

**SNMP-ID:** 2.10.20.12

**Pfad Telnet:** /Setup/DHCP/Netzliste

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

### 2.10.20.13 Master-Server

Hier wird die IP-Adresse des übergeordneten DHCP-Servers eingetragen, an den DHCP-Anfragen weitergeleitet werden, wenn für das Netzwerk die Betriebsart 'Anfragen Weiterleiten' gewählt wurde.

**SNMP-ID:** 2.10.20.13

**Pfad Telnet:** /Setup/DHCP/Netzliste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.10.20.14 Cache

Mit dieser Option können die Antworten des übergeordneten DHCP-Servers im LANCOM Wireless gespeichert werden. Spätere Anfragen können dann vom LANCOM Wireless selbst beantwortet werden. Diese Option ist nützlich, wenn der übergeordnete DHCP-Server nur über eine kostenpflichtige Verbindung erreicht werden kann.

**SNMP-ID:** 2.10.20.14

**Pfad Telnet:** /Setup/DHCP/Netzliste

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

### 2.10.20.15 Anpassung

Mit dieser Option können die Antworten des übergeordneten DHCP-Servers an das lokale Netzwerk angepasst werden. Bei aktiviert Anpassung ersetzt der LANCOM Wireless in den Antworten des übergeordneten DHCP-Servers folgende Einträge durch seine eigene Adresse (bzw. lokal konfigurierte Adressen):

- Gateway

- Netzmaske

- Broadcast-Adresse

- DNS-Server

- NBNS-Server

- Server-ID

Diese Option ist sinnvoll, wenn der übergeordnete DHCP-Server keine getrennte Konfiguration für DHCP-Clients in einem anderen Netzwerk zulässt.

**SNMP-ID:** 2.10.20.15

**Pfad Telnet:** /Setup/DHCP/Netzliste

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

### 2.10.20.16 Cluster

Wählen Sie hier aus, ob der DHCP-Server für dieses ARF-Netz im Cluster oder separat betrieben werden soll.

**SNMP-ID:** 2.10.20.16

**Pfad Telnet:** /Setup/DHCP/Netzliste

**Mögliche Werte:**

- Ja: Wenn der Cluster-Betrieb aktiviert ist, verfolgt der DHCP-Server alle im Netz laufenden DHCP-Verhandlungen mit und trägt auch Stationen in seine Tabelle ein, die sich nicht bei ihm, sondern bei anderen DHCP-Servern in Cluster angemeldet haben. Diese Stationen werden in der DHCP-Tabelle mit dem Flag "cache" gekennzeichnet.
- Nein: Der DHCP-Server verwaltet nur Informationen über die bei ihm selbst angeschlossenen Stationen.

**Default:**

Nein

Wenn die Lease-Time der über DHCP zugewiesenen Informationen abläuft, schickt eine Station eine Anfrage zur Erneuerung an den DHCP-Server, von dem sie die Informationen erhalten hat (Renew-Request). Falls der ursprüngliche DHCP-Server auf diesen Request nicht antwortet, versendet die Station eine Anfrage nach einer neuen DHCP-Anbindung (Rebinding Request) als Broadcast an alle erreichbaren DHCP-Server. Renew-Requests werden von den DHCP-Servern im Cluster ignoriert – so wird ein Rebinding erzwungen, damit alle im Cluster vorhandenen DHCP-Server über den Broadcast ihren Eintrag für die Station erneuern können. Auf den Rebind-Request antwortet zunächst nur der DHCP-Server, bei dem die Station ursprünglich registriert war. Wird der Rebind-Request von einer Station wiederholt, dann gehen alle DHCP-Server im Cluster davon aus, das der ursprünglich zuständige DHCP-Server im Cluster nicht mehr aktiv ist und beantworten die Anfrage. Diese Antwort enthält zwar die gleiche IP-Adresse für die Station, kann aber unterschiedliche Gateway- und DNS-Serveradressen enthalten. Die Station sucht sich nun aus den Antworten einen neuen DHCP-Server aus, an den sie von nun an gebunden ist und übernimmt von ihm Gateway und DNS-Server (sowie alle anderen zugewiesenen Parameter).

### 2.10.20.17 2ter-Master-Server

Hier wird die IP-Adresse eines alternativen DHCP-Servers eingetragen, an den DHCP-Anfragen weitergeleitet werden, wenn für das Netzwerk die Betriebsart 'Anfragen Weiterleiten' gewählt wurde.

**SNMP-ID:** 2.10.20.17

**Pfad Telnet:** /Setup/DHCP/Netzliste/2ter-Master-Server

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.10.20.18 3ter-Master-Server

Hier wird die IP-Adresse eines alternativen DHCP-Servers eingetragen, an den DHCP-Anfragen weitergeleitet werden, wenn für das Netzwerk die Betriebsart 'Anfragen Weiterleiten' gewählt wurde.

**SNMP-ID:** 2.10.20.18

**Pfad Telnet:** /Setup/DHCP/Netzliste/2ter-Master-Server

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.10.20.19 4ter-Master-Server

Hier wird die IP-Adresse eines alternativen DHCP-Servers eingetragen, an den DHCP-Anfragen weitergeleitet werden, wenn für das Netzwerk die Betriebsart 'Anfragen Weiterleiten' gewählt wurde.

**SNMP-ID:** 2.10.20.19

**Pfad Telnet:** /Setup/DHCP/Netzliste/2ter-Master-Server

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.10.20.2 Start-Adress-Pool

Erste IP-Adresse des Adressbereiches, der den Clients zur Verfügung steht. Wenn hier keine Adresse eingetragen ist, dann verwendet der DHCP-Server die erste freie IP-Adresse aus diesem Netzwerk (wird bestimmt aus Netzadresse und Netzmaske).

**SNMP-ID:** 2.10.20.2

**Pfad Telnet:** /Setup/DHCP/Netzliste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.10.20.3 Ende-Adress-Pool

Letzte IP-Adresse des Adressbereiches, der den Clients zur Verfügung steht. Wenn hier keine Adresse eingetragen ist, dann verwendet der DHCP-Server die letzte freie IP-Adresse aus diesem Netzwerk (wird bestimmt aus Netzadresse und Netzmaske).

**SNMP-ID:** 2.10.20.3

**Pfad Telnet:** /Setup/DHCP/Netzliste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.10.20.4 Netz-Maske

Zugehörige Netzmaske für den Adressbereich, der den Clients zur Verfügung steht. Wenn hier keine Adresse eingetragen ist, dann verwendet der DHCP-Server die Netzmaske aus dem zugehörigen Netzwerk.

**SNMP-ID:** 2.10.20.4

**Pfad Telnet:** /Setup/DHCP/Netzliste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.10.20.5 Broadcast-Adresse

In der Regel wird im lokalen Netz für Broadcast-Pakete eine Adresse verwendet, die sich aus den gültigen IP-Adressen und der Netzmaske ergibt. Nur in Sonderfällen (z. B. bei Verwendung von Sub-Netzen für einen Teil der Arbeitsplatzrechner) kann es nötig sein, eine andere Broadcast-Adresse zu verwenden. In diesem Fall wird die zu verwendende Broadcast-Adresse im DHCP-Modul eingetragen.

**SNMP-ID:** 2.10.20.5

**Pfad Telnet:** /Setup/DHCP/Netzliste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0 (Broadcast-Adresse wird automatisch ermittelt)

Wir empfehlen Änderungen der voreingestellten Broadcast-Adresse nur für erfahrene Netzwerk-Spezialisten. Fehlkonfigurationen können zu unerwünschten, gebührenpflichtigen Verbindungen führen!

### 2.10.20.6 Gateway-Adresse

Der DHCP-Server weist dem anfragenden Rechner standardmäßig seine eigene IP-Adresse als Gateway-Adresse zu. Falls erforderlich, kann durch den Eintrag einer entsprechenden IP-Adresse auch ein anderes Gateway übertragen werden.

**SNMP-ID:** 2.10.20.6

**Pfad Telnet:** /Setup/DHCP/Netzliste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.10.20.7 DNS-Default

IP-Adresse des DNS-Nameservers, den die anfragenden Arbeitsstation verwenden soll.

**SNMP-ID:** 2.10.20.7

**Pfad Telnet:** /Setup/DHCP/Netzliste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

Wenn weder ein Default- noch ein Backup-DNS-Server eingetragen wurde, weist das Gerät der anfragenden Arbeitsstation seine eigene IP-Adresse im jeweiligen ARF-Netz als (primären) DNS-Server zu.

### 2.10.20.8 DNS-Backup

IP-Adresse des Backup-DNS-Nameservers. Diesen DNS-Nameserver verwendet die Arbeitsstation, wenn der erste DNS-Nameserver ausfällt.

**SNMP-ID:** 2.10.20.8

**Pfad Telnet:** /Setup/DHCP/Netzliste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

Wenn weder ein Default- noch ein Backup-DNS-Server eingetragen wurde, weist das Gerät der anfragenden Arbeitsstation seine eigene IP-Adresse im jeweiligen ARF-Netz als (primären) DNS-Server zu.

### 2.10.20.9 NBNS-Default

IP-Adresse des NBNS-Nameservers, den die anfragende Arbeitsstation verwenden soll.

**SNMP-ID:** 2.10.20.9

**Pfad Telnet:** /Setup/DHCP/Netzliste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

## 2.10.21 Zusaetzliche-Optionen

Mit den DHCP-Optionen können zusätzliche Konfigurationsparameter an die Stationen übertragen werden. Der Vendor-Class-Identifier (DHCP-Option 60) zeigt so z. B. den Gerätetyp an. In dieser Tabelle werden zusätzliche Optionen für den DHCP-Betrieb definiert.

**SNMP-ID:** 2.10.21

**Pfad Telnet:** /Setup/DHCP

### 2.10.21.1 Options-Nummer

Nummer der Option, die an die DHCP-Clients übermittelt werden soll. Die Options-Nummer beschreibt die übermittelte Information, z. B. "17" (Root Path) für den Pfad zu einem Boot-Image für einen PC ohne eigene Festplatte, der über BOOTP sein Betriebssystem bezieht.

**SNMP-ID:** 2.10.21.1

**Pfad Telnet:** /Setup/DHCP/Zusaetzliche-Optionen

**Mögliche Werte:** max. 3 Zeichen

**Default:** Leer

Eine Liste aller DHCP-Optionen finden Sie im RFC 2132 – DHCP Options and BOOTP Vendor Extensions der Internet Engineering Task Force (IETF).

### 2.10.21.2 Netzwerkname

Name des IP-Netzwerks, in dem diese DHCP-Option verwendet werden soll.

**SNMP-ID:** 2.10.21.2

**Pfad Telnet:** /Setup/DHCP/Zusaetzliche-Optionen

**Mögliche Werte:**

- Auswahl aus der Liste der definierten IP-Netzwerke.

**Default:** Leer

**Besondere Werte:** Leer: Wird kein Netzwekname angegeben, so wird die in diesem Eintrag definierte DHCP-Option in allen IP--Netzwerken verwendet.

### 2.10.21.3 Options-Wert

In diesem Feld wird der Inhalt der DHCP-Option definiert. IP-Adressen gibt man normalerweise in der üblichen IPv4-Notation an, z. B. "123.123.123.100". Integer-Typen geben Sie in normalen Dezimalzahlen an, String-Typen als Simple Text. Verschiedene Werte in einem Textfeld werden mit Kommas getrennt, z. B. "123.123.123.100, 123.123.123.200".

**SNMP-ID:** 2.10.21.3

**Pfad Telnet:** /Setup/DHCP/Zusaetzliche-Optionen

**Mögliche Werte:**

- max. 128 Zeichen

Die mögliche Länge des Optionswertes hängt von der gewählten Optionsnummer ab. Der RFC 2132 listet für jede Option ein zulässige Länge auf.

### 2.10.21.4 Typ

Typ des Eintrags.

**SNMP-ID:** 2.10.21.4

**Pfad Telnet:** /Setup/DHCP/Zusaetzliche-Optionen

Dieser Wert ist abhängig von der jeweiligen Option. Für die Option "35" wird hier im RFC 2132 z. B. der ARP Cache Timeout so definiert (in englischer Sprache):

**ARP Cache Timeout Option**

This option specifies the timeout in seconds for ARP cache entries.

The time is specified as a 32-bit unsigned integer.

The code for this option is 35, and its length is 4.

| Code | Len | Time | | | |
|---|---|---|---|---|---|
| 35 | 4 | t1 | t2 | t3 | t4 |

Aus dieser Beschreibung können Sie ablesen, dass für diese Option der Typ "32-Bit-Integer" verwendet wird.

**Mögliche Werte:**

- String
- Integer8
- Integer16
- Integer32
- IP-Adresse

**Default:** String

Den Typ der Option entnehmen Sie bitte dem entsprechenden RFC bzw. bei herstellerspezifischen DCHP-Optionen der jeweiligen Herstellerdokumentation.

## 2.11 Config

Enthält die allgemeinen Konfigurationseinstellungen.

**SNMP-ID:** 2.11

**Pfad Telnet:** /Setup

## 2.11.9 Admin.-EAZ-MSN

Wenn der LANCAPI-Server auch ankommende Rufe entgegen nehmen soll, so geben Sie im Feld 'Rufnummern (MSN/EAZ)' alle eigenen ISDN-Rufnummern an, auf denen die LANCAPI Anrufe entgegennehmen soll. Mehrere Rufnummern werden voneinander durch Semikola getrennt. Wenn Sie hier keine Rufnummer eingeben, nimmt die LANCAPI Anrufe aller eigenen ISDN-Rufnummern entgegen.

**SNMP-ID:** 2.11.9

**Pfad Telnet:** /Setup/Config

**Mögliche Werte:**

- max. 31 Zeichen

**Default:** leer

## 2.11.41 Admin-Geschlecht

Geben Sie hier das Geschlecht des Admins an.

**SNMP-ID:** 2.11.41

**Pfad Telnet:** /Setup/Config/Admin-Geschlecht

**Mögliche Werte:**

- unbekannt
- maennlich
- weiblich

**Default:** unbekannt

## 2.11.42 Assert-Action

Dieser Parameter beeinflusst das Verhalten des Geräts bei der Prüfung des Firmware-Codes.

**SNMP-ID:** 2.11.42

**Pfad Telnet:** /Setup/Config/Assert-Action

**Mögliche Werte:**

- log_only
- reboot

**Default:** log_only

Die Einstellungen für diesen Parameter werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

## 2.11.16 Bildschirmhoehe

Gibt die maximale Höhe des Bildschirms in Zeilen an. Wenn Sie hier eine 0 eingeben, dann bestimmt das Gerät beim Einloggen die optimale Bildschirmhöhe automatisch.

**SNMP-ID:** 2.11.16

**Pfad Telnet:** /Setup/Config

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 24

**Besondere Werte:** 0

## 2.11.5 Config-Aging-Minutes

Hier können Sie angeben, nach wieviel Minuten der Inaktivität eine Konfigurations-Verbindung über TCP (z. B. Telnet-Verbindung) automatisch beendet wird.

**SNMP-ID:** 2.11.5

**Pfad Telnet:** /Setup/Config

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 15

## 2.11.60 CPU-Last-Intervall

Hier können Sie die den Zeitraum zur Mittelung der CPU-Lastanzeige auswählen. Die Anzeige der CPU-Last im LANmonitor, im Status-Bereich, im Display (sofern vorhanden) sowie in evtl. genutzten SNMP-Tools basiert auf dem hier eingestellten Mittelungszeitraum. Im Status-Bereich unter WEBconfig oder CLI werden zusätzlich die CPU-Lastwerte für alle vier möglichen Mittelungszeiträume angezeigt.

Mittlere Werte für den CPU-Load sind verfügbar über die folgenden Zeitintervalle:

**SNMP-ID:** 2.11.60

**Pfad Telnet:** /Setup/Config

**Mögliche Werte:**

T1s (arithmetisches Mittel)

T5s (arithmetisches Mittel)

T60s (gleitender Mittelwert)

T300s (gleitender Mittelwert)

**Default:** T60s

## 2.11.40 Crash-Meldung

Legen Sie hier die Meldung fest, die beim Absturz des Geräts im Bootlog erscheint.

**SNMP-ID:** 2.11.40

**Pfad Telnet:** /Setup/Config/Crash-Meldung

**Mögliche Werte:**

- maximal 32 alphanumerische Zeichen

**Default:** LCOS-Watchdog

## 2.11.10 Display-Kontrast

Stellen Sie hier den Kontrast für das Display des Geräts ein.

**SNMP-ID:** 2.11.10

**Pfad Telnet:** /Setup/Config/Display-Kontrast

**Mögliche Werte:**

- K1 (geringer Kontrast) bis K8 (hoher Kontrast).

**Default:** K4

## 2.11.18 LED-Test

Aktiviert den Testmodus für die LEDs, bei der die Funktion der LEDs in verschiedenen Farben getestet wird.

**SNMP-ID:** 2.11.18

**Pfad Telnet:** /Setup/Config

**Mögliche Werte:**

- Aus: Schaltet alle LEDs aus
- Rot: Schaltet alle LEDs ein, die rot leuchten können
- Grün: Schaltet alle LEDs ein, die grün leuchten können
- Orange: Schaltet alle LEDs ein, die orange leuchten können
- Kein_Test: Normaler Betriebszustand der LEDs

**Default:** Kein_Test

## 2.11.39 Lizenzablauf-Email

Die Nutzung einer Lizenz kann auf einen bestimmten Zeitraum begrenzt sein. Sie werden 30 Tage, eine Woche und einen Tag vor Ablauf der Lizenz mit einer Nachricht an die hier eingestellte E-Mail-Adresse an die auslaufende Lizenz erinnert.

**Pfad Telnet:** /Setup/Config/Lizenzablauf-Email

**Mögliche Werte:**

- Gültige E-Mail-Adresse

**Default:** leer

## 2.11.7 Login-Fehler

Um die Konfiguration Ihres Gerätes vor unberechtigtem Zugriff zu schützen, kann sich das Gerät nach mehreren fehlerhaften Anmelde-Versuchen automatisch sperren. Geben Sie hier ein, nach wieviel Fehlversuchen die Sperre aktiviert werden soll.

**SNMP-ID:** 2.11.7

**Pfad Telnet:** /Setup/Config

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 10

## 2.11.4 max. Verbindungen

max. Anzahl von Konfigurationsverbindungen, die gleichzeitig zu diesem Gerät bestehen dürfen.

**SNMP-ID:** 2.11.4

**Pfad Telnet:** /Setup/Config

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

**Besondere Werte:** 0 schaltet die Begrenzung aus.

## 2.11.33 Outband-Aging-Minutes

Hier können Sie angeben, nach wieviel Minuten der Inaktivität eine Konfigurations-Verbindung über eine Serielle-Verbindung (z. B. Hyper Terminal) automatisch beendet wird.

**SNMP-ID:** 2.11.33

**Pfad Telnet:** /Setup/Config

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 1

## 2.11.3 Pass.Zwang-fuer-SNMP-Lesezugriff

Wenn diese Option eingeschaltet ist und noch kein Passwort vergeben ist, werden Sie immer wenn Sie sich auf das Gerät einloggen aufgefordert ein Passwort zu setzen.

**SNMP-ID:** 2.11.3

**Pfad Telnet:** /Setup/Config

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

## 2.11.17 Prompt

Mit diesem Wert definieren Sie den Prompt (die Eingabeaufforderung) an der Kommandozeile.

**SNMP-ID:** 2.11.17

**Pfad Telnet:** /Setup/Config

**Mögliche Werte:**

- max. 31 Zeichen mit den folgenden Variablen:
- %f: Gibt ein [Test] aus, wenn Sie an der Kommandozeile zuvor den Befehl 'flash no' eingegeben haben. Mit dem Befehl 'flash no' aktivieren Sie den Testmodus für die folgenden Konfigurationsänderungen. Bei aktiviertem Testmodus speichert das Gerät die Änderungen an der Konfiguration nur im RAM. Da das Gerät den RAM bei einem Neustart (Boot) löscht, gehen die Konfigurationsänderungen im Testmodus beim Booten verloren. Die Anzeige [Test] warnt den Administrator vor diesem möglichen Verlust der Konfigurationsänderungen.

- %u: Benutzername
- %n: Gerätename
- %p: aktueller Pfad
- %t: aktuelle Uhrzeit
- %o: aktuelle Betriebszeit

**Default:** leer

## 2.11.32 Reset-Knopf

Der Reset-Taster hat mit Booten (Neustart) und Reset (Rücksetzen auf Werkseinstellung) grundsätzlich zwei verschiedene Funktionen, die durch unterschiedlich lange Betätigungszeiten des Tasters ausgelöst werden.

Manche Geräte können jedoch nicht unter Verschluss aufgestellt werden. Hier besteht die Gefahr, dass die Konfiguration versehentlich gelöscht wird, wenn ein Mitarbeiter den Reset-Taster zu lange gedrückt hält. Mit einer entsprechenden Einstellung kann das Verhalten des Reset-Tasters gesteuert werden.

**SNMP-ID:** 2.11.32

**Pfad Telnet:** /Setup/Config

**Mögliche Werte:**

- Ignorieren: Der Taster wird ignoriert.
- Nur-Booten: Beim Druck auf den Taster wird nur ein Neustart ausgelöst, unabhängig von der gedrückten Dauer.
- Reset-oder-Booten (Standardeinstellung): In dieser Einstellung hat der Reset-Taster verschiedene Funktionen, die durch unterschiedlich lange Betätigungszeiten des Tasters ausgelöst werden:
  - Weniger als 5 Sekunden: Booten (Neustart), dabei wird die benutzerdefinierte Konfiguration aus dem Konfigurationsspeicher geladen. Wenn die benutzerdefinierte Konfiguration leer ist, werden die kundenspezifischen Standardeinstellungen (erster Speicherplatz) geladen. Das Laden der kundenspezifischen Standardeinstellungen wird angezeigt, indem alle LEDs des Geräts einmal kurzzeitig rot aufleuchten. Wenn auch der erste Speicherplatz leer ist, werden die LANCOM Werkseinstellungen geladen.
  - Mehr als 5 Sekunden bis zum ersten Aufleuchten aller LEDs am Gerät: Konfigurations-Reset (Löschen des Konfigurationsspeichers) und anschließender Neustart. Damit werden die kundenspezifischen Standardeinstellungen (erster Speicherplatz) geladen. Das Laden der kundenspezifischen Standardeinstellungen wird angezeigt, indem alle LEDs des Geräts einmal kurzzeitig rot aufleuchten. Wenn der erste Speicherplatz leer ist, werden die LANCOM Werkseinstellungen geladen.
  - Mehr als 15 Sekunden bis zum zweiten Aufleuchten aller LEDs am Gerät: Aktivieren der Rollout-Konfiguration und Löschen der benutzerdefinierten Konfiguration. Nach dem Neustart wird die Rollout-Konfiguration (zweiter Speicherplatz) geladen. Das Laden der Rollout-Konfiguration wird angezeigt, indem alle LEDs des Geräts zweimal kurzzeitig rot aufleuchten. Wenn der zweite Speicherplatz leer ist, werden die LANCOM Werkseinstellungen geladen.

Weitere Informationen zu den verschiedenen Boot-Konfigurationen finden Sie im Referenzhandbuch.

**Default:** reset-oder-booten

Ein LANCOM Access Point befindet sich nach dem Reset wieder im „Managed-Modus“, in dem kein direkter Zugriff über die WLAN-Schnittstelle zur Konfiguration möglich ist!

Das Gerät startet nach dem Reset neu im unkonfigurierten Zustand, alle Einstellungen gehen dabei verloren. Sichern Sie daher vor dem Reset nach Möglichkeit die aktuelle Konfiguration des Geräts!

Mit der Einstellung 'Ignorieren' oder 'Nur-Booten' wird das Rücksetzen der Konfiguration auf den Auslieferungszustand sowie das Laden der Rollout-Konfiguration durch einen Reset unmöglich gemacht. Falls für ein Gerät in diesem Zustand das Konfigurationskennwort nicht mehr vorliegt, gibt es keine Möglichkeit mehr,

auf das Gerät zuzugreifen! In diesem Fall kann über die serielle Konfigurationsschnittstelle eine neue Firmware in das Gerät geladen werden – dabei wird das Gerät in den Auslieferungszustand zurückgesetzt, und die bisherige Konfiguration wird gelöscht. Hinweise zum Firmware-Upload über die serielle Konfigurationsschnittstelle finden Sie im LCOS-Referenzhandbuch.

## 2.11.8 Sperr-Minuten

Um die Konfiguration Ihres Gerätes vor unberechtigtem Zugriff zu schützen, kann sich das Gerät nach mehreren fehlerhaften Anmelde-Versuchen selber sperren. Geben Sie hier den Zeitraum ein, für den die Sperre aktiv bleiben soll. Erst nach Ablauf dieses Zeitraums kann wieder auf das Gerät zugegriffen werden.

**SNMP-ID:** 2.11.8

**Pfad Telnet:** /Setup/Config

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 45

**Besondere Werte:** 0 schaltet die Sperre aus.

## 2.11.6 Sprache

Der Terminalmodus steht in den Sprachen Deutsch und Englisch zur Verfügung. Er wird werkseitig auf Englisch als Konsolensprache eingestellt.

**SNMP-ID:** 2.11.6

**Pfad Telnet:** /Setup/Config

**Mögliche Werte:**

- Deutsch
- Englisch

**Default:** Englisch

Bitte beachten Sie, dass die Sprache der eingetragenen Befehle zur eingestellten Konsolensprache passt, da ansonsten die Kommandos der Zeitautomatik nicht beachtet werden.

## 2.11.25 SSH-Port

Dieser Port wird für Konfigurationsverbindungen über SSH verwendet.

**SNMP-ID:** 2.11.25

**Pfad Telnet:** /Setup/Config

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 22

## 2.11.23 Telnet-Port

Dieser Port wird für unverschlüsselte Konfigurationsverbindungen über Telnet verwendet.

**SNMP-ID:** 2.11.23

**Pfad Telnet:** /Setup/Config

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 23

## 2.11.24 Telnet-SSL-Port

Dieser Port wird für verschlüsselte Konfigurationsverbindungen über Telnet verwendet.

**SNMP-ID:** 2.11.24

**Pfad Telnet:** /Setup/Config

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 992

## 2.11.13 TFTP-Client

Die Nutzung der Standardwerte für die Geräte-Konfiguration, die Firmware und/oder ein Skript bietet sich an, wenn die aktuellen Konfigurationen, Firmware-Versionen und Skripte immer unter dem gleichen Namen an der gleichen Stelle gespeichert werden. In diesem Fall können mit den einfachen Befehlen LoadConfig, LoadFirmware und LoadScript die jeweils gültige Dateien geladen werden.

**SNMP-ID:** 2.11.13

**Pfad Telnet:** /Setup/Config

### 2.11.13.5 Bytes-pro-Hashmark

Anzahl der Bytes, die per Hashmark verwendet werden.

**SNMP-ID:** 2.11.13.5

**Pfad Telnet:** /Setup/Config/TFTP-Client

**Mögliche Werte:**

- max. 6 Ziffern

**Default:** 8192

### 2.11.13.1 Config-Addresse

Standardpfad für Konfigurationsdateien, wenn der Parameter -f bei den Befehlen LoadConfig nicht angegeben wird.

**SNMP-ID:** 2.11.13.1

**Pfad Telnet:** /Setup/Config/TFTP-Client

**Mögliche Werte:**

- Pfadangabe in der Schreibweise //Server/Verzeichnis/Dateiname

**Default:** leer

### 2.11.13.2 Config-Dateiname

Standard-Konfigurationsdatei, wenn der Parameter -f bei den Befehlen LoadConfig nicht angegeben wird.

**SNMP-ID:** 2.11.13.2

**Pfad Telnet:** /Setup/Config/TFTP-Client

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** leer

### 2.11.13.3 Firmware-Addresse

Standardpfad für Firmwaredateien, wenn der Parameter -f bei LoadFirmware nicht angegeben wird.

**SNMP-ID:** 2.11.13.3

**Pfad Telnet:** /Setup/Config/TFTP-Client

**Mögliche Werte:**

- Pfadangabe in der Schreibweise //Server/Verzeichnis/Dateiname

**Default:** leer

### 2.11.13.4 Firmware-Dateiname

Standard-Firmwaredatei, wenn der Parameter -f bei LoadFirmware nicht angegeben wird.

**SNMP-ID:** 2.11.13.4

**Pfad Telnet:** /Setup/Config/TFTP-Client

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** leer

### 2.11.13.6 Script-Addresse

Standardpfad für Skripte, wenn der Parameter -f bei LoadScript nicht angegeben wird.

**SNMP-ID:** 2.11.13.6

**Pfad Telnet:** /Setup/Config/TFTP-Client

**Mögliche Werte:**

- Pfadangabe in der Schreibweise //Server/Verzeichnis/Dateiname

**Default:** leer

### 2.11.13.7 Script-Dateiname

Standard-Skript, wenn der Parameter -f bei LoadScript nicht angegeben wird.

**SNMP-ID:** 2.11.13.7

**Pfad Telnet:** /Setup/Config/TFTP-Client

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** leer

## 2.11.15 Zugriffstabelle

Hier können Sie für jedes Netz und jedes unterstützte Konfigurationsprotokoll gesondert die Zugriffsrechte einstellen. Außerdem können Sie den Zugriff auf bestimmte Stationen einschränken.

**SNMP-ID:** 2.11.15

**Pfad Telnet:** /Setup/Config

### 2.11.15.1 Ifc.

Schnittstelle des Gerätes, auf die sich dieser Eintrag bezieht.

**SNMP-ID:** 2.11.15.1

**Pfad Telnet:** /Setup/Config/Zugriffstabelle

### 2.11.15.2 Telnet

Stellen Sie hier das Zugriffsrecht für die Konfiguration des Gerätes über das TELNET-Protokoll ein. Dieses Protokoll wird für die textbasierte und Betriebssystem-unabhängige Konfiguration dieses Gerätes über die implementierte Telnet-Konsole benötigt.

**SNMP-ID:** 2.11.15.2

**Pfad Telnet:** /Setup/Config/Zugriffstabelle

**Mögliche Werte:**

- VPN
- Ja
- Read
- Nein

**Default:** Ja

### 2.11.15.3 TFTP

Stellen Sie hier das Zugriffsrecht für die Konfiguration des Gerätes über das TFTP-Protokoll (Trivial File Transfer Protocol) ein. Dieses Protokoll wird zum Beispiel für die Konfiguration mit dem Programm LANconfig benötigt.

**SNMP-ID:** 2.11.15.3

**Pfad Telnet:** /Setup/Config/Zugriffstabelle

**Mögliche Werte:**

- VPN
- Ja
- Read
- Nein

**Default:** Ja

### 2.11.15.4 HTTP

Stellen Sie hier das Zugriffsrecht für die Konfiguration des Gerätes über das HTTP-Protokoll (Hypertext Transfer Protocol) ein. Dieses Protokoll wird für die Betriebssystem-unabhängige Konfiguration dieses Gerätes über das implementierte Web-Browser-Interface benötigt.

**SNMP-ID:** 2.11.15.4

**Pfad Telnet:** /Setup/Config/Zugriffstabelle

**Mögliche Werte:**

- VPN
- Ja
- Read
- Nein

**Default:** Ja

### 2.11.15.5 SNMP

Stellen Sie hier das Zugriffsrecht für die Konfiguration des Gerätes über das SNMP-Protokoll (Simple Network Management Protocol) ein. Dieses Protokoll wird zum Beispiel für die Überwachung des Gerätes mit dem Programm LANmonitor benötigt.

**SNMP-ID:** 2.11.15.5

**Pfad Telnet:** /Setup/Config/Zugriffstabelle

**Mögliche Werte:**

- VPN
- Ja
- Read
- Nein

**Default:** Ja

### 2.11.15.6 HTTPS

Stellen Sie hier das Zugriffsrecht für die Konfiguration des Gerätes über das HTTPS-Protokoll (Hypertext Transfer Protocol Secure bzw. HTTP über SSL) ein. Dieses Protokoll wird für die Betriebssystem-unabhängige und sichere Konfiguration dieses Gerätes über das implementierte Web-Browser-Interface benötigt.

**SNMP-ID:** 2.11.15.6

**Pfad Telnet:** /Setup/Config/Zugriffstabelle

**Mögliche Werte:**

- VPN
- Ja
- Read
- Nein

**Default:** Ja

### 2.11.15.7 Telnet-SSL

Stellen Sie hier das Zugriffsrecht für die Konfiguration des Gerätes über das TELNET-Protokoll ein. Dieses Protokoll wird für die textbasierte und Betriebssystem-unabhängige Konfiguration dieses Gerätes über die implementierte Telnet-Konsole benötigt.

**SNMP-ID:** 2.11.15.7

**Pfad Telnet:** /Setup/Config/Zugriffstabelle

**Mögliche Werte:**

- VPN
- Ja

- Read
- Nein

**Default:** LAN: ja, WAN:Nein

### 2.11.15.8 SSH

Stellen Sie hier das Zugriffsrecht für die Konfiguration des Gerätes über das TELNET/SSH-Protokoll ein. Dieses Protokoll wird für die textbasierte, Betriebssystem-unabhängige und sichere Konfiguration dieses Gerätes über die implementierte Telnet-Konsole benötigt.

**SNMP-ID:** 2.11.15.8

**Pfad Telnet:** /Setup/Config/Zugriffstabelle

**Mögliche Werte:**

- VPN
- Ja
- Read
- Nein

**Default:** Ja

## 2.11.20 Cron-Tabelle

Mit Hilfe von CRON-Jobs lassen sich regelmäßige Aktionen zu bestimmten Zeiten automatisch auf einem LANCOM ausführen. Sind in einer Installation sehr viele Geräte aktiv, die zu einem gemeinsamen Zeitpunkt über einen CRON-Job die gleiche Aktion ausführen (z. B. eine Konfiguration per Script aktualisieren), kann das zu unerwünschten Effekten führen, weil z. B. alle Geräte gleichzeitig die VPN-Verbindungen abbauen. Um diesen Effekt zu vermeiden, können die CRON-Jobs mit einer zufälligen Verzögerungszeit von 0 bis 59 Minuten definiert werden.

**SNMP-ID:** 2.11.20

**Pfad Telnet:** /Setup/Config

### 2.11.20.1 Index

Index für diesen Eintrag.

**SNMP-ID:** 2.11.20.1

**Pfad Telnet:** /Setup/Config/Cron-Tabelle

### 2.11.20.10 Besitzer

Als Besitzer des Cron-Jobs kann ein im Gerät definierter Administrator ausgewählt werden. Sofern ein Besitzer angegeben ist, werden die Befehle des Cron-Jobs mit den Rechten des Besitzers ausgeführt.

**SNMP-ID:** 2.11.20.10

**Pfad Telnet:** /Setup/Config/Cron-Tabelle

**Mögliche Werte:**

- max. 16 Zeichen

**Default:** leer

### 2.11.20.11 Variation

Dieser Parameter gibt eine Zeit in Minuten an, um welche die Ausführung eines CRON-Jobs gegenüber der definierten Startzeit maximal verzögert wird. Die tatsächliche Verzögerungszeit wird zufällig ermittelt und liegt zwischen Null und der hier eingetragenen Zeit.

**SNMP-ID:** 2.11.20.11

**Pfad Telnet:** /Setup/Config/Cron-Tabelle

**Mögliche Werte:**

- 0 bis 65535 Sekunden

**Default:** 0

**Besondere Werte:** Bei einer Variation von Null wird der CRON-Job exakt zur definierten Zeit ausgeführt.

Echtzeit-basierte Regeln können nur ausgeführt werden, sofern das Gerät über einen gültigen Zeitbezug verfügt, also z. B. via NTP.

### 2.11.20.2 Minute

Der Wert definiert den Zeitpunkt, an dem ein Kommando ausgeführt werden soll. Wird kein Wert angegeben, so wird er auch nicht in die Steuerung einbezogen. Es kann auch eine Komma-separierte Liste von Werten, oder aber ein Bereich (angegeben als "Minimalwert-max.wert") eingegeben werden.

**SNMP-ID:** 2.11.20.2

**Pfad Telnet:** /Setup/Config/Cron-Tabelle

**Mögliche Werte:**

- max. 50 Zeichen

**Default:** leer

### 2.11.20.3 Stunde

Der Wert definiert den Zeitpunkt, an dem ein Kommando ausgeführt werden soll. Wird kein Wert angegeben, so wird er auch nicht in die Steuerung einbezogen. Es kann auch eine Komma-separierte Liste von Werten, oder aber einen Bereich (angegeben als "Minimalwert-max.wert") eingegeben werden.

**SNMP-ID:** 2.11.20.3

**Pfad Telnet:** /Setup/Config/Cron-Tabelle

**Mögliche Werte:**

- max. 50 Zeichen

**Default:** leer

### 2.11.20.4 Wochentag

Der Wert definiert den Zeitpunkt, an dem ein Kommando ausgeführt werden soll. Wird kein Wert angegeben, so wird er auch nicht in die Steuerung einbezogen. Es kann auch eine Komma-separierte Liste von Werten, oder aber einen Bereich (angegeben als "Minimalwert-max.wert") eingegeben werden.

**SNMP-ID:** 2.11.20.4

**Pfad Telnet:** /Setup/Config/Cron-Tabelle

**Mögliche Werte:**

- 0: Sonntag
- 1: Montag
- 2: Dienstag
- 3: Mittwoch
- 4: Donnerstag
- 5: Freitag
- 6: Samstag

**Default:** leer

### 2.11.20.5 Tag

Der Wert definiert den Zeitpunkt, an dem ein Kommando ausgeführt werden soll. Wird kein Wert angegeben, so wird er auch nicht in die Steuerung einbezogen. Es kann auch eine Komma-separierte Liste von Werten, oder aber ein Bereich (angegeben als "Minimalwert-max.wert") eingegeben werden.

**SNMP-ID:** 2.11.20.5

**Pfad Telnet:** /Setup/Config/Cron-Tabelle

**Mögliche Werte:**

- max. 50 Zeichen

**Default:** leer

### 2.11.20.6 Monat

Der Wert definiert den Zeitpunkt, an dem ein Kommando ausgeführt werden soll. Wird kein Wert angegeben, so wird er auch nicht in die Steuerung einbezogen. Es kann auch eine Komma-separierte Liste von Werten, oder aber ein Bereich (angegeben als "Minimalwert-max.wert") eingegeben werden.

**SNMP-ID:** 2.11.20.6

**Pfad Telnet:** /Setup/Config/Cron-Tabelle

**Mögliche Werte:**

- 0: Sonntag
- 1: Montag
- 2: Dienstag
- 3: Mittwoch
- 4: Donnerstag
- 5: Freitag
- 6: Samstag

**Default:** leer

### 2.11.20.7 Kommando

Das auszuführende Kommando oder eine Komma-separierte Kommando-Liste. Ausgeführt werden kann dabei jede beliebige LANCOM Kommandozeilenfunktion.

**SNMP-ID:** 2.11.20.7

**Pfad Telnet:** /Setup/Config/Cron-Tabelle

**Mögliche Werte:**

- max. 100 Zeichen

**Default:** leer

### 2.11.20.8 Basis

Bestimmt ob die zeitliche Steuerung auf Grundlage der Echtzeit oder auf Grundlage der Betriebszeit des Gerätes ausgeführt werden soll.

**SNMP-ID:** 2.11.20.8

**Pfad Telnet:** /Setup/Config/Cron-Tabelle

**Mögliche Werte:**

- Echtzeit: Diese Regeln werten alle Zeit-/Datumsangaben aus. Echtzeit-basierte Regel können nur ausgeführt werden, sofern das Gerät über einen gültigen Zeitbezug verfügt, also z. B. via NTP.
- Betriebszeit: Diese Regeln werten nur die Minuten- und Stundenangaben seit dem letzten Gerätestart aus.

**Default:** Echtzeit

### 2.11.20.9 Aktiv

Aktiviert oder deaktiviert den Eintrag.

**SNMP-ID:** 2.11.20.9

**Pfad Telnet:** /Setup/Config/Cron-Tabelle

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

## 2.11.21 Admins

Hier können Sie weitere Admin-Benutzerkonten anlegen.

**SNMP-ID:** 2.11.21

**Pfad Telnet:** /Setup/Config

### 2.11.21.1 Administrator

In der Konfiguration des Gerätes können mehrere Administratoren angelegt werden, die über unterschiedliche Zugriffsrechte verfügen. Für ein LANCOM können bis zu 16 verschiedene Administratoren eingerichtet werden.

**SNMP-ID:** 2.11.21.1

**Pfad Telnet:** /Setup/Config/Admins

**Mögliche Werte:**

- max. 16 Zeichen

**Default:** leer

Neben den in der Konfiguration angelegten Administratoren gibt es auch noch den „root"-Administrator mit dem Haupt-Geräte-Passwort. Dieser Administrator hat immer die vollen Rechte und kann auch nicht gelöscht oder umbenannt werden. Um sich als root-Administrator anzumelden, geben Sie im Login-Fenster den Benutzernamen „root" ein oder Sie lassen dieses Feld frei. Sobald in der Konfiguration des Gerätes ein Passwort für den „root"-Administrator gesetzt ist, erscheint beim Aufruf von WEBconfig auf der Startseite die Schaltfläche Login, mit dem das Fenster zur Anmeldung eingeblendet wird. Nach Eingabe von korrektem Benutzernamen und Passwort erscheint das Hauptmenü der WEBconfig. In diesem Menü sind nur die Punkte vorhanden, für die der Administrator Zugriffs- bzw. Funktionsberechtigungen hat. Ist mindestens ein weiterer Administrator in der

Admin-Tabelle eingerichtet, so enthält das Hauptmenü zusätzlich eine Schaltfläche Administrator wechseln, der es erlaubt zu einer anderen Benutzerkennung (mit ggf. anderen Rechten) zu wechseln.

### 2.11.21.2 Passwort

Kennwort für diesen Eintrag.

**SNMP-ID:** 2.11.21.2

**Pfad Telnet:** /Setup/Config/Admins

**Mögliche Werte:**

- max. 16 Zeichen

**Default:** leer

### 2.11.21.3 Funktionsrechte

Jeder Administrator verfügt über „Funktionsrechte", die den persönlichen Zugriff auf bestimmte Funktionen wie z. B. die Setup-Assistenten regeln.

**SNMP-ID:** 2.11.21.3

**Pfad Telnet:** /Setup/Config/Admins

**Mögliche Werte:**

- Zur Darstellung der Funktionsrechte stehen die folgenden Hexadezimalwerte zur Verfügung:
- 0x00000001 Der Benutzer darf den Grundkonfigurations-Assistenten ausführen
- 0x00000002 Der Benutzer darf den Sicherheits-Assistenten ausführen
- 0x00000004 Der Benutzer darf den Internet-Assistenten ausführen
- 0x00000008 Der Benutzer darf den Assistenten zur Auswahl von Internet-Providern ausführen
- 0x00000010 Der Benutzer darf den RAS-Assistenten ausführen
- 0x00000020 Der Benutzer darf den LAN-LAN-Kopplungs-Assistenten ausführen
- 0x00000040 Der Benutzer darf die Uhrzeit und das Datum stellen (gilt auch für Telnet und TFTP)
- 0x00000080 Der Benutzer darf nach weiteren Geräten suchen
- 0x00000100 Der Benutzer darf den WLAN-Linktest ausführen (gilt auch für Telnet)
- 0x00000200 Der Benutzer darf den a/b-Assistenten ausführen
- 0x00000400 Der Benutzer darf den WTP-Zuordnungs-Assistenten ausführen
- 0x00000800 Der Benutzer darf den Public-Spot-Assistenten ausführen
- 0x00001000 Der Benutzer darf den WLAN-Assistenten ausführen
- 0x00002000 Der Benutzer darf den Rollout-Assistenten ausführen
- 0x00004000 Der Benutzer darf den Dynamic-DNS-Assistenten ausführen
- 0x00008000 Der Benutzer darf den VoIP-CallManager-Assistenten ausführen
- 0x00010000 Der Benutzer darf den WLC-Profil-Assistenten ausführen
- 0x00020000 Der Benutzer darf den eingebauten Telnet- bzw. SSH-Client benutzen

**Default:** leer

### 2.11.21.4 Aktiv

Aktiviert bzw. Deaktiviert die Funktion.

**SNMP-ID:** 2.11.21.4

**Pfad Telnet:** /Setup/Config/Admins

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

### 2.11.21.5 Zugriffsrechte

Der Zugriff auf die internen Funktionen kann wie folgt getrennt nach Interfaces getrennt konfiguriert werden:

- ISDN-Aministrationszugang

- LAN

- Wireless LAN (WLAN)

- WAN (z. B. ISDN, DSL oder ADSL)

Bei den Netzwerk-Konfigurationszugriffen können weitere Einschränkungen vorgenommen werden, z. B. dass nur die Konfiguration von bestimmten IP-Adressen oder LANCAPI-Clients vorgenommen werden darf. Ferner sind die folgenden internen Funktionen getrennt schaltbar:

- LANconfig (TFTP)

- WEBconfig (HTTP, HTTPS)

- SNMP

- Terminal/Telnet

Bei Geräten mit VPN-Unterstützung kann die Nutzung der einzelnen internen Funktionen über WAN-Interfaces auch nur auf VPN-Verbindungen beschränkt werden.

**SNMP-ID:** 2.11.21.5

**Pfad Telnet:** /Setup/Config/Admins

**Mögliche Werte:**

- Kein
- Admin-RO-Limit
- Admin-RW-Limit
- Admin-Ro
- Admin-RW
- Supervisor

**Default:** leer

## 2.11.26 SSH-Authentisierungs-Methoden

Legen Sie hier fest welche Authentizifierungsmethoden für SSH verwendet werden sollen.

**SNMP-ID:** 2.11.26

**Pfad Telnet:** /Setup/Config

### 2.11.26.1 lfc.

Die zulässigen Authentifizierungs-Methoden für den SSH-Zugang können für LAN, WAN und WLAN getrennt eingestellt werden.

**SNMP-ID:** 2.11.26.1

**Pfad Telnet:** /Setup/Config/SSH-Authentisierungs-Methoden

**Mögliche Werte:**

- LAN
- WAN
- WLAN

### 2.11.26.2 Methoden

Das SSH-Protokoll erlaubt grundsätzlich zwei verschiedene Authentifizierungs-Mechanismen: Benutzername und Kennwort, mit Hilfe eines öffentlichen Schlüssels (Public Key) oder oder interaktiv über die Tastatur .

**SNMP-ID:** 2.11.26.2

**Pfad Telnet:** /Setup/Config/SSH-Authentisierungs-Methoden

**Mögliche Werte:**

- Public Key: Erlaubt nur die Authentifizierung über Zertifikat.
- Keyboard-Interactive: Erlaubt nur die interaktive Authentifizierung über die Tastatur.
- Password: Erlaubt nur die Authentifizierung über Kennwort.
- Password und Keyboard-Interactive: Erlaubt die Authentifizierung über Kennwort oder interaktiv über die Tastatur.
- Password und Public Key: Erlaubt die Authentifizierung über Kennwort oder über Zertifikat.
- Keyboard-Interactive und Public Key: Erlaubt nur die interaktive Authentifizierung über die Tastatur oder über Zertifikat.
- Alle: Erlaubt die Authentifizierung über alle Methoden.

**Default:** Alle

## 2.11.27 Predef.-Admins

Hier finden Sie den vordefinierten Admin-Account des Gerätes. Dieser Admin-Account wird verwendet, wenn beim Login kein Benutzername angegeben wird.

**SNMP-ID:** 2.11.27

**Pfad Telnet:** /Setup/Config/Predef.-Admins

### 2.11.27.1 Name

Geben Sie hier den Namen für den vordefinierten Admin-Account ein.

**SNMP-ID:** 2.11.27.1

**Pfad Telnet:** /Setup/Config/Predef.-Admins/Name

**Mögliche Werte Telnet:**

- maximal 16 Zeichen

**Default:** leer

## 2.11.30 Update-Client

Dieses Menü enthält die Einstellungen für den Update-Client

**SNMP-ID:** 2.11.30

**Pfad Telnet:** /Setup/Config

Die Einstellungen für den Update-Client werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

### 2.11.30.1 Aktiv

Aktiviert oder deaktiviert den Update-Client.

**SNMP-ID:** 2.11.30.1

**Pfad Telnet:** /Setup/Config/Update-Client

**Mögliche Werte:**

- nein
- ja

**Default:** nein

Die Einstellungen für den Update-Client werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

### 2.11.30.4 Antwort-Timeout

Timeout in Sekunden für die Antworten des Update-Clients.

**SNMP-ID:** 2.11.30.4

**Pfad Telnet:** /Setup/Config/Update-Client

**Mögliche Werte:**

- maximal 10 numerische Werte im Bereich von 0 - 4289999999

**Default:** 3

Die Einstellungen für den Update-Client werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

### 2.11.30.7 Letztes-Firmware-Update

Datum und Uhrzeit des letzten Firmware-Updates.

**SNMP-ID:** 2.11.30.7

**Pfad Telnet:** /Setup/Config/Update-Client

Die Einstellungen für den Update-Client werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

### 2.11.30.8 Letztes-Konfig-Update

Datum und Uhrzeit des letzten Konfigurations-Updates.

**SNMP-ID:** 2.11.30.8

**Pfad Telnet:** /Setup/Config/Update-Client

Die Einstellungen für den Update-Client werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

### 2.11.30.2 Server-Name

Dieser Parameter gibt die Server-Adresse an, die das Gerät für den Update-Client nutzt.

**SNMP-ID:** 2.11.30.2

**Pfad Telnet:** /Setup/Config/Update-Client

**Mögliche Werte:**

- maximal 64 alphanumerische Zeichen

**Default:** leer

Die Einstellungen für den Update-Client werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

### 2.11.30.3 Server-Port

Dieser Parameter gibt den Server-Port an, die das Gerät für den Update-Client nutzt.

**SNMP-ID:** 2.11.30.3

**Pfad Telnet:** /Setup/Config/Update-Client

**Mögliche Werte:**

- maximal 5 numerische Zeichen im Bereich von 1 - 65535

**Default:** 12501

Die Einstellungen für den Update-Client werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

### 2.11.30.5 Wiederholung-Fehler

Nach dieser Zeit in Sekunden meldet das Gerät einen Fehler, wenn der Update-Server nicht auf Anfragen antwortet.

**SNMP-ID:** 2.11.30.5

**Pfad Telnet:** /Setup/Config/Update-Client

**Mögliche Werte:**

- maximal 10 numerische Werte im Bereich von 0 bis 4289999999

**Default:** 60

Die Einstellungen für den Update-Client werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

### 2.11.30.6 Wiederholung-Ok

Zeit in Sekunden für den Update-Client, nach der das Gerät einen neuen Update-Versuch startet.

**SNMP-ID:** 2.11.30.6

**Pfad Telnet:** /Setup/Config/Update-Client

**Mögliche Werte:**

- maximal 10 numerische Zeichen im Bereich von 0 - 4289999999

**Default:** 86400

Die Einstellungen für den Update-Client werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

## 2.11.31 Standortverifikation

Nach einem Diebstahl kann ein Gerät theoretisch von Unbefugten an einem anderen Ort betrieben werden. Auch bei einer passwortgeschützten Geräte-Konfiguration könnten so die im Gerät konfigurierten RAS-Zugänge, LAN-Kopplungen oder VPN-Verbindungen unerlaubt genutzt werden, ein Dieb könnte sich Zugang zu geschützten Netzwerken verschaffen. Der Betrieb des Gerätes kann jedoch mit verschiedenen Mitteln so geschützt werden, dass es nach dem Wiedereinschalten oder beim Einschalten an einem anderen Ort nicht mehr verwendet werden kann.

GPS-Standort-Verifikation

Für die GPS-Standort-Verifikation können Sie im Gerät eine erlaubte geografische Position definieren. Nach dem Einschalten aktiviert das Gerät bei Bedarf automatisch das GPS-Modul und prüft, ob es sich an der „richtigen" Position befindet – nur bei einer positiven Prüfung wird das Router-Modul eingeschaltet. Nach Abschluss der Standort-Verifikation wird das GPS-Modul automatisch wieder deaktiviert, sofern es nicht manuell eingeschaltet ist. ISDN-Standort-Verifikation Mit der ISDN-Standort-Verifikation können Sie den Missbrauch eines Routers verhindern: Der Router überprüft dann nach jedem Einschalten über einen ISDN-Anruf zu sich selbst, ob er am vorgesehenen Standort installiert ist. Erst wenn die Standort-Überprüfung erfolgreich ausgeführt wurde, wird das Router-Modul eingeschaltet.

ISDN-Standort-Verifikation

Das Gerät muss aus dem öffentlichen ISDN-Netz erreichbar sein. Während der Überprüfung mit dem Selbstanruf benötigt das Gerät zwei freie B-Kanäle. Solange nur ein freier Kanal bereitsteht, z. B. weil an einem Mehrgeräteanschluss mit zwei B-Kanälen ein Kanal zum Telefonieren verwendet wird, kann sich das Gerät nicht selbst über ISDN anrufen.

**SNMP-ID:** 2.11.31

**Pfad Telnet:** /Setup/Config

### 2.11.31.3 Zielrufnummer

Diese Rufnummer wird bei einem Anruf zur Standortverifikation über ISDN angerufen.

**SNMP-ID:** 2.11.31.3

**Pfad Telnet:** /Setup/Config/Standortverifikation

**Mögliche Werte:**

- max. 14 Zeichen

**Default:** leer

### 2.11.31.8 Abweichung

Abweichung von der erlaubten Position in Metern

**SNMP-ID:** 2.11.31.8

**Pfad Telnet:** /Setup/Config/Standortverifikation

**Mögliche Werte:**

- 50

### 2.11.31.10 Breitengrad

Breitengrad des Standortes, an dem das Gerät in Betrieb genommen wird.

**SNMP-ID:** 2.11.31.10

**Pfad Telnet:** /Setup/Config/Standortverifikation

**Mögliche Werte:**

- leer

## 2.11.31.4 Erwartete-abgehende-Rufnummer

Diese Rufnummer wird bei einem Anruf zur Standortverifikation über ISDN als eingehende Rufnummer erwartet.

**SNMP-ID:** 2.11.31.4

**Pfad Telnet:** /Setup/Config/Standortverifikation

**Mögliche Werte:**

- max. 14 Zeichen

**Default:** leer

## 2.11.31.12 GPS-Position-holen

Mit dieser Option kann das Gerät die Geo-Koordinaten für den aktuellen Standort selbst ermitteln. Nach dem Rückschreiben der Konfiguration in das Gerät werden automatisch die aktuellen Längen- und Breitengrade eingetragen, wenn die Standortverifikation aktiv ist und gültige GPS-Daten vorliegen. Anschließend wird diese Option selbsttätig wieder deaktiviert.

**Pfad Telnet:** /Setup/Config/Standortverifikation

**Mögliche Werte:**

- Ja
- Nein

## 2.11.31.1 In-Betrieb

Mit der Option 'Standort-Überprüfung einschalten' aktivieren Sie die Standort-Verifikation. Mit der ISDN-Standort-Verifikation können Sie den Missbrauch eines Routers verhindern: Der Router überprüft dann nach jedem Einschalten über einen ISDN-Anruf zu sich selbst, ob er am vorgesehenen Standort installiert ist. Erst wenn die Standort-Überprüfung erfolgreich ausgeführt wurde, wird das Router-Modul eingeschaltet. Voraussetzungen für eine erfolgreiche ISDN-Standort-Verifikation: Das Gerät muss aus dem öffentlichen ISDN-Netz erreichbar sein. Während der Überprüfung mit dem Selbstanruf benötigt das Gerät zwei freie B-Kanäle. Solange nur ein freier Kanal bereitsteht, z. B. weil an einem Mehrgeräteanschluss mit zwei B-Kanälen ein Kanal zum Telefonieren verwendet wird, kann sich das Gerät nicht selbst über ISDN anrufen.

**SNMP-ID:** 2.11.31.1

**Pfad Telnet:** /Setup/Config/Standortverifikation

## 2.11.31.7 ISDN-Ifc

Schnittstelle des Gerätes, auf die sich dieser Eintrag bezieht.

**SNMP-ID:** 2.11.31.7

**Pfad Telnet:** /Setup/Config/Standortverifikation

**Mögliche Werte:**

- S0-1
- S0-2

### 2.11.31.9 Laengengrad

Längengrad des Standortes, an dem das Gerät in Betrieb genommen wird.

**SNMP-ID:** 2.11.31.9

**Pfad Telnet:** /Setup/Config/Standortverifikation

**Mögliche Werte:**

- leer

### 2.11.31.6 Methode

Wählen Sie die Methode für die Standort-Überprüfung.

**SNMP-ID:** 2.11.31.6

**Pfad Telnet:** /Setup/Config/Standortverifikation

**Mögliche Werte:**

- Basic-Call: Selbst-Anruf für die Überprüfung über ISDN mit einem Rückruf.
- Facility: Rufweiterleitungs-Überprüfung für die Überprüfung über ISDN durch Abfrage der Rufnummer aus der Vermittlungsstelle. Hierbei ist kein Rückruf erforderlich.
- GPS: GPS-Verifikation für die Überprüfung über die Geo-Koordinaten.

Für die Standort-Überprüfung über GPS muss eine entsprechende GPS-Antenne an den AUX-Anschluss des Gerätes angeschlossen werden. Zusätzlich muss eine SIM-Karte für den Mobilfunkbetrieb eingelegt werden und das Gerät muss in ein Mobilfunknetz eingebucht sein. Für eine erfolgreiche ISDN-Standort-Verifikation muss das Gerät aus dem öffentlichen ISDN-Netz erreichbar sein. Während der Überprüfung mit dem Selbstanruf benötigt das Gerät zwei freie B-Kanäle. Solange nur ein freier Kanal bereitsteht, z. B. weil an einem Mehrgeräteanschluss mit zwei B-Kanälen ein Kanal zum Telefonieren verwendet wird, kann sich das Gerät nicht selbst über ISDN anrufen.

### 2.11.31.2 Abgehende Rufnummer

Diese Rufnummer wird bei einem Anruf zur Standortverifikation über ISDN als ausgehende Rufnummer verwendet.

**SNMP-ID:** 2.11.31.2

**Pfad Telnet:** /Setup/Config/Standortverifikation

**Mögliche Werte:**

- max. 14 Zeichen

**Default:** leer

## 2.11.35 Monitortrace

Dieses Menü enthält die Einstellungen für Monitor-Tracing

**SNMP-ID:** 2.11.35

**Pfad Telnet:** /Setup/Config

### 2.11.35.1 Tracemask1

Dieser Parameter wird nur für Supportzwecke gebraucht.

**SNMP-ID:** 2.11.35.1

**Pfad Telnet:** /Setup/Config/Monitortrace

### 2.11.35.2 Tracemask2

Dieser Parameter wird nur für Supportzwecke benötigt.

**SNMP-ID:** 2.11.35.2

**Pfad Telnet:** /Setup/Config/Monitortrace

## 2.11.43 Funktionstasten

Mit den Funktionstasten haben Sie die Möglichkeit, häufig genutzte Befehlssequenzen zu speichern und an der Kommandozeile komfortabel aufzurufen. In der entsprechenden Tabelle werden den Funktionstasten F1 bis F12 die Befehle so zugeordnet, wie sie an der Kommandozeile eingegeben werden.

**SNMP-ID:** 2.11.43

**Pfad Telnet:** /Setup/Config

### 2.11.43.1 Taste

Bezeichnung der Funktionstaste.

**SNMP-ID:** 2.11.43.1

**Pfad Telnet:** /Setup/Config/Funktionstasten

**Mögliche Werte:**

- Auswahl aus den Funktionstasten F1 bis F12.

**Default:** F1

### 2.11.43.2 Abbildung

Beschreibung des Befehls bzw. der Tastenkombination, die bei Aufruf der Funktionstaste an der Kommandozeile ausgeführt werden soll.

**SNMP-ID:** 2.11.43.2

**Pfad Telnet:** /Setup/Config/Funktionstasten

**Mögliche Werte:**

- Alle an der Kommandozeile möglichen Befehle bzw. Tastenkombinationen

**Default:** Leer

**Besondere Werte:** Das Caret-Zeichen ^ wird verwendet, um spezielle Steuerungsbefehle mit ASCII-Werten unterhalb von 32 abzubilden.^a

^A steht für Strg-A (ASCII 1)

^Z steht für Strg-Z (ASCII 26)

^[ steht für Escape (ASCII 27)

^M steht für Return/Enter erwähnen. Dieses Zeichen ist z. B. dann nützlich, wenn Sie ein Kommando mit der Funktionstaste nicht nur eingeben, sondern auch direkt abschicken möchten.

^^ Ein doppeltes Caret-Zeichen steht für das Caret-Zeichen selbst ^.

Wenn Sie ein Caret-Zeichen direkt gefolgt von einem anderen Zeichen in ein Dialogfeld oder in einem Editor eingeben, wird das Betriebssystem diese Sequenz möglicherweise als ein anderes Sonderzeichen deuten. Aus der Eingabe von Caret-Zeichen + A macht ein Windows-Betriebssystem z. B. ein Â. Um das Caret-Zeichen selbst

aufzurufen, geben Sie vor dem folgenden Zeichen ein Leerzeichen ein. Aus Caret-Zeichen + Leerzeichen + A wird dann die Sequenz ^A.

## 2.11.50 LL2M

Dieses Menü enthält die Einstellungen für LANCOM Layer-2 Management.

**SNMP-ID:** 2.11.50

**Pfad Telnet:** /Setup/Config

### 2.11.50.1 In-Betrieb

Schaltet den LL2M-Server ein oder aus. Ein aktivierter LL2M-Server kann nach dem Booten/Einschalten des Gerätes für die Dauer des Zeit-Limits von einem LL2M-Client angesprochen werden.

**SNMP-ID:** 2.11.50.1

**Pfad Telnet:** /Setup/Config/LL2M

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

### 2.11.50.2 Zeit-Limit

Definiert die Zeitspanne in Sekunden, in der ein aktivierter LL2M-Server nach dem Booten/Einschalten des Gerätes von einem LL2M-Client angesprochen werden kann. Nach Ablauf des Zeit-Limits wird der LL2M-Server automatisch deaktiviert.

**SNMP-ID:** 2.11.50.2

**Pfad Telnet:** /Setup/Config/LL2M

**Mögliche Werte:**

- 0 bis 4294967295

**Default:** 0

**Besondere Werte:** 0 deaktiviert das Zeit-Limit, in diesem Zustand bleibt der LL2MServer dauerhaft aktiv.

# 2.12 WLAN

Dieses Menü enthält die Einstellungen für kabellose Netzwerke (WLAN)

**SNMP-ID:** 2.12

**Pfad Telnet:** /Setup

## 2.12.114 Aggregat-Wiederholungs-Limit

Dieser Parameter gibt an, wie viele Male ein Aggregat von zu sendenden Paketen von der Hardware wiederholt werden darf, bis es erst einmal wieder zurückgestellt wird und andere zu sendende Pakete zum Zuge kommen können. Mit der Begrenzung auf wenige Wiederholungen wird so z. B. in VoIP-Umgebungen die maximale Verzögerung von VoIP-Paketen begrenzt.

**SNMP-ID:** 2.12.114

**Pfad Telnet:** /Setup/WLAN/Aggregat-Wiederholungs-Limit

**Mögliche Werte:**

- 0 bis 255

**Default:** 255

Das unter 'Hard-Retries' eingestellte absolute Limit für Sendeversuche bleibt von diesem Wert unbeeinflusst.

## 2.12.38 ARP-Behandlung

Will eine Station im LAN eine Verbindung zu einer Station im WLAN aufbauen, die im Stromspar-Modus ist, so klappt dies häufig entweder gar nicht oder nur mit großen Verzögerungen. Der Grund ist, dass die Auslieferung von Broadcasts, z. B. ARP-Anfragen, an im Powersave befindliche Stationen von der Basisstation nicht garantiert werden kann.

Wenn Sie die ARP-Behandlung einschalten, beantwortet die Basisstation ARP-Anfragen für bei ihr eingebuchte Stationen selber und damit in solchen Fällen zuverlässiger.

**SNMP-ID:** 2.12.38

**Pfad Telnet:** /Setup/WLAN

**Mögliche Werte:**

- Ein
- Aus

**Default:** Ein

Ab der LCOS-Version 8.00 wird mit diesem Schalter eine analoge Behandlung für IPv6-Neighbor-Solicitations aktiviert.

## 2.12.48 Benutze-vollen-Kanalsatz

Dieser Parameter erlaubt bei Benutzung von 5 GHz und DFS die Verwendung der ansonsten wegen 'Wetterradars' gesperrten Kanäle 120, 124, 128.

**SNMP-ID:** 2.12.48

**Pfad Telnet:** /Setup/WLAN/Benutze-vollen-Kanalsatz

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

Beachten Sie, dass die Aktivierung dieser Option eine Verletzung der ETSI- Bestimmungen darstellt, da für LCOS keine Zulassungen dieser Kanäle durchgeführt wurden.

## 2.12.44 Erlaube-illegale-Assoziation-ohne-Authentifizierung

Dieser Parameter aktiviert oder deaktiviert die Möglichkeit, dass das Gerät sich mit einem WLAN ohne Authentifizierung verbindet.

**SNMP-ID:** 2.12.44

**Pfad Telnet:** /Setup/WLAN

**Mögliche Werte:**

- ja
- nein

**Default:** nein

## 2.12.115 Globale-Krypto-Sequenz-Pruefung-auslassen

Stellen Sie hier die globale Prüfung der Krypto-Sequenz ein.

**SNMP-ID:** 2.12.115

**Pfad Telnet:** /Setup/WLAN

**Mögliche Werte:**

- Auto
- Ja
- Nein

**Default:** Auto

**Besondere Werte:** Auto: LCOS enthält eine Liste der für diese Verhalten bekannten Geräte und schaltet in der Einstellung 'Auto' die globale Sequenzprüfung ab. Für andere, noch nicht in der Liste enthaltenen Geräte muss die globale Sequenzprüfung manuell deaktiviert werden.

## 2.12.3 Heap-Reserve

Die Heap-Reserve gibt an, wie viele Blöcke des LAN-Heaps für die direkte Kommunikation (Telnet) mit dem Gerät reserviert werden. Wenn die Anzahl der Blöcke im Heap unter den angegebenen Wert fällt, dann werden empfangene Pakete sofort verworfen (außer bei TCP-Paketen, die direkt an das Gerät gerichtet sind).

**SNMP-ID:** 2.12.3

**Pfad Telnet:** /Setup/WLAN

**Mögliche Werte:**

- max. 3 Ziffern

**Default:** 10

## 2.12.13 IAPP-Announce-Interval

In diesem Intervall (in Sekunden) geben die Access Points ihre SSIDs bekannt.

**SNMP-ID:** 2.12.13

**Pfad Telnet:** /Setup/WLAN

**Mögliche Werte:**

- max. 10 Ziffern

**Default:** 120

## 2.12.14 IAPP-Handover-Timeout

Bei einem erfolgreichen Roaming-Vorgang (Handover) informiert der neue Access Point den bisherigen Access Point darüber, dass ein bestimmter Client jetzt bei einem anderen Access Point angemeldet ist. Mit dieser Information kann der alte Access Point den Client aus seiner Stationstabelle austragen und leitet nicht mehr (unnötigerweise) Pakete für diesen Client in seine Funkzelle weiter. Für diesen Zeitraum (in Millisekunden) wartet der neue Access Point, bis er

versucht, den bisherigen Access Point noch einmal zu kontaktieren. Nach fünf Versuchen gibt der neue Access Point diese Versuche auf.

**SNMP-ID:** 2.12.14

**Pfad Telnet:** /Setup/WLAN

**Mögliche Werte:**

- max. 10 Ziffern

**Default:** 1000

## 2.12.60 IAPP-IP-Netzwerk

Wählen Sie hier aus, welches ARF-Netzwerk als IAPP-IP-Netzwerk verwendet werden soll.

**SNMP-ID:** 2.12.60

**Pfad Telnet:** /Setup/WLAN

**Mögliche Werte:**

- Auswahl aus der Liste der im Gerät definierten ARF-Netzwerke
- maximal 16 alphanumerische Zeichen

**Default:** leer

**Besondere Werte:** leer: Wenn kein IAPP-IP-Netzwerk definiert ist, werden die IAPP-Announces in alle definierten ARF-Netze versendet.

## 2.12.12 IAPP-Protokoll

Über das Inter Access Point Protocol (IAPP) tauschen die Access Points untereinander Informationen über die eingebuchten Clients aus. Diese Informationen werden beim Roaming von Clients zwischen verschiedenen Access Points verwendet. Der neue Access Point informiert den bisherigen Access Point über den Roaming-Vorgang, damit der bisherige Access Point den Client aus seiner Stationstabelle löschen kann.

**SNMP-ID:** 2.12.12

**Pfad Telnet:** /Setup/WLAN

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

## 2.12.47 Idle-Timeout

Das ist die Zeit in Sekunden, nach der ein Client getrennt wird, wenn der Aceess Point keine Pakete von ihm empfangen hat.

**SNMP-ID:** 2.12.47

**Pfad Telnet:** /Setup/WLAN/Idle-Timeout

**Mögliche Werte Telnet:**

- Max. 10 numerische Zeichen

**Default:** 3600 Sekunden

## 2.12.26 Inter-SSID-Verkehr

Je nach Anwendungsfall ist es gewünscht oder eben auch nicht erwünscht, dass die an einem Access Point angeschlossenen WLAN-Clients mit anderen Clients kommunizieren. Die Kommunikation der Clients in unterschiedlichen SSIDs kann mit dieser Option erlaubt oder verhindert werden. Bei Modellen mit mehreren WLAN-Modulen gilt diese Einstellung global für allem WLANs aller Module.

**SNMP-ID:** 2.12.26

**Pfad Telnet:** /Setup/WLAN

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

Die Kommunikation der Clients innerhalb eines logischen WLANs wird separat bei den logischen WLAN-Einstellungen gesteuert (Inter-Station-Verkehr). Wenn der Inter-SSID-Verkehr aktiviert ist und der Inter-Station-Verkehr deaktiviert, kann ein Client aus einem logischen WLAN mit den Clients in anderen logischen WLANs kommunizieren. Diese Möglichkeit kann über VLAN-Einstellungen oder Protokollfilter verhindert werden.

## 2.12.100 Karten-Reinit-Zyklus

In diesem Intervall (in Sekunden) werden die internen WLAN-Karten bei älteren Access Points reinitialisiert, um Point-to-Point-Verbindungen aufrecht zu erhalten. Diese Funktion wird bei aktuelleren Modellen über den "Alive-Test" ersetzt.

**SNMP-ID:** 2.12.100

**Pfad Telnet:** /Setup/WLAN

**Mögliche Werte:**

- max. 10 Ziffern

**Default:** 0

**Besondere Werte:** 0: Deaktiviert diese Funktion.

## 2.12.36 Land

Damit Ihr Wireless-Netz mit den richtigen Parametern betrieben werden kann, muss das Gerat seinen nationalen Standort kennen.

**SNMP-ID:** 2.12.36

**Pfad Telnet:** /Setup/WLAN

**Mögliche Werte:**

- Auswahl aus der Liste der angebotenen Länder.

**Default:** unbekannt

**Besondere Werte:** unbekannt: Lässt nur die Einstellungen zu, die weltweit zugelassen sind.

## 2.12.41 Mail-Adresse

An diese E-Mail-Adresse werden Informationen über die Ereignisse im WLAN versendet.

**SNMP-ID:** 2.12.41

**Pfad Telnet:** /Setup/WLAN

**Mögliche Werte:**

- Gültige E-Mail-Adresse

**Default:** Leer

Zur Nutzung der E-Mail-Benachrichtigung muss ein SMTP-Konto eingerichtet sein.

## 2.12.46 Nur-Indoor-Betrieb

Bei aktiviertem Indoor-Only Modus werden im 5 GHz Band in ETSI-Ländern die Kanäle auf den Bereich 5,15 bis 5,25 GHz (Kanäle 36-48) beschränkt. Die Radarerkennung (DFS) wird ausgeschaltet und es entfällt die Zwangsunterbrechung alle 24 Stunden. In dieser Betriebsart ist daher das Risiko von Unterbrechungen durch (falsche) Radarerkennungen reduziert. Im 2,4 GHz Band in Frankreich werden die Kanäle 8 bis 13 freigegeben, wodurch mehr Kanäle zur Verfügung stehen.

**SNMP-ID:** 2.12.46

**Pfad Telnet:** /Setup/WLAN

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

Die Aktivierung des Indoor-Only-Modus ist nur erlaubt, wenn die Basisstation und alle Stationen in einem geschlossenen Raum betrieben werden.

Die Aktivierung des Indoor-Only Modus ist nur erlaubt, wenn die Basisstation und alle Stationen in einem geschlossenen Raum betrieben werden.

## 2.12.108 Radar-Last-Schwellwert

Dieser Wert gibt die prozentuale Auslastung des WLAN-Moduls an, bei dem die Genauigkeit der Radarerkennung reduziert wird.

**SNMP-ID:** 2.12.108

**Pfad Telnet:** /Setup/WLAN

**Mögliche Werte:**

- maximal 3 numerische Zeichen im Bereich von 0 - 100

**Default:** 40

## 2.12.101 Rausch-Messzyklus

In diesem Intervall (in Sekunden) wird bei WLAN-Karten mit Atheros-Chipsatz der Rauschpegel auf dem Medium gemessen.

**SNMP-ID:** 2.12.101

**Pfad Telnet:** /Setup/WLAN

**Mögliche Werte:**

- max. 10 Ziffern

**Default:** 0

**Besondere Werte:** 0: Deaktiviert diese Funktion.

## 2.12.105 Therm.-Rekal.-Messzyklus

In diesem Intervall (in Sekunden) wird bei älteren WLAN-Karten mit Atheros-Chipsatz die Sendeleistung korrigiert, um thermische Schwankungen auszugleichen.

**SNMP-ID:** 2.12.105

**Pfad Telnet:** /Setup/WLAN

**Mögliche Werte:**

- max. 10 Ziffern

**Default:** 20

**Besondere Werte:** 0: Deaktiviert diese Funktion.

Bitte beachten Sie, dass die Hardware der WLAN-Karte bei deaktiviertem Therm.-Rekal.-Messzyklus nicht mehr auf thermische Schwankungen reagieren kann!

## 2.12.103 Trace-MAC

Für den WLAN-Data-Trace kann die Ausgabe von Tracemeldungen auf einen bestimmten Client eingestellt werden, dessen WLAN-MAC-Adresse hier eingetragen wird.

**SNMP-ID:** 2.12.103

**Pfad Telnet:** /Setup/WLAN

**Mögliche Werte:**

- max. 12 hexadezimale Zeichen

**Default:** 000000000000

**Besondere Werte:** 000000000000: Deaktiviert diese Funktion und gibt die Tracemeldungen von allen Clients aus.

## 2.12.116 Trace-Pakete

Ähnlich wie bei der Trace-MAC und der Trace-Stufe lassen sich die Ausgaben im WLAN-DATA-Traces anhand des Typs der empfangenen bzw. gesendeten Pakete einschränken, z. B. Management (Authenticate, Association, Action, Probe-Request/Response), Control (z. B. Powersave-Poll), EAPOL (802.1x-Verhandlung, WPA-Key-Handshake).

**SNMP-ID:** 2.12.116

**Pfad Telnet:** /Setup/WLAN

**Mögliche Werte:**

- Einer oder mehrere Werte aus Management, Control, Daten, EAPOL, Alle

**Default:** Alle

## 2.12.110 Trace-Stufe

Für den WLAN-Data-Trace kann die Ausgabe von Tracemeldungen auf einen bestimmten Inhalt beschränkt werden. Die Meldungen werden dazu in Form einer Bit-Maske eingetragen.

**SNMP-ID:** 2.12.110

**Pfad Telnet:** /Setup/WLAN

**Mögliche Werte:**

- 0 bis 255.
- 0: nur die Meldung, dass ein Paket überhaupt empfangen/gesendet wurde
- 1: zusätzlich die physikalischen Parameter der Pakete /Datenrate, Signalstärke...)
- 2: zusätzlich der MAC-Header
- 3: zusätzlich der Layer3-Header (z. B. IP/IPX)
- 4: zusätzlich der Layer4-Header (TCP, UDP...)
- 5: zusätzlich die TCP/UDP-Payload

**Default:** 255

## 2.12.27 Ueberwachung-Stationen

Besonders bei öffentlichen WLAN-Zugriffspunkten (Public Spots) ist es für die Abrechnung der Nutzungsgebühren erforderlich, nicht mehr aktive Stationen zu erkennen. Dazu kann der Access Point zur Überwachung in regelmäßigen Abständen Pakete an die eingebuchten Stationen schicken. Kommen von einer Station keine Antworten mehr auf diese Pakete, wird sie als nicht mehr aktiv an das Abrechnungssystem gemeldet.

**SNMP-ID:** 2.12.27

**Pfad Telnet:** /Setup/WLAN

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

## 2.12.8 Zugriffsmodus

Um den Datenverkehr zwischen dem Wireless-LAN und Ihrem lokalen Netz einzuschränken, können Sie bestimmte Stationen von der Übertragung ausschließen oder nur bestimmte Stationen gezielt freischalten.

**SNMP-ID:** 2.12.8

**Pfad Telnet:** /Setup/WLAN

**Mögliche Werte:**

- Daten von den aufgeführten Stationen ausfiltern, alle anderen Stationen übertragen
- Daten von den aufgeführten Stationen übertragen, alle anderen über RADIUS authentifizieren oder ausfiltern

**Default:** Daten von den aufgeführten Stationen ausfiltern, alle anderen Stationen übertragen

## 2.12.7 Zugangs-Liste

Um den Datenverkehr zwischen dem Wireless-LAN und Ihrem lokalen Netz einzuschränken, können Sie bestimmte Stationen von der Übertragung ausschließen oder nur bestimmte Stationen gezielt freischalten.

**SNMP-ID:** 2.12.7

**Pfad Telnet:** /Setup/WLAN

### 2.12.7.1 MAC-Adresse

Geben Sie hier die MAC-Adresse einer Station ein.

**SNMP-ID:** 2.12.7.1

**Pfad Telnet:** /Setup/WLAN/Zugangs-Liste

**Mögliche Werte:**

- Gültige MAC-Adresse

**Default:** Leer

Jede Netzwerkkarte hat eine eigene, weltweit eindeutige MAC-Adresse. Diese Adresse ist eine 12-stellige Hexadezimalzahl (zum Beispiel 00A057010203). Sie finden diese Adresse meistens als Aufdruck auf der Netzwerkkarte selbst.

### 2.12.7.2 Name

Sie können zu jeder Station einen beliebigen Namen und einen Kommentar eingeben.

Dies ermöglicht Ihnen eine einfachere Zuordnung der MAC-Adressen zu bestimmten Stationen oder Benutzern.

**SNMP-ID:** 2.12.7.2

**Pfad Telnet:** /Setup/WLAN/Zugangs-Liste

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

### 2.12.7.3 Kommentar

Kommentar zu diesem Eintrag

**SNMP-ID:** 2.12.7.3

**Pfad Telnet:** /Setup/WLAN/Zugangs-Liste

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

### 2.12.7.4 WPA-Passphrase

Hier können Sie optional für jede physikalische Adresse (MAC) eine separate Passphrase eintragen, die in den 802.11i/WPA/AES-PSK gesicherten Netzwerken benutzt wird. Ohne die Angabe einer gesonderten Passphrase für diese MAC-Adresse werden die im Bereich '802.11i/WEP' für jedes logische Wireless-LAN-Netzwerk hinterlegten Passphrases verwendet.

**SNMP-ID:** 2.12.7.4

**Pfad Telnet:** /Setup/WLAN/Zugangs-Liste

**Mögliche Werte:**

- ASCII-Zeichenkette mit einer Lange von 8 bis 63 Zeichen

**Default:** Leer

Bei WEP gesicherten Netzwerken hat dieses Feld keine Bedeutung.

Verwenden Sie als Passphrase zufällige Zeichenketten von mindestens 22 Zeichen Länge, was einer kryptographischen Stärke von 128 Bit entspricht.

### 2.12.7.5 Tx-Limit

Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients.

Ein Client übermittelt seine eigene Einstellung bei der Anmeldung an die Basisstation. Diese bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

**SNMP-ID:** 2.12.7.5

**Pfad Telnet:** /Setup/WLAN/Zugangs-Liste

**Mögliche Werte:**

- 0 bis 4294967296 (2^32)

**Default:** 0

**Besondere Werte:** 0: keine Begrenzung

Die Bedeutung der Werte Rx und Tx ist abhängig von der Betriebsart des Gerätes. In diesem Fall als Access Point steht Rx für „Daten senden“ und Tx für „Daten empfangen“.

### 2.12.7.6 Rx-Limit

Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients.

Ein Client übermittelt seine eigene Einstellung bei der Anmeldung an die Basisstation. Diese bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

**SNMP-ID:** 2.12.7.6

**Pfad Telnet:** /Setup/WLAN/Zugangs-Liste

**Mögliche Werte:**

- 0 bis 4 294 967 296 (2^32)

**Default:** 0

**Besondere Werte:** 0: keine Begrenzung

Die Bedeutung der Werte Rx und Tx ist abhängig von der Betriebsart des Gerätes. In diesem Fall als Access Point steht Rx für „Daten senden“ und Tx für „Daten empfangen“.

### 2.12.7.7 VLAN-Id

Diese VLAN-ID wird Paketen zugewiesen, die von dem Client mit der eingetragenen MAC-Adresse empfangen wurden.

**SNMP-ID:** 2.12.7.7

**Pfad Telnet:** /Setup/WLAN/Zugangs-Liste

**Mögliche Werte:**

- 0 bis 4096

**Default:** 0

## 2.12.29 RADIUS-Zugriffspruefung

Dieses Menü enthält die Einstellungen für die RADIUS-Zugriffsprüfung

**SNMP-ID:** 2.12.29

**Pfad Telnet:** /Setup/WLAN

### 2.12.29.7 Antwort-Lebenszeit

Mit diesem Wert definieren Sie die Lebensdauer einer im Gerät gespeicherten, abgelehnten MAC-Prüfung über den RADIUS-Server.

Wenn zur Prüfung der MAC-Adressen der WLAN-Clients ein RADIUS-Server eingesetzt wird, sendet das Gerät alle Verbindungsanfragen von WLAN-Clients an den RADIUS-Server weiter. Ist eine MAC-Adresse in diesem RADIUS-Server gesperrt, dann wird die ablehnende Antwort des RADIUS-Servers für die hier eingestellte Zeit im Gerät zwischengespeichert. So wird verhindert, dass das Gerät die wiederholten Anfragen einer gesperrten MAC-Adresse nicht immer wieder an den RADIUS-Server weitergeleitet.

**Pfad Telnet:** /Setup/WLAN/RADIUS-Zugriffspruefung

**Mögliche Werte:**

- maximal 10 numerische Zeichen im Bereich von 0 bis 4294967295 (2^32-1)

**Default:** 15

Die aktuellen Einträge der zwischengespeicherten MAC-Adressen können Sie in der Tabelle '1.3.48 RADIUS-Cache' einsehen.

### 2.12.29.2 Auth.-Port

Port zur Kommunikation mit dem RADIUS-Server bei der Authentifizierung

**Pfad Telnet:** /Setup/WLAN/RADIUS-Zugriffspruefung

**Mögliche Werte:**

- Gültige Port-Angabe

**Default:** 1812

### 2.12.29.5 Backup-Auth.-Port

Port zur Kommunikation mit dem Backup-RADIUS-Server bei der Authentifizierung

**Pfad Telnet:** /Setup/WLAN/RADIUS-Zugriffspruefung

**Mögliche Werte:**

- Gültige Port-Angabe

**Default:** 1812

### 2.12.29.12 Backup-Loopback-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

**Pfad Telnet:** /Setup/WLAN/RADIUS-Zugriffspruefung

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LBO ... LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

**Default:** Leer

### 2.12.29.14 Backup-Protokoll

Protokoll für die Kommunikation zwischen dem Backup-RADIUS-Server und den Clients.

**Pfad Telnet:** /Setup/WLAN/RADIUS-Zugriffspruefung/Backup-Protokoll

**Mögliche Werte:**

- RADIUS
- RADSEC

**Default:** RADIUS

### 2.12.29.6 Backup-Schluessel

Kennwort für den Zugang zum Backup-RADIUS-Server

**Pfad Telnet:** /Setup/WLAN/RADIUS-Zugriffspruefung

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

### 2.12.29.4 Backup-Server-IP-Adresse

IP-Adresse des Backup-RADIUS-Servers an, mit dem die Berechtigungen von WLAN-Clients über die MAC-Adresse geprüft werden (Authentifizierung).

**Pfad Telnet:** /Setup/WLAN/RADIUS-Zugriffspruefung

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** Leer

### 2.12.29.11 Loopback-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

**Pfad Telnet:** /Setup/WLAN/RADIUS-Zugriffspruefung

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

**Default:** Leer

Wenn es eine Schnittstelle mit Namen "DMZ" gibt, dann wird deren Adresse verwendet.

### 2.12.29.8 Passwort-Quelle

Legen Sie hier fest, ob das Gerät bei der Autenthifizierung mit dem RADIUS-Server das Shared Secret oder die MAC-Adresse als Passwort einsetzt.

**Pfad Telnet:** /Setup/WLAN/RADIUS-Zugriffspruefung

**Mögliche Werte:**

- Secret
- MAC-Adresse

**Default:** Secret

### 2.12.29.13 Protokoll

Protokoll für die Kommunikation zwischen dem RADIUS-Server und den Clients.

**SNMP-ID:** 2.12.29.13

**Pfad Telnet:** /Setup/WLAN/RADIUS-Zugriffspruefung

**Mögliche Werte:**

- RADSEC
- RADIUS

**Default:** RADIUS

### 2.12.29.9 Pruef-Zyklus

Wenn Sie einen Wert größer als Null wählen, überprüft das Gerät Ihre MAC-Adresse sowohl beim Anmelden, als auch während der Verbindung im angegebenen Zyklus in Sekunden. Wenn Sie Null angeben, wird die MAC-Adresse nur beim Anmelden überprüft. Eine zyklische Überprüfung ermöglicht es dem Gerät zu erkennen, wenn sich für eine MAC-Adresse z. B. die Bandbreiten-Limits ändern. In diesem Fall bleibt der Client angemeldet und die Verbindung bleibt bestehen.

**Pfad Telnet:** /Setup/WLAN/RADIUS-Zugriffspruefung

**Mögliche Werte:**

- maximal 10 numerische Zeichen im Bereich von 0 - 4294967295 (2^32-1)

**Default:** 0

### 2.12.29.3 Schluessel

Kennwort für den Zugang zum RADIUS-Server

**Pfad Telnet:** /Setup/WLAN/RADIUS-Zugriffspruefung

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

### 2.12.29.1 Server-Adresse

IP-Adresse des RADIUS-Servers an, mit dem die Berechtigungen von WLAN-Clients über die MAC-Adresse geprüft werden (Authentifizierung).

**Pfad Telnet:** /Setup/WLAN/RADIUS-Zugriffspruefung

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** Leer

Zur Nutzung der RADIUS-Funktion für WLAN-Clients muss für den Parameter „Stationen filtern" die Option „Daten von den aufgeführten Stationen übertragen, alle anderen über RADIUS authentifizieren" ausgewählt sein. Die allgemeinen Werte für Wiederholung und Timeout müssen im RADIUS-Bereich ebenfalls konfiguriert werden.

Im RADIUS-Server müssen die WLAN-Clients folgendermaßen eingetragen sein: Der Benutzername ist die MAC-Adresse im Format AABBCC-DDEEFF. Das Passwort ist für alle Benutzer identisch mit dem Schlüssel (Shared-Secret) für den RADIUS-Server.

### 2.12.29.10 Server-Datenbank-liefern

Aktivieren Sie diese Option, wenn ein RADIUS-Server die MAC-Adressliste zur Verfügung stellt.

**Pfad Telnet:** /Setup/WLAN/RADIUS-Zugriffspruefung

**Mögliche Werte:**

- nein
- ja

**Default:** ja

## 2.12.45 RADIUS-Accounting

Die Accounting-Funktion im LANCOM kann u. a. dazu genutzt werden, das Budget von angeschlossenen WLAN-Clients zu kontrollieren. Wireless Internet Service Provider (WISPs) nutzen diese Möglichkeit teilweise zur Abrechnung ihrer Kunden. Da die Abrechnungsintervalle üblicherweise zum Monatsende wechseln, kann über eine entsprechende Aktion der Neustart aller aktuellen Accounting-Sitzungen ausgelöst werden – die eigentliche WLAN-Verbindung bleibt dabei bestehen. Mit Hilfe eines Cron-Jobs kann dieser Neustart komfortabel automatisiert werden.

**SNMP-ID:** 2.12.45

**Pfad Telnet:** /Setup/WLAN

### 2.12.45.2 Accnt.-Port

Port zur Kommunikation mit dem RADIUS-Server beim Accounting.

**SNMP-ID:** 2.12.45.2

**Pfad Telnet:** /Setup/WLAN/RADIUS-Accounting

**Mögliche Werte:**

- Gültige Port-Angabe

**Default:** 1813

### 2.12.45.9 Ausgeschlossenes-VLAN

Geben Sie hier die ID des VLANs ein, welches das Gerät vom RADIUS-Accounting ausschließen soll. Der RADIUS-Server erhält dann keine Informationen über den Verkehr dieses VLANs.

**SNMP-ID:** 2.12.45.9

**Pfad Telnet:** /Setup/WLAN/RADIUS-Accounting

**Mögliche Werte:**

- maximal 4 numerische Zeichen im Bereich von 0 bis 9999

- 0 deaktiviert diese Funktion.

**Default:** 0

### 2.12.45.5 Backup-Auth.-Port

Port zur Kommunikation mit dem Backup-RADIUS-Server beim Accounting

**SNMP-ID:** 2.12.45.5

**Pfad Telnet:** /Setup/WLAN/RADIUS-Accounting

**Mögliche Werte:**

- Gültige Port-Angabe

**Default:** 1813

### 2.12.45.11 Backup-Loopback-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

**SNMP-ID:** 2.12.45.11

**Pfad Telnet:** /Setup/WLAN/RADIUS-Accounting

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LBO ... LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

**Default:** Leer

### 2.12.45.13 Backup-Protokoll

Protokoll für die Kommunikation zwischen dem Backup-RADIUS-Server und den Clients.

**Pfad Telnet:** /Setup/WLAN/RADIUS-Accounting/Backup-Protokoll

**Mögliche Werte:**

- RADIUS
- RADSEC

**Default:** RADIUS

### 2.12.45.6 Backup-Schluessel

Kennwort für den Zugang zum Backup-RADIUS-Server

**SNMP-ID:** 2.12.45.6

**Pfad Telnet:** /Setup/WLAN/RADIUS-Accounting

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

### 2.12.45.4 Backup-Server-IP-Adresse

IP-Adresse des Backup-RADIUS-Servers an, mit dem das Accounting von WLAN-Clients durchgeführt wird.

**SNMP-ID:** 2.12.45.4

**Pfad Telnet:** /Setup/WLAN/RADIUS-Accounting

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** Leer

### 2.12.45.7 Client-Brg.-Behandlung

Konfigurieren Sie hier die Einstellungen des Gerätes zum RADIUS-Accounting, wenn das Gerät im Client-Bridge-Modus arbeitet.

**SNMP-ID:** 2.12.45.7

**Pfad Telnet:** /Setup/WLAN/RADIUS-Accounting

**Mögliche Werte:**

- Aller-Traffic: Das Gerät meldet jeglichen Verkehr an der Accounting-Server.
- Bridge-Traffic: Das Gerät meldet nur den Verkehr an den Accounting-Server, den die Client-Bridge selbst erzeugt.
- Client-Traffic: Das Gerät meldet nur den Verkehr an den Accounting-Server, den die anderen Stationen der Client-Bridge erzeugen.
- Separates-Accounting: In diesem Modus eröffnet das Gerät zwei separate Sessions beim RADIUS-Server. Eine davon nutzt das Gerät um den Verkehr der Bridge selbst zu melden. In der anderen meldet das Gerät den Verkehr der an die Bridge angeschlossenen Stationen.

**Default:** Aller-Traffic

### 2.12.45.8 Interim-Update-Periode

Geben Sie hier das Zeitintervall in Sekunden an, in dem das Gerät ein Interim-Update an den Accounting-Server sendet.

**SNMP-ID:** 2.12.45.8

**Pfad Telnet:** /Setup/WLAN/RADIUS-Accounting

**Mögliche Werte:**

- maximal 10 numerische Zeichen im Bereich von 0 bis 4289999999

**Default:** 0

### 2.12.45.10 Loopback-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

**SNMP-ID:** 2.12.45.10

**Pfad Telnet:** /Setup/WLAN/RADIUS-Accounting

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets

- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

**Default:** Leer

Wenn es eine Schnittstelle mit Namen "DMZ" gibt, dann wird deren Adresse verwendet.

### 2.12.45.14 Neustart-Accounting

Mit dieser Funktion beendet das Gerät alle aktuell laufenden WLAN-Accounting-Sessions mit einem Accounting-Stop zum RADIUS-Server. Hilfreich ist dies z. B. am Ende eines Abrechungszeitraums.

**Pfad Telnet:** /Setup/WLAN/RADIUS-Accounting/Neustart-Accounting

### 2.12.45.12 Protokoll

Protokoll für die Kommunikation zwischen dem RADIUS-Server und den Clients.

**SNMP-ID:** 2.12.45.12

**Pfad Telnet:** /Setup/WLAN/RADIUS-Accounting

**Mögliche Werte:**

- RADSEC
- RADIUS

**Default:** RADIUS

### 2.12.45.3 Schluessel

Kennwort für den Zugang zum RADIUS-Server

**SNMP-ID:** 2.12.45.3

**Pfad Telnet:** /Setup/WLAN/RADIUS-Accounting

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

### 2.12.45.1 Server-Adresse

IP-Adresse des RADIUS-Servers an, mit dem das Accounting von WLAN-Clients durchgeführt wird.

**SNMP-ID:** 2.12.45.1

**Pfad Telnet:** /Setup/WLAN/RADIUS-Accounting

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** Leer

Die allgemeinen Werte für Wiederholung und Timeout müssen im RADIUS-Bereich ebenfalls konfiguriert werden.

Im RADIUS-Server müssen die WLAN-Clients folgendermaßen eingetragen sein: Der Benutzername ist die MAC-Adresse im Format AABBCC-DDEEFF. Das Passwort ist für alle Benutzer identisch mit dem Schlüssel (Shared-Secret) für den RADIUS-Server.

## 2.12.50 Signalmittelung

Dieses Menü enthält die Einstellungen für die Signalmittelung.

**SNMP-ID:** 2.12.50

**Pfad Telnet:** /Setup/WLAN

Die Einstellungen zur Signalmittelung werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

### 2.12.50.1 Methode

Methode zur Signalmittelung.

**SNMP-ID:** 2.12.50.1

**Pfad Telnet:** /Setup/WLAN/Signalmittelung

**Mögliche Werte:**

- Standard
- Gefiltert

**Default:** Standard

Die Einstellungen zur Signalmittelung werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

### 2.12.50.2 Standard-Parameter

Dieses Menü enthält die Konfiguration der Standard-Parameter für die Signalmittelung.

**SNMP-ID:** 2.12.50.2

**Pfad Telnet:** /Setup/WLAN/Signalmittelung

Die Einstellungen zur Signalmittelung werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

#### 2.12.50.2.1 Faktor

Faktor für die Signalmittelung.

**Pfad Telnet:** /Setup/WLAN/Signalmittelung/Standard-Parameter

**Mögliche Werte:**

- maximal 3 numerische Zeichen

**Default:** 4

Die Einstellungen zur Signalmittelung werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

### 2.12.50.3 Gefilterte-Parameter

Dieses Menü enthält die Konfiguration der gefilterten Parameter für die Signalmittelung.

**SNMP-ID:** 2.12.50.3

**Pfad Telnet:** /Setup/WLAN/Signalmittelung

Die Einstellungen zur Signalmittelung werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

#### 2.12.50.3.1 Ct

Ct-Wert für die Signalmittelung.

**Pfad Telnet:** /Setup/WLAN/Signalmittelung/Gefilterte-Parameter

**Mögliche Werte:**

- maximal 10 numerische Zeichen

**Default:** 0

Die Einstellungen zur Signalmittelung werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

#### 2.12.50.3.2 Koeffizienten

In dieser Tabelle werden die Koeffizienten zum Filtern der Parameter definiert.

**Pfad Telnet:** /Setup/WLAN/Signalmittelung/Gefilterte-Parameter

Die Einstellungen zur Signalmittelung werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

##### 2.12.50.3.2.1 Index

Index des Tabelleneintrags.

**Pfad Telnet:** /Setup/WLAN/Signalmittelung/Gefilterte-Parameter/Koeffizienten

**Mögliche Werte:**

- 1 bis 24

Die Einstellungen zur Signalmittelung werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

##### 2.12.50.3.2.2 Wert

Wert für den Koeffizieten bei der Signalmittelung.

**Pfad Telnet:** /Setup/WLAN/Signalmittelung/Gefilterte-Parameter/Koeffizienten

**Mögliche Werte:**

- maximal 11 numerische Zeichen

**Default:** 0

Die Einstellungen zur Signalmittelung werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

## 2.12.51 Raten-Adaption

Dieses Menü enthält die Einstellungen für den Ratenadaptionsalgorithmus.

**SNMP-ID:**

2.12.51

**Pfad Telnet:**

**Setup** > **WLAN**

### 2.12.51.1 Methode

Sie haben die Möglichkeit, den gewünschten Ratenadaptionsalgorithmus einzustellen.

**SNMP-ID:**

2.12.51.1

**Pfad Telnet:**

**Setup** > **WLAN** > **Raten-Adaption**

**Mögliche Werte:**

Standard

Minstrel

**Default:**

Minstrel

### 2.12.51.2 Initiale Rate

Die Initiale Rate bestimmt, bei welcher Bitrate der Algorithmus beginnt die optimale Bitrate zu bestimmen.

**SNMP-ID:**

2.12.51.2

**Pfad Telnet:**

**Setup** > **WLAN** > **Raten-Adaption**

**Mögliche Werte:**

Minimum

RSSI-abhaengig

**Default:**

Minimum

### 2.12.51.3 Ministrel-Glaettungsfaktor

Der Glättungsfaktor, der bei der Neuberechnung der Nettoraten pro Bitrate nach der Methode Ministrel zum Tragen kommt.

**SNMP-ID:**

2.12.51.3

**Pfad Telnet:**

**Setup** > **WLAN** > **Raten-Adaption**

**Mögliche Werte:**

0 bis 99

**Default:**

75

### 2.12.51.4 Standard-Glaettungsfaktor

Der Glättungsfaktor, der bei der Neuberechnung der Nettoraten pro Bitrate nach der Methode Standard zum Tragen kommt.

**SNMP-ID:**

2.12.51.4

**Pfad Telnet:**

**Setup** > **WLAN** > **Raten-Adaption**

**Mögliche Werte:**

0 bis 99

**Default:**

0

## 2.12.70 VLAN-Gruppenschluessel-Abbildung

Die Tabelle enthält die Zuordnungen der VLAN-Gruppenschlüssel zu den logischen WLAN-Netzen.

**SNMP-ID:**

2.12.70

**Pfad Telnet:**

**Setup** > **WLAN** > **VLAN-Gruppenschluessel-Abbildung**

### 2.12.70.1 Netzwerk

Enthält den Namen eines im Gerät registrierten WLAN-Netzes.

**SNMP-ID:**

2.12.70.1

**Pfad Telnet:**

**Setup** > **WLAN** > **VLAN-Gruppenschluessel-Abbildung**

### 2.12.70.2 VLAN-Id

Enthält die dem logischen WLAN-Netz zugeordnete VLAN-ID.

**SNMP-ID:**

2.12.70.2

**Pfad Telnet:**

**Setup** > **WLAN** > **VLAN-Gruppenschluessel-Abbildung**

**Mögliche Werte:**

1 bis 4094

**Default:**

1

### 2.12.70.3 Gruppenschluessel-Index

Die Tabelle enthält den Gruppenschlüssel-Index.

**SNMP-ID:**

2.12.70.3

**Pfad Telnet:**

**Setup** > **WLAN** > **VLAN-Gruppenschluessel-Abbildung**

**Mögliche Werte:**

1 bis 3

## 2.12.107 Radar-Muster-Schwellwerte

In dieser Tabelle werden Grenzwerte definiert, wann die Radarerkennung eingeschaltet wird.

**SNMP-ID:** 2.12.107

**Pfad Telnet:** /Setup/WLAN

Diese Einstellungen sind relevant bei Geräten, die nach ETSI EN 301 893 Version 1.3 arbeiten. Für Geräte ab ETSI EN 301 893 Version 1.5 haben diese Einstellungen keine Bedeutung.

### 2.12.107.1 Muster-pps

Wählen Sie hier eines der vordefinierten Radarmuster, um den Schwellwert bei der Radarmustererkennung einzutragen oder zu ändern.

**Pfad Telnet:** /Setup/WLAN/Radar-Muster-Schwellwerte

**Mögliche Werte:**

- EN301893-1.2-700pps
- EN301893-1.2-1800pps
- EN301893-1.2-330pps
- EN301893-1.3-750pps
- EN301893-1.3-200pps
- EN301893-1.3-300pps
- EN301893-1.3-500pps
- EN301893-1.3-800pps
- EN301893-1.3-1000pps
- EN301893-1.3-1200pps
- EN301893-1.3-1500pps
- EN301893-1.3-1600pps
- EN301893-1.3-2000pps
- EN301893-1.3-2300pps
- EN301893-1.3-3000pps
- EN301893-1.3-3500pps
- EN301893-1.3-4000pps

- EN302502-3000pps
- EN302502-4500pps

### 2.12.107.2 Schwellwert

Der eingetragene Wert beschreibt die Genauigkeit, mit der das entsprechende Radarmuster erkannt wird.

**Pfad Telnet:** /Setup/WLAN/Radar-Muster-Schwellwerte

**Mögliche Werte:**

- maximal 10 numerische Zeichen im Bereich von 0 - 4289999999

**Defaults:**

- EN301893-1.2-700pps: 8
- EN301893-1.2-1800pps: 6
- EN301893-1.2-330pps: 15
- EN301893-1.3-750pps: 7
- EN301893-1.3-200pps: 7
- EN301893-1.3-300pps: 7
- EN301893-1.3-500pps: 7
- EN301893-1.3-800pps: 7
- EN301893-1.3-1000pps: 7
- EN301893-1.3-1200pps: 4
- EN301893-1.3-1500pps: 7
- EN301893-1.3-1600pps: 5
- EN301893-1.3-2000pps: 7
- EN301893-1.3-2300pps: 7
- EN301893-1.3-3000pps: 7
- EN301893-1.3-3500pps: 7
- EN301893-1.3-4000pps: 7
- EN302502-3000pps: 4
- EN302502-4500pps: 4

Wenn Sie die voreingestellten Werte verändern, verletzt das Gerät im Betrieb möglicherweise den Standard ETSI EN 301 893 Version 1.3.

## 2.12.109 Rausch-Offsets

In dieser Tabelle werden Korrekturfaktoren definiert, mit der die angezeigten Signalwerte angepasst werden.

**SNMP-ID:** 2.12.109

**Pfad Telnet:** /Setup/WLAN

### 2.12.109.1 Band

Auswahl des Frequenzbands für die Rauschwertanpassung.

**SNMP-ID:** 2.12.109.1

**Pfad Telnet:** /Setup/WLAN/Rausch-Offsets

**Mögliche Werte:**

- Auswahl aus den im Gerät unterstützten Frequenzbändern, z. B. 2,4 GHz oder 5 GHz

**Default:** 2,4 GHz

### 2.12.109.2 Kanal

Auswahl des Kanals für die Rauschwertanpassung.

**SNMP-ID:** 2.12.109.2

**Pfad Telnet:** /Setup/WLAN/Rausch-Offsets

**Mögliche Werte:**

- maximal 5 numerische Zeichen

**Default:** leer

### 2.12.109.3 Schnittstelle

Auswahl der WLAN-Schnittstelle für die Rauschwertanpassung.

**SNMP-ID:** 2.12.109.3

**Pfad Telnet:** /Setup/WLAN/Rausch-Offsets

**Mögliche Werte:**

- je nach Ausstattung der Hardware, z. B. WLAN-1 oder WLAN-2

**Default:** WLAN-1

### 2.12.109.4 Wert

Dieser numerische Wert wird zum aktuellen Rauschwert addiert.

**SNMP-ID:** 2.12.109.4

**Pfad Telnet:** /Setup/WLAN/Rausch-Offsets

**Mögliche Werte:**

- maximal 3 numerische Zeichen im Bereich von 0 bis 127

**Default:** 0

## 2.12.111 Rausch-Immunitaet

Hier können Sie Einstellungen für die Rausch-Immunität (Adaptive Noise Immunity - ANI) vornehmen.

**SNMP-ID:** 2.12.111

**Pfad Telnet:** /Setup/WLAN/Rausch-Immunitaet

Die Einstellungen für Rausch-Immunitaet werden in der Regel vom Treiber des WLAN-Moduls automatisch anhand der Funkfeldsituation geregelt. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

### 2.12.111.3 CCK-Schaches-Signal-Erkennungs-Schwellwert

Definieren Sie hier den Schwellwert für die Erkennung von schwachen CCK-Signalen.

**Pfad Telnet:** /Setup/WLAN/Rausch-Immunitaet/CCK-Schaches-Signal-Erkennungs-Schwellwert

**Mögliche Werte**

- Numerische Zeichen von 0 bis 255

**Default:** 255

Die Einstellungen für Rausch-Immunitaet werden in der Regel vom Treiber des WLAN-Moduls automatisch anhand der Funkfeldsituation geregelt. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

### 2.12.111.4 Fir-Step

Definieren Sie hier den Wert für den Fir-Step.

**Pfad Telnet:** /Setup/WLAN/Rausch-Immunitaet/Fir-Step

**Mögliche Werte:**

- Numerische Zeichen von 0 bis 255

**Default:** 255

Die Einstellungen für Rausch-Immunitaet werden in der Regel vom Treiber des WLAN-Moduls automatisch anhand der Funkfeldsituation geregelt. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

### 2.12.111.2 OFDM-Schwache-Signale-Erkennung

Definieren Sie hier den Schwellwert für die Erkennung von schwachen OFDM-Signalen.

**Pfad Telnet:** /Setup/WLAN/Rausch-Immunitaet/OFDM-Schwache-Signale-Erkennung

**Mögliche Werte:**

- Numerische Zeichen von 0 bis 255

**Default:** 255

Die Einstellungen für Rausch-Immunitaet werden in der Regel vom Treiber des WLAN-Moduls automatisch anhand der Funkfeldsituation geregelt. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

### 2.12.111.1 Rausch-Immunitaet

Definieren Sie hier den Schwellwert für die Rausch-Immunität.

**Pfad Telnet:** /Setup/WLAN/Rausch-Immunitaet/Rausch-Immunitaet

**Mögliche Werte:**

- Numerische Zeichen von 0 bis 255

**Default:** 255

Die Einstellungen für Rausch-Immunitaet werden in der Regel vom Treiber des WLAN-Moduls automatisch anhand der Funkfeldsituation geregelt. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

### 2.12.111.5 Spurious-Immunitaet

Definieren Sie hier den Schwellwert für die Spurious-Immunität.

**Pfad Telnet:** /Setup/WLAN/Rausch-Immunitaet/Spurious-Immunitaet

**Mögliche Werte**

- Numerische Zeichen von 0 bis 255

**Default:** 255

Die Einstellungen für Rausch-Immunitaet werden in der Regel vom Treiber des WLAN-Moduls automatisch anhand der Funkfeldsituation geregelt. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

# 2.13 LANCAPI

Die LANCAPI von LANCOM Systems ist eine spezielle Form der weit verbreiteten ISDN CAPI-Schnittstelle. CAPI steht für Common ISDN Application Programming Interface und stellt die Verbindung von ISDN-Adaptern zu Kommunikationsprogrammen her. Diese Programme wiederum stellen den Rechnern Funktionen der Bürokommunikation, wie z. B. ein Fax oder einen Anrufbeantworter, bereit.

**SNMP-ID:** 2.13

**Pfad Telnet:** /Setup

## 2.13.3 UDP-Port

Hier können Sie die UDP-Port-Nummer des LANCAPI-Servers ändern.

**SNMP-ID:** 2.13.3

**Pfad Telnet:** /Setup/LANCAPI/UDP-Port

**Mögliche Werte:** max. 5 Zeichen

**Default:** 75 (any private telephony service)

## 2.13.1 Zugangs-Liste

In dieser Tabelle können Sie Adressen oder Adressbereiche eintragen, die Zugang zu dem Server haben sollen. Wenn die Tabelle leer ist, hat automatisch jeder Zugang.

**SNMP-ID:** 2.13.1

**Pfad Telnet:** /Setup/LANCAPI/Zugangs-Liste

### 2.13.1.1 IP-Adresse

Geben Sie hier eine IP-Adresse ein, die Zugang erhalten soll.

**Pfad Telnet:** /Setup/LANCAPI/Zugangs-Liste/IP-Adresse

**Mögliche Werte:** max. 15 Zeichen

**Default:** Leer

### 2.13.1.2 IP-Netzmaske

Geben Sie hier die zugehörige Netzmaske ein.

Wenn Sie nur eine einzelne Station mit der zuvor angegebenen Adresse freischalten wollen, geben Sie **255.255.255.255** ein. Wenn Sie ein ganzes IP-Netz freigeben wollen, geben Sie die zugehörige Netzmaske ein.

**Pfad Telnet:** /Setup/LANCAPI/Zugangs-Liste/IP-Netzmaske

**Mögliche Werte:** max. 15 Zeichen

**Default:** Leer

### 2.13.1.3 Rtg-Tag

Wenn sie ein Routing-Tag für diese Zugriffs-Regel angeben, so werden nur solche Pakete angenommen, die entweder in der Firewall mit dem gleichen Tag markiert oder über ein Netzwerk mit passendem Schnittstellen-Tag empfangen wurden. Wenn als Routing-Tag 0 angegeben ist, wird jeder Zugriff einer passenden IP-Adresse zugelassen.

**Pfad Telnet:** /Setup/LANCAPI/Zugangs-Liste/Rtg-Tag

**Mögliche Werte:** max. 5 Zeichen

**Default:** Leer

Die Verwendung von Routing-Tags macht folglich nur in Kombination mit entsprechend begleitenden Regeln in der Firewall oder getaggten Netzwerken Sinn.

## 2.13.6 Interface-Liste

Diese Liste enthält einen Eintrag für jedes Interface Ihres Gerätes. Sie können für jedes Interface einstellen, ob es für LANCAPI-Clients verfügbar sein soll und welche Rufnummern verwendet sollen.

**SNMP-ID:** 2.13.6

**Pfad Telnet:** /Setup/LANCAPI

### 2.13.6.1 lfc

Dies ist die Bezeichnung des Interface (z. B. S0-1).

**SNMP-ID:** 2.13.6.1

**Pfad Telnet:** /Setup/LANCAPI/Interface-Liste

### 2.13.6.2 Aktiv

Wählen Sie aus, ob und wie dieses Interface **für LANCAPI-Clients verfügbar** sein soll. Sie können angeben, dass über dieses Interface:

- alle/ ja
- keine/nein
- nur ankommende oder
- nur abgehende

Rufe zugelassen werden sollen.

**SNMP-ID:** 2.13.6.2

**Pfad Telnet:** /Setup/LANCAPI/Interface-Liste

### 2.13.6 EAZ-MSN(s)

Wenn der LANCAPI-Server auch ankommende Rufe entgegen nehmen soll, so geben Sie im Feld 'EAZ/MSNs' alle eigenen ISDN-Rufnummern an, auf denen die LANCAPI Anrufe entgegennehmen soll. Mehrere Rufnummern werden voneinander durch Semikola getrennt. Wenn Sie hier keine Rufnummer eingeben, nimmt die LANCAPI Anrufe an allen eigenen ISDN-Rufnummern entgegen.

**SNMP-ID:** 2.13.6.3

**Pfad Telnet:** /Setup/LANCAPI/Interface-Liste

#### 2.13.6.5 Erzw.-Out-MSN

Wenn bei einem abgehenden Ruf die eigene Rufnummer nicht gesetzt ist, dann bestimmt diese Option, dass die Rufnummer dieses Interfaces als eigene Rufnummer eingetragen wird. Aktivieren Sie diese Option, wenn Ihre Telefonanlage keine abgehenden Rufe ohne gesetzte eigene Rufnummer zulässt.

**SNMP-ID:** 2.13.6.5

**Pfad Telnet:** /Setup/LANCAPI/Interface-Liste

**Mögliche Werte:**

- ja
- nein

**Default:** nein

#### 2.13.6.6 Max-Verbindungen

Hier können Sie die maximale Anzahl der Verbindungen pro S0-Bus begrenzen (max. 3 Zeichen)

**SNMP-ID:** 2.13.6.6

**Pfad Telnet:** /Setup/LANCAPI/Interface-Liste

### 2.13.7 Prioritaeten-Liste

In dieser Tabelle definieren Sie die Prioritäten der ISDN-Schnittstellen für abgehende Rufe über die LANCAPI.

**Pfad Telnet:** /Setup/LANCAPI/Prioritaeten-Liste

#### 2.13.7.1 Ifc

Wählen Sie hier die ISDN-Schnittstelle, für welche Sie die Priorität festlegen wollen.

**Pfad Telnet:** /Setup/LANCAPI/Prioritaeten-Liste/Ifc

**Mögliche Werte:**

- Auswahl aus den im Gerät vorhandenen ISDN-Schnittstellen, z. B. S0-1

#### 2.13.7.2 Prio-ab

Wählen Sie hier die Priorität der ISDN-Schnittstelle für abgehende Rufe über die LANCAPI.

**Pfad Telnet:** /Setup/LANCAPI/Prioritaeten-Liste/Prio-ab

**Mögliche Werte:**

- P1 (hohe Priorität) bis P3 (niedrige Priorität)

**Default:** P3

## 2.14 Zeit

Dieses Menü enthält die Konfiguration der Zeit-Einstellungen im Gerät.

**SNMP-ID:** 2.14

**Pfad Telnet:** /Setup

## 2.14.2 Aktuelle-Zeit

Anzeige der aktuellen Zeit.

**SNMP-ID:** 2.14.2

**Pfad Telnet:** /Setup/Zeit

## 2.14.5 Anwahl-Versuche

Legen Sie fest, wie oft maximal versucht werden soll, die angegebene Rufnummer zum Zwecke der Zeitinitialisierung.

**SNMP-ID:** 2.14.5

**Pfad Telnet:** /Setup/Zeit

**Mögliche Werte:**

- max.3 Ziffern

**Default:** 3

## 2.14.1 Hol-Methode

Wählen Sie hier aus, ob und wie das Gerät seine interne Echtzeit-Uhr synchronisiert.

**SNMP-ID:** 2.14.1

**Pfad Telnet:** /Setup/Zeit

**Mögliche Werte:**

- keine
- ISDN
- NTP

**Default:** NTP

## 2.14.11 Sommerzeit

Die Zeitumstellung zwischen lokaler Normal- und Sommerzeit kann hier manuell vorgenommen werden oder automatisch erfolgen. Stellen Sie für eine automatische Zeitumstellung die passende Zeit-Region des Standorts Ihres Gerätes ein. Nur, wenn Ihr Gerät außerhalb der aufgeführten Zeit-Regionen steht, ist es für eine automatische Zeitumstellung notwendig, die Auswahl 'Benutzer definiert' zu treffen und in der folgenden Tabelle die Werte für die automatische Zeitumstellung anzugeben.

**SNMP-ID:** 2.14.11

**Pfad Telnet:** /Setup/Zeit

**Mögliche Werte:**

- Ja
- Nein
- Europa (EU)
- Russland
- USA
- Benutzerdefiniert

**Default:** Europa (EU)

## 2.14.13 Zeit-holen

Dieser Befehl veranlasst das Gerät sich die aktuelle Zeit von dem eingetragenen Zeitserver zu holen.

**SNMP-ID:** 2.14.13

**Pfad Telnet:** /Setup/Zeit

## 2.14.3 Zeit-Rufnummer

Geben Sie hier eine beliebige Telefonnummer ein, die das Gerät anrufen soll, um Zeitinformationen aus dem ISDN zu erhalten. Das Gerät wird unmittelbar nach dem Einschalten diese Nummer anwählen und die Verbindung anschließend sofort wieder trennen. Dabei wird von der ISDN-Vermittlungsstelle die aktuelle Zeit übermittelt.

**SNMP-ID:** 2.14.3

**Pfad Telnet:** /Setup/Zeit

**Mögliche Werte:**

- max. 39 Zeichen

**Default:** Leer

## 2.14.10 Zeitzone

Stellen Sie hier die Zeitzone Ihres Gerätestandorts ein. Die Zeitzone ist die Differenz aus der lokalen Zeit und der koordinierten Weltzeit (UTC) in Stunden. Diese Angabe ist insbesondere für das Netzwerk-Zeit-Protokoll (NTP) wichtig

**SNMP-ID:** 2.14.10

**Pfad Telnet:** /Setup/Zeit

**Mögliche Werte:**

- 0
- +1
- +2
- +3
- +4
- +5
- +6
- +7
- +8
- +9
- +10
- +11
- +12
- +13
- +14
- -1
- -2
- -3
- -4
- -5
- -6
- -7

- -8
- -9
- -10
- -11
- -12

**Default:** +1

## 2.14.12 Umstellungen-Sommerzeit

Konfigurieren Sie hier individuelle Werte für die automatischen Zeitumstellungen zwischen Normal- und Sommerzeit, wenn in der Auswahlliste für Sommerzeit-Einstellungen 'Benutzer definiert' ausgewählt ist.

**SNMP-ID:** 2.14.12

**Pfad Telnet:** /Setup/Zeit

### 2.14.12.1 Ereignis

Definiert den Anfang bzw. das Ende der Sommerzeit

**Pfad Telnet:** /Setup/Zeit/Umstellungen-Sommerzeit

### 2.14.12.2 Index

Erster oder letzter Tag des Monats, in dem die Sommerzeitumstellung ausgeführt wird.

**Pfad Telnet:** /Setup/Zeit/Umstellungen-Sommerzeit

### 2.14.12.3 Tag

Definiert an welchem wiederkehrenden Wochentag des Monats die Umstellung ausgeführt wird.

**Pfad Telnet:** /Setup/Zeit/Umstellungen-Sommerzeit

### 2.14.12.4 Monat

Definiert den Monat in dem die Umstellung ausgeführt wird.

**Pfad Telnet:** /Setup/Zeit/Umstellungen-Sommerzeit

### 2.14.12.5 Stunde

Definiert die Stunde in der die Umstellung ausgeführt wird.

**Pfad Telnet:** /Setup/Zeit/Umstellungen-Sommerzeit

### 2.14.12.6 Minute

Definiert die Minute in der die Umstellung ausgeführt wird.

**Pfad Telnet:** /Setup/Zeit/Umstellungen-Sommerzeit

### 2.14.12.7 Zeit-Typ

Zeit-Standard, z. B. UTC (Universal Time Coordinated).

**Pfad Telnet:** /Setup/Zeit/Umstellungen-Sommerzeit

## 2.14.15 Feiertage

In dieser Tabelle finden Sie die definierten Feiertage.

**SNMP-ID:** 2.14.15

**Pfad Telnet:** /Setup/Zeit/Feiertage

### 2.14.15.1 Index

Index des Eintrags, der dessen Position in der Tabelle beschreibt.

**SNMP-ID:** 2.14.15.1

**Pfad Telnet:** /Setup/Zeit/Feiertage/Index

**Mögliche Werte:**

- 0 bis 9999

**Default:** leer

### 2.14.15.2 Datum

Wenn Sie in der Least-Cost-Tabelle oder in der Zeitsteuerungs-Tabelle Einträge angelegt haben, die an Feiertagen gelten sollen, dann tragen Sie diese Tage hier ein.

**SNMP-ID:** 2.14.15.2

**Pfad Telnet:** /Setup/Zeit/Feiertage/Datum

**Mögliche Werte:**

- Gültiges Datum

**Default:** Leer

## 2.14.16 Zeitrahmen

Zeitrahmen werden verwendet, um die Gültigkeitsdauer von Content-Filter-Profilen zu definieren. Zu einem Profil kann es auch mehrere Zeilen mit unterschiedlichen Zeitrahmen geben. Dabei sollten sich die Zeitrahmen unterschiedlicher Zeilen ergänzen, d.h. wenn Sie eine ARBEITSZEIT festlegen, wollen Sie wahrscheinlich auch einen Zeitrahmen FREIZEIT festlegen, der die Zeit außerhalb der Arbeitszeit umfasst.

**SNMP-ID:** 2.14.16

**Pfad Telnet:** /Setup/Zeit

### 2.14.16.1 Name

Hier muss der Name des Zeitrahmens angegeben werden, über den er im Content-Filter-Profil referenziert wird.

**SNMP-ID:** 2.14.16.1

**Pfad Telnet:** /Setup/Zeit/Zeitrahmen

**Mögliche Werte:**

- Name eines Zeitrahmens
- maximal 31 Zeichen

**Default:** leer

### 2.14.16.2 Start

Hier kann die Startzeit (Tageszeit) angegeben werden, ab der das gewählte Profil gelten soll.

**SNMP-ID:** 2.14.16.2

**Pfad Telnet:** /Setup/Zeit/Zeitrahmen

**Mögliche Werte:**

- max. 5 Zeichen
- Format HH:MM

**Default:** 00:00

### 2.14.16.3 Stopp

Hier kann die Endzeit (Tageszeit) angegeben werden, bis zu der das gewählte Profil gelten soll.

**SNMP-ID:** 2.14.16.3

**Pfad Telnet:** /Setup/Zeit/Zeitrahmen

**Mögliche Werte:**

- max. 5 Zeichen
- Format HH:MM

**Default:** 23:59

### 2.14.16.4 Wochentage

Hier können Sie die Wochentage auswählen, an denen der Zeitrahmen gültig sein soll.

**SNMP-ID:** 2.14.16.4

**Pfad Telnet:** /Setup/Zeit/Zeitrahmen

**Mögliche Werte:**

- Montag
- Dienstag
- Mittwoch
- Donnerstag
- Freitag
- Samstag
- Sonntag
- Feiertag

**Default:** Aktiviert für Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag, Feiertag

## 2.15 LCR

Dieses Menü enthält die Konfiguration des Least-Cost-Routers.

**SNMP-ID:** 2.15

**Pfad Telnet:** /Setup

## 2.15.2 Lancapi-Nutzung

Wenn Sie diese Option aktivieren, dann werden alle Verbindungen, die von CAPI-Clients aufgebaut werden, vom Least-Cost-Routing gesteuert.

**SNMP-ID:** 2.15.2

**Pfad Telnet:** /Setup/LCR

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

## 2.15.1 Router-Nutzung

Ein Router ist eine intelligente Netzwerkkomponente; vergleichbar mit einer Poststelle, die aufgrund von logischer Zieladresse eines Paketes entscheiden kann, an welche nächste Netzwerkkomponente dieses Paket übertragen wird; kennt die gesamte Topologie des Netzes. Wenn Sie diese Option aktivieren, dann werden alle Verbindungen, die der Router aufbaut, vom Least-Cost-Routing gesteuert.

**SNMP-ID:** 2.15.1

**Pfad Telnet:** /Setup/LCR

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

## 2.15.4 Zeit-Liste

In dieser Tabelle können Sie abhängig von der Uhrzeit, dem Tag und der gewählten Vorwahl angeben, über welche Call-by-Call-Nummern ein Anruf umgeleitet werden soll.

**SNMP-ID:** 2.15.4

**Pfad Telnet:** /Setup/LCR

### 2.15.4.1 Index

Index für diesen Eintrag in der Tabelle.

**SNMP-ID:** 2.15.4.1

**Pfad Telnet:** /Setup/LCR/Zeit-Liste

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

### 2.15.4.2 Praefix

Geben Sie hier die Vorwahl oder die ersten Ziffern einer Gruppe von Vorwahlen ein, für die dieser Eintrag gelten soll. Wenn Sie beispielsweise 030 für Berlin eingeben, dann werden alle Anrufe mit dieser Vorwahl wie hier angegeben

umgeleitet. Sie können aber auch nur 03 eingeben, dann werden alle Anrufe zu Orten, deren Vorwahl mit 03 beginnt, umgeleitet.

**SNMP-ID:** 2.15.4.2

**Pfad Telnet:** /Setup/LCR/Zeit-Liste

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** leer

### 2.15.4.3 Tage

Die Tage an denen dieser Eintrag verwendet werden soll. Sie können mehrere Einträge fiir die gleiche Vorwahl anlegen, die jedoch zu verschiedenen Zeiten oder an verschiedenen Tagen gelten.

**SNMP-ID:** 2.15.4.3

**Pfad Telnet:** /Setup/LCR/Zeit-Liste

**Mögliche Werte:**

- Montag
- Dienstag
- Mittwoch
- Donnerstag
- Freitag
- Samstag
- Sonntag
- Feiertag

**Default:** leer

### 2.15.4.4 Start

Gibt den Anfang des Zeitraums an, in dem der Eintrag verwendet werden soll.

**SNMP-ID:** 2.15.4.4

**Pfad Telnet:** /Setup/LCR/Zeit-Liste

**Mögliche Werte:**

- max. 5 Zeichen

**Default:** leer

### 2.15.4.5 Stop

Gibt das Ende des Zeitraums an, in dem der Eintrag verwendet werden soll.

**SNMP-ID:** 2.15.4.5

**Pfad Telnet:** /Setup/LCR/Zeit-Liste

**Mögliche Werte:**

- max. 5 Zeichen

**Default:** leer

### 2.15.4.6 Nummernliste

Tragen Sie hier die Vorwahl des Call-by-Call Anbieters ein, über den die zu diesem Eintrag passenden Rufe umgeleitet werden sollen.

Sie können auch mehrere Vorwahlen durch Semikolon getrennt eingeben. Wenn mit der ersten Vorwahl keine Verbindung aufgebaut werden kann, dann werden anschließend die anderen Nummern nacheinander versucht.

Lassen Sie dieses Feld leer, wenn Sie die zu diesem Eintrag passenden Rufe nicht umleiten wollen.

**SNMP-ID:** 2.15.4.6

**Pfad Telnet:** /Setup/LCR/Zeit-Liste

**Mögliche Werte:**

- max. 29 Zeichen

**Default:** leer

### 2.15.4.7 Rueckfall

Automatischer Rückfall: Wenn über keine der eingetragenen Call-by-Call-Nummern eine Verbindung hergestellt werden kann, baut der Least-Cost-Router die Verbindung über Ihren regulären Telefonanbieter auf. Wenn Sie dies nicht wünschen, dann schalten Sie diese Option aus.

**SNMP-ID:** 2.15.4.7

**Pfad Telnet:** /Setup/LCR/Zeit-Liste

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

## 2.16 NetBIOS

Dieses Menü enthält die Konfiguration des NetBIOS.

**SNMP-ID:** 2.16

**Pfad Telnet:** /Setup

## 2.16.9 Abgleich

Das Gerät muss mit anderen NetBIOS-Routern von Zeit zu Zeit Routing-Informationen austauschen. Um unnötige Verbindungsaufbauten zu vermeiden, können Sie auswählen, wann dies geschehen soll.

**SNMP-ID:** 2.16.9

**Pfad Telnet:** /Setup/NetBIOS

**Mögliche Werte:**

- pBack
- Trig
- Zeit

**Default:** pBack

## 2.16.1 Aktiv

Wenn Sie diese Option aktivieren, kann der Router auch NetBIOS-Pakete gezielt an die richtigen Gegenstellen in entfernten Netzen weiterleiten. Ohne diese Option verursachen diese Pakete oft unnötige Verbindungen, da die einzelnen Rechner in einem auf NetBIOS basierenden Netzwerk (zum Beispiel Microsoft Windows Netzwerke) ständig Status-Informationen austauschen.

**SNMP-ID:** 2.16.1

**Pfad Telnet:** /Setup/NetBIOS

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

## 2.16.11 Gültigkeit

Die maximale Zeit in Minuten, für die NetBIOS-Namen gültig sind.

Ein Host registriert sich mit einem NetBIOS-Namen im Gerät. Wenn diese Zeitspanne abgelaufen ist, dann ist für den Host eine erneute Registrierung mit seinem Namen erforderlich.

**SNMP-ID:** 2.16.11

**Pfad Telnet:** /Setup/NetBIOS

**Mögliche Werte:**

- max. 10 numerische Zeichen

**Default:** 500

## 2.16.2 Scope-ID

Diese Zeichenkette hängt das Gerät in allen TCP-IP-Verbindungen über NetBIOS an den NetBIOS-Namen an.

**SNMP-ID:** 2.16.2

**Pfad Telnet:** /Setup/NetBIOS

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** leer

## 2.16.14 Suchdienst-Unterstuetzung

Windows nutzt den sog. Browser oder Suchdienst, um die Netzwerkumgebung aufzubauen. Da der Browserservice mit Broadcasts arbeitet, ist die Netzwerkumgebung in gerouteten Netzen unvollständig, wenn keine Domänen verwendet werden. Die Suchdienst-Unterstützung schließt diese Lücke, indem sie für jede lokale Arbeitsgruppe den zuständigen Masterbrowser auf die remote Seite propagiert, bzw. von der remoten Seite empfangene Masterbrowser im LAN per Broadcast propagiert. Die Liste der dem NetBIOS-Proxy bekannten Masterbrowser kann unter /Status/TCP-IP/NetBIOS/Browser-List eingesehen werden. Die Suchdienst-Unterstuetzung muß nur in Arbeitsgruppennetzen aktiviert werden. In Domänennetzen wird ohne Broadcasts gearbeitet und der Master-Browser ist immer der Domänen-Controler.

**Pfad Telnet:** /Setup/NetBIOS/Suchdienst-Untersuetzung

**Mögliche Werte:**

- ja
- nein

**Default**: ja

## 2.16.10 WAN-Update-Minuten

Wenn Sie festgelegt haben, dass Routing-Informationen in bestimmten Intervallen ausgetauscht werden sollen, dann geben Sie hier dieses Intervall in Minuten an.

**SNMP-ID:** 2.16.10

**Pfad Telnet:** /Setup/NetBIOS

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 60

## 2.16.8 Watchdogs

Manche Stationen versenden von Zeit zu Zeit Watchdog-Pakete, um zu prüfen, ob andere Stationen im Netzwerk noch erreichbar sind. Solche Watchdogs können unnötige Verbindungsaufbauten verursachen. Hier können Sie festlegen, ob das Gerät solche Watchdogs abfangen und selber beantworten soll, um diese Verbindungsaufbauten zu vermeiden.

**SNMP-ID:** 2.16.8

**Pfad Telnet:** /Setup/NetBIOS

**Mögliche Werte:**

- spoof
- route

**Default:** spoof

## 2.16.4 Gegenstellen

Geben Sie in dieser Liste die Gegenstellen ein, zu denen NetBIOS über IP übertragen werden soll. Diese Gegenstellen müssen ebenfalls in der IP-Routing-Tabelle vorhanden sein.

**SNMP-ID:** 2.16.4

**Pfad Telnet:** /Setup/NetBIOS

### 2.16.4.1 Name

Geben Sie hier den Namen einer Gegenstelle ein. Diese Gegenstelle muss ebenfalls in der Routing-Tabelle des IP- Routers vorhanden sein.

**SNMP-ID:** 2.16.4.1

**Pfad Telnet:** /Setup/NetBIOS/Gegenstellen

**Mögliche Werte:**

- max. 16 Zeichen

**Default:** leer

### 2.16.4.3 Typ

Geben Sie an, ob es sich bei der Gegenstelle auch um einen Router handelt, oder ob dies ein einzelner Rechner ist, der sich für Fernzugriff einwählt.

**SNMP-ID:** 2.16.4.3

**Pfad Telnet:** /Setup/NetBIOS/Gegenstellen

**Mögliche Werte:**

- Workstation
- Router

**Default:** Router

## 2.16.5 Gruppen-Liste

Diese Liste zeigt Ihnen alle NetBIOS-Gruppen an.

**SNMP-ID:** 2.16.5

**Pfad Telnet:** /Setup/NetBIOS

### 2.16.5.1 Gruppe/Domaene

Name der Arbeitsgruppe, der über NetBIOS übermittelt wurde.

**SNMP-ID:** 2.16.5.1

**Pfad Telnet:** /Setup/NetBIOS/Gruppen-Liste

### 2.16.5.2 Typ

NetBIOS legt eine bestimmte Menge von Servertypen fest, die durch hexadezimale Zahlen dargestellt werden. Die wichtigsten dieser Typen sind:

- Standard-Workstation 00
- Win-PopUp Dienst 03
- RAS-Server 06
- Domain Master-Browser oder PDC 1B
- Master-Browser 1D
- NetDDE Dienst 1F
- Datei- oder Druckerdienst 20
- RAS-Client 21
- Network Monitor Agent BE
- Network Monitor Utility BF

**SNMP-ID:** 2.16.5.2

**Pfad Telnet:** /Setup/NetBIOS/Gruppen-Liste

### 2.16.5.3 IP-Addresse

IP-Adresse der Station.

**SNMP-ID:** 2.16.5.3

**Pfad Telnet:** /Setup/NetBIOS/Gruppen-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

### 2.16.5.4 Gegenstelle

Name der Gegenstelle, über welche diese NetBIOS-Gruppe erreicht werden kann.

**SNMP-ID:** 2.16.5.4

**Pfad Telnet:** /Setup/NetBIOS/Gruppen-Liste

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen

### 2.16.5.5 Timeout

Gültigkeitsdauer für diesen Eintrag in Minuten.

**SNMP-ID:** 2.16.5.5

**Pfad Telnet:** /Setup/NetBIOS/Gruppen-Liste

### 2.16.5.6 Flags

Flags zur weiteren Kennzeichnung der Station oder Gruppe.

**SNMP-ID:** 2.16.5.6

**Pfad Telnet:** /Setup/NetBIOS/Gruppen-Liste

### 2.16.5.7 Netzwerkname

Name des IP-Netzwerks, in dem sich die Station befindet.

**SNMP-ID:** 2.16.5.7

**Pfad Telnet:** /Setup/NetBIOS/Gruppen-Liste

### 2.16.5.8 Rtg-Tag

Routing-Tag für diesen Eintrag.

**SNMP-ID:** 2.16.5.8

**Pfad Telnet:** /Setup/NetBIOS/Gruppen-Liste

## 2.16.6 Host Liste

Diese Liste zeigt Ihnen alle NetBIOS-Hosts an.

**SNMP-ID:** 2.16.6

**Pfad Telnet:** /Setup/NetBIOS

### 2.16.6.1 Name

Name der Station, der über NetBIOS übermittelt wurde.

**SNMP-ID:** 2.16.6.1

**Pfad Telnet:** /Setup/NetBIOS/Host-Liste

### 2.16.6.2 Typ

NetBIOS legt eine bestimmte Menge von Servertypen fest, die durch hexadezimale Zahlen dargestellt werden. Die wichtigsten dieser Typen sind:

- Standard-Workstation 00
- Win-PopUp Dienst 03
- RAS-Server 06
- Domain Master-Browser oder PDC 1B
- Master-Browser 1D
- NetDDE Dienst 1F
- Datei- oder Druckerdienst 20
- RAS-Client 21
- Network Monitor Agent BE
- Network Monitor Utility BF

**SNMP-ID:** 2.16.6.2

**Pfad Telnet:** /Setup/NetBIOS/Host-Liste

### 2.16.6.3 IP-Addresse

IP-Adresse der Station.

**SNMP-ID:** 2.16.6.3

**Pfad Telnet:** /Setup/NetBIOS/Host-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

### 2.16.6.4 Gegenstelle

Name der Gegenstelle, über welche diese Station erreicht werden kann.

**SNMP-ID:** 2.16.6.4

**Pfad Telnet:** /Setup/NetBIOS/Host-Liste

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen

### 2.16.6.5 Timeout

Gültigkeitsdauer für diesen Eintrag in Minuten.

**SNMP-ID:** 2.16.6.5

**Pfad Telnet:** /Setup/NetBIOS/Host-Liste

### 2.16.6.6 Flags

Flags zur weiteren Kennzeichnung der Station oder Gruppe.

**SNMP-ID:** 2.16.6.6

**Pfad Telnet:** /Setup/NetBIOS/Host-Liste

### 2.16.6.7 Netzwerkname

Name des IP-Netzwerks, in dem sich die Station befindet.

**SNMP-ID:** 2.16.6.7

**Pfad Telnet:** /Setup/NetBIOS/Host-Liste

### 2.16.6.8 Rtg-Tag

Routing-Tag für diesen Eintrag.

**SNMP-ID:** 2.16.6.8

**Pfad Telnet:** /Setup/NetBIOS/Host-Liste

## 2.16.7 Server-Liste

Diese Liste zeigt Ihnen alle NetBIOS-Server an.

**SNMP-ID:** 2.16.7

**Pfad Telnet:** /Setup/NetBIOS

### 2.16.7.1 Host

Zeigt den NetBIOS-Namen des Hosts.

**SNMP-ID:** 2.16.7.1

**Pfad Telnet:** /Setup/NetBIOS/Server-Liste

### 2.16.7.10 Flags

Zeigt die für den NetBIOS-Host ermittelten NetBIOS-Flags.

**SNMP-ID:** 2.16.7.10

**Pfad Telnet:** /Setup/NetBIOS/Server-Liste

### 2.16.7.11 Netzwerkname

Zeigt das IP-Netzwerk, in dem sich der NetBIOS-Host befindet.

**SNMP-ID:** 2.16.7.11

**Pfad Telnet:** /Setup/NetBIOS/Server-Liste

### 2.16.7.12 Rtg-Tag

Routing-Tag für die Verbindung zum NetBIOS-Host.

**SNMP-ID:** 2.16.7.12

**Pfad Telnet:** /Setup/NetBIOS/Server-Liste

### 2.16.7.2 Gruppe/Domaene

Zeigt die Arbeitsgruppe/Domäne, in dem sich der NetBIOS-Host befindet.

**SNMP-ID:** 2.16.7.2

**Pfad Telnet:** /Setup/NetBIOS/Server-Liste

### 2.16.7.4 IP-Addresse

Zeigt die IP-Adresse des NetBIOS-Hosts.

**SNMP-ID:** 2.16.7.4

**Pfad Telnet:** /Setup/NetBIOS/Server-Liste

### 2.16.7.5 OS-Ver.

Zeigt das Betriebssystem des NetBIOS-Hosts.

**SNMP-ID:** 2.16.7.5

**Pfad Telnet:** /Setup/NetBIOS/Server-Liste

### 2.16.7.6 SMB-Ver.

Zeigt die SMB-Version des NetBIOS-Hosts.

**SNMP-ID:** 2.16.7.6

**Pfad Telnet:** /Setup/NetBIOS/Server-Liste

### 2.16.7.7 Server-Typ

Zeigt den Servertyp des NetBIOS-Hosts.

**SNMP-ID:** 2.16.7.7

**Pfad Telnet:** /Setup/NetBIOS/Server-Liste

### 2.16.7.8 Gegenstelle

Gegenstelle, über welche der NetBIOS-Host erreicht werden kann.

**SNMP-ID:** 2.16.7.8

**Pfad Telnet:** /Setup/NetBIOS/Server-Liste

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen

### 2.16.7.9 Timeout

Zeigt die Dauer in Minuten bevor die NetBIOS-Information aktualisiert wird.

**SNMP-ID:** 2.16.7.9

**Pfad Telnet:** /Setup/NetBIOS/Server-Liste

## 2.16.12 Netzwerke

In dieser Tabelle können Sie NetBIOS Einstellungen vornehmen und auswählen für welches Netzwerk diese gelten sollen.

**SNMP-ID:** 2.16.12

**Pfad Telnet:** /Setup/NetBIOS

### 2.16.12.1 Netzwerkname

Wählen Sie hier den Netzwerknamen des Netzes aus, für das die Einstellungen gelten sollen.

**SNMP-ID:** 2.16.12.1

**Pfad Telnet:** /Setup/NetBIOS/Netzwerke

**Mögliche Werte:**

- max. 16 Zeichen

**Default:** leer

### 2.16.12.2 Aktiv

Wählen Sie hier aus, ob der NetBIOS-Proxy für das gewählte Netzwerk verwendet wird oder nicht.

**SNMP-ID:** 2.16.12.2

**Pfad Telnet:** /Setup/NetBIOS/Netzwerke

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

### 2.16.12.3 NT-Domaene

Geben Sie hier den Namen der Arbeitsgruppe ein, die von den Rechnern in Ihrem Netz verwendet wird. Wenn in Ihrem Netz mehrere Arbeitsgruppen existieren, dann reicht es, eine von diesen anzugeben.

**SNMP-ID:** 2.16.12.3

**Pfad Telnet:** /Setup/NetBIOS/Netzwerke

**Mögliche Werte:**

- max. 16 Zeichen

**Default:** leer

## 2.17 DNS

Dieses Menü enthält die Konfiguration des Domain-Name-System (DNS).

**SNMP-ID:** 2.17

**Pfad Telnet:** /Setup

## 2.17.1 Aktiv

Aktiviert oder deaktiviert DNS.

**SNMP-ID:** 2.17.1

**Pfad Telnet:** /Setup/DNS/Aktiv

**Mögliche Werte:**

- ja
- nein

**Default:** ja

## 2.17.3 DHCP-verwenden

Der DNS-Server kann die Namen der Stationen auflösen, die über DHCP eine IP-Adresse angefordert haben.

Mit diesem Schalter können Sie diese Option aktivieren.

**SNMP-ID:** 2.17.3

**Pfad Telnet:** /Setup/DNS

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

## 2.17.2 Domain

Eigene Domäne des Gerätes.

**SNMP-ID:** 2.17.2

**Pfad Telnet:** /Setup/DNS

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** intern

## 2.17.12 Domain-aufloesen

Wenn diese Option aktiviert ist, werden Anfragen nach der eigenen Domäne mit der eigenen IP-Adresse beantwortet.

**SNMP-ID:** 2.17.12

**Pfad Telnet:** /Setup/DNS

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

## 2.17.7 Gueltigkeit

Manche Computer speichern die Namen und Adressen der Stationen, die sie beim DNS-Server angefragt haben, um später schneller auf diese Informationen zugreifen zu können.

Geben Sie hier ein, wie lange diese Daten gespeichert bleiben dürfen, bevor sie ungültig werden. Danach muss der betreffende Computer die Informationen erneut anfragen.

**SNMP-ID:** 2.17.7

**Pfad Telnet:** /Setup/DNS

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 2000

## 2.17.4 NetBIOS-verw.

Der DNS-Server kann die Namen der Stationen auflösen, die dem NetBIOS-Router bekannt sind.

Mit diesem Schalter können Sie diese Option aktivieren.

**SNMP-ID:** 2.17.4

**Pfad Telnet:** /Setup/DNS

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

## 2.17.5 DNS-Liste

Tragen Sie hier Stations-Namen und die zugehörigen IP-Adressen ein.

**SNMP-ID:** 2.17.5

**Pfad Telnet:** /Setup/DNS

### 2.17.5.1 Rechnername

Tragen Sie hier den Namen einer Station ein.

Wenn Sie beispielsweise einen Rechner mit dem Namen myhost haben und der Name Ihrer Domäne myhome.intern lautet, dann müssen Sie hier als Stationsnamen myhost.myhome.intern eingeben.

**SNMP-ID:** 2.17.5.1

**Pfad Telnet:** /Setup/DNS/DNS-Liste

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

### 2.17.5.2 IP-Adresse

Tragen Sie hier die IP-Adresse der Station ein.

Wenn ein Client den Namen einer Station auflösen möchte, dann schickt er eine Anfrage mit diesem Namen an den DNS-Server. Der Server beantwortet diese Anfrage mit der hier eingegebenen IP-Adresse.

**SNMP-ID:** 2.17.5.2

**Pfad Telnet:** /Setup/DNS/DNS-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

## 2.17.6 Filter-Liste

Benutzen Sie den DNS-Filter, um den Zugriff auf bestimmte Stationen oder Domänen zu unterbinden.

**SNMP-ID:** 2.17.6

**Pfad Telnet:** /Setup/DNS

### 2.17.6.1 Idx.

Index für die Filtereinträge.

**SNMP-ID:** 2.17.6.1

**Pfad Telnet:** /Setup/DNS/Filter-Liste

**Mögliche Werte:**

- max. 4 Zeichen

**Default:** Leer

### 2.17.6.2 Domain

Tragen Sie hier den Namen einer Station oder einer Domäne ein, die Sie sperren wollen. Die Zeichen '*' und '?' können als Wildcards verwendet werden.

**SNMP-ID:** 2.17.6.2

**Pfad Telnet:** /Setup/DNS/Filter-Liste

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

### 2.17.6.3 IP-Adresse

Wenn die Zugriffs-Einschränkung nur für einen bestimmten Rechner oder für ein Teilnetz gelten soll, dann geben Sie hier die IP-Adresse des Rechners bzw. des Netzes ein.

**SNMP-ID:** 2.17.6.3

**Pfad Telnet:** /Setup/DNS/Filter-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.17.6.4 Netzmaske

Wenn Sie für die Zugriffs-Einschränkung die Adresse eines Teilnetzes angegeben haben, dann müssen Sie hier die zugehörige Netzmaske eingeben.

**SNMP-ID:** 2.17.6.4

**Pfad Telnet:** /Setup/DNS/Filter-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

## 2.17.8 Dyn.-DNS-Liste

Die Dyn-DNS-Liste nimmt Namen auf die, über einen Register-Request angemeldet wurden. Das macht z. B. Windows, wenn unter den erweiterten TCP/IP-Einstellungen einer Netzwerkverbindung unter "DNS" die Optionen bei "Adressen dieser Verbindung in DNS registrieren" und "DNS-Suffix dieser Verbindung in DNS-Registrierung verwenden" aktiviert sind und sich die Station in der Domäne anmeldet.

**SNMP-ID:** 2.17.8

**Pfad Telnet:** /Setup/DNS

### 2.17.8.1 Rechnername

Name der Station, die sich über Register-Request angemeldet hat.

**SNMP-ID:** 2.17.8.1

**Pfad Telnet:** /Setup/DNS/Dyn.-DNS-Liste

### 2.17.8.2 IP-Adresse

IP-Adresse der Station, die sich über Register-Request angemeldet hat.

**SNMP-ID:** 2.17.8.2

**Pfad Telnet:** /Setup/DNS/Dyn.-DNS-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

### 2.17.8.3 Timeout

Gültigkeitsdauer für diesen Eintrag.

**SNMP-ID:** 2.17.8.3

**Pfad Telnet:** /Setup/DNS/Dyn.-DNS-Liste

## 2.17.9 DNS-Weiterleitungen

Sie können Anfragen für bestimmte Domänen explizit an bestimmte Gegenstellen weiterleiten.

**SNMP-ID:** 2.17.9

**Pfad Telnet:** /Setup/DNS

### 2.17.9.1 Domainname

Um Namen einer bestimmten Domäne von einem anderen DNS-Server auflösen zu lassen, können Sie hier die Domäne eintragen und dieser eine Gegenstelle bzw. einen DNS-Server dediziert zuweisen.

**SNMP-ID:** 2.17.9.1

**Pfad Telnet:** /Setup/DNS/DNS-Weiterleitungen

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

### 2.17.9.2 Gegenstelle

Gegenstelle, an die Anfragen für die definierte Domäne weitergeleitet werden sollen.

**SNMP-ID:** 2.17.9.2

**Pfad Telnet:** /Setup/DNS/DNS-Weiterleitungen

**Mögliche Werte:**

- max. 31 Zeichen

**Default:** Leer

## 2.17.10 Service-Location-Liste

Konfigurieren Sie hier ob und wohin bestimmte Dienste aufgelöst werden sollen.

**SNMP-ID:** 2.17.10

**Pfad Telnet:** /Setup/DNS

### 2.17.10.1 Service-Name

Definieren Sie hier welcher Dienst vom DNS wie aufgelöst werden soll.

Der Dienst-Bezeichner ist der aufzulösende Dienst nach RFC 2782.

Zur Veranschaulichung werden in folgendem Beispiel einige Einträge zur Auflösung von SIP-Diensten aufgelistet: (Dienst-ID, Stations-Name, Port)

- _sips._tcp.myhome.intern . 0
- _sip._tcp.myhome.intern myhost.myhome.intern 5060
- _sip._udp.myhome.intern [self] 5060

**Pfad Telnet:** /Setup/DNS/Service-Location-Liste

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

### 2.17.10.2 Rechnername

Der Stationsname gibt den Namen der Station an, die den angegebenen Dienst bereitstellt. Wenn Sie beispielsweise einen Rechner mit dem Namen myhost haben und der Name Ihrer Domäne myhome.intern lautet, dann müssen Sie hier als Stationsnamen myhost.myhome.intern eingeben. Der Stationsname '[self]' kann als Name angegeben werden, wenn es sich um dieses Gerät selbst handelt. Ein Punkt '.' kann angegeben werden, wenn dieser Dienst gesperrt ist und demzufolge nicht aufgelöst werden soll (In diesem Fall wird eine Angabe im nachfolgenden Port-Feld ignoriert).

**Pfad Telnet:** /Setup/DNS/Service-Location-Liste

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

### 2.17.10.3 Port

Der Dienst-Port bezeichnet die verwendete Port-Nummer des angegebenen Dienstes an der genannten Station.

**Pfad Telnet:** /Setup/DNS/Service-Location-Liste

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

## 2.17.11 Dynamische-SRV-Liste

In der Dynamic-SRV-List werden Service-Location-Records abgelegt, die das Gerät selbst verwendet. Hier trägt sich z. B. das VoIP-Modul ein.

**SNMP-ID:** 2.17.11

**Pfad Telnet:** /Setup/DNS

### 2.17.11.1 Service-Name

Name des Dienstes.

**SNMP-ID:** 2.17.11.1

**Pfad Telnet:** /Setup/DNS/Dynamische-SRV-Liste

### 2.17.11.2 Rechnername

Name der Station, die diesen Dienst anbietet.

**SNMP-ID:** 2.17.11.2

**Pfad Telnet:** /Setup/DNS/Dynamische-SRV-Liste

### 2.17.11.3 Port

Port, über den dieser Dienst angemeldet wird.

**SNMP-ID:** 2.17.11.3

**Pfad Telnet:** /Setup/DNS/Dynamische-SRV-Liste

## 2.17.13 Sub-Domains

Hier kann für jedes logische Netzwerk eine separate Domäne konfiguriert werden.

**SNMP-ID:** 2.17.13

**Pfad Telnet:** /Setup/DNS

### 2.17.13.1 Netzwerkname

IP-Netzwerk, für das eine eigene Subdomäne definiert werden soll.

**SNMP-ID:** 2.17.13.1

**Pfad Telnet:** /Setup/DNS/Sub-Domains

**Mögliche Werte:**

- Auswahl aus der Liste der definierten IP-Netzwerke.

**Default:** Leer

### 2.17.13.2 Sub-Domain

Sub-Domäne, die für das gewählte IP-Netzwerk verwendet werden soll.

**SNMP-ID:** 2.17.13.2

**Pfad Telnet:** /Setup/DNS/Sub-Domains

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

## 2.18 Accounting

Dieses Menü enthält die Konfiguration des Accounting.

**SNMP-ID:** 2.18

**Pfad Telnet:** /Setup

### 2.18.1 Aktiv

Accounting ein- oder ausschalten.

**SNMP-ID:** 2.18.1

**Pfad Telnet:** /Setup/Accounting

**Mögliche Werte:**

- Ja
- Nein

### 2.18.10 Diskriminator

Hier können Sie das Merkmal auswählen, nach dem die Accounting-Daten kumuliert werden. MAC-Adresse: Die Daten werden anhand der MAC-Adresse der Clients gesammelt. IP-Adresse: Die Daten werden anhand der IP-Adresse der Clients gesammelt. --> siehe Info

**SNMP-ID:** 2.18.10

**Pfad Telnet:** /Setup/Accounting

**Mögliche Werte:**

- MAC-Adresse
- IP-Adresse

Die Option 'IP-Adresse' kann bei wechselnden IP-Adressen, z. B. bei Verwendung eines DHCP-Servers, zu ungenauen Accounting-Daten führen. Eine Zuordnung der Daten zu Benutzern ist dann ggf. nicht exakt möglich. Auf der anderen Seite können mit dieser Einstellung die Daten von Clients separiert werden, die sich hinter einem weiteren Router befinden und daher mit der gleichen MAC-Adresse des Routers in der Accounting-Liste auftauchen.

### 2.18.6 Loeschen-Accounting-Liste

Hier haben Sie die Möglichkeit Parameter zu löschen.

**SNMP-ID:** 2.18.6

**Pfad Telnet:** /Setup/Accounting

## 2.18.3 Sortieren-nach

Wählen Sie hier aus, ob die Daten in der Accounting-Tabelle nach Verbindungszeiten oder Datenvolumen sortiert werden sollen.

**SNMP-ID:** 2.18.3

**Pfad Telnet:** /Setup/Accounting

**Mögliche Werte:**

- Zeit
- Daten

## 2.18.2 Speichern-Flashrom

Accounting-Daten im Flashspeicher ein- oder ausschalten. Wenn die Accounting-Daten im Flash gespeichert werden, gehen sie auch bei einem Stromausfall nicht verloren.

**SNMP-ID:** 2.18.2

**Pfad Telnet:** /Setup/Accounting

**Mögliche Werte:**

- Ja
- Nein

## 2.18.4 Aktuelle-User

Zeigt Ihnen eine Accounting-Liste aller aktuellen Benutzer.

**SNMP-ID:** 2.18.4

**Pfad Telnet:** /Setup/Accounting

### 2.18.4.1 Username

Zeigt den Benutzernamen an.

**SNMP-ID:** 2.18.4.1

**Pfad Telnet:** /Setup/Accounting/Aktuelle-User

### 2.18.4.3 Gegenstelle

Zeigt den Namen der Gegenstelle an.

**SNMP-ID:** 2.18.4.3

**Pfad Telnet:** /Setup/Accounting/Aktuelle-User

### 2.18.4.4 Verbindungs-Typ

Zeigt den Verbindungs-Typ an (z. B. DSL-Verbindung)

**SNMP-ID:** 2.18.4.4

**Pfad Telnet:** /Setup/Accounting/Aktuelle-User

### 2.18.4.5 Rx-KBytes

Zeigt die empfangenen Bytes an.

**SNMP-ID:** 2.18.4.5

**Pfad Telnet:** /Setup/Accounting/Aktuelle-User

### 2.18.4.6 Tx-KBytes

Zeigt die gesendeten Bytes an

**SNMP-ID:** 2.18.4.6

**Pfad Telnet:** /Setup/Accounting/Aktuelle-User

### 2.18.4.8 Gesamt-Zeit

Zeigt die Gesamtzeit der jeweiligen Verbindung an.

**SNMP-ID:** 2.18.4.8

**Pfad Telnet:** /Setup/Accounting/Aktuelle-User

### 2.18.4.9 Verbindungen

Zeigt die Anzahl der Verbindungen an.

**SNMP-ID:** 2.18.4.9

**Pfad Telnet:** /Setup/Accounting/Aktuelle-User

## 2.18.5 Accounting-Liste

In der Accounting-Tabelle werden Informationen über die Verbindungen der Clients im eigenen Netzwerk zu verschiedenen Gegenstellen mit Angabe der Verbindungszeit und der übertragenen Datenvolumen gespeichert. Mit Hilfe von Accounting-Snapshots können die Accounting-Daten zu bestimmten Zeitpunkten regelmäßig für eine weitere Auswertung festgehalten werden.

**SNMP-ID:** 2.18.5

**Pfad Telnet:** /Setup/Accounting

### 2.18.5.1 Username

Zeigt den Benutzernamen an.

**Pfad Telnet:** /Setup/Accounting/Accounting-Liste

### 2.18.5.3 Gegenstelle

Zeigt den Namen der Gegenstelle an.

**Pfad Telnet:** /Setup/Accounting/Accounting-Liste

### 2.18.5.4 Verbindungs-Typ

Zeigt den Verbindungs-Typ an (z. B. DSL-Verbindung)

**Pfad Telnet:** /Setup/Accounting/Accounting-Liste

#### 2.18.5.5 Rx-KBytes

Zeigt die empfangenen Bytes an.

**Pfad Telnet:** /Setup/Accounting/Accounting-Liste

#### 2.18.5.6 Tx-KBytes

Zeigt die gesendeten Bytes an

**Pfad Telnet:** /Setup/Accounting/Accounting-Liste

#### 2.18.5.8 Gesamt-Zeit

Zeigt die Gesamtzeit der jeweiligen Verbindung an.

**Pfad Telnet:** /Setup/Accounting/Accounting-Liste

#### 2.18.5.9 Verbindungen

Zeigt die Anzahl der Verbindungen an.

**Pfad Telnet:** /Setup/Accounting/Accounting-Liste

### 2.18.8 Zeit-Schnappschuss

Bei der Konfiguration des Snapshots wird das Interval festgelegt, in dem die Accounting-Daten in einem Snapshot zwischengespeichert werden.

**SNMP-ID:** 2.18.8

**Pfad Telnet:** /Setup/Accounting

#### 2.18.8.1 Index

Zeigt den systeminternen Index an.

**Pfad Telnet:** /Setup/Accounting/Zeit-Schnappschuss

**Default:** 1

#### 2.18.8.2 Aktiv

Zwischenspeichern der Accounting-Daten ein- oder ausschalten.

**Pfad Telnet:** /Setup/Accounting/Zeit-Schnappschuss

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

#### 2.18.8.3 Type

Hier können Sie das Intervall einstellen in dem der Zeit-Schnappschuss erstellt wird.

**Pfad Telnet:** /Setup/Accounting/Zeit-Schnappschuss

**Mögliche Werte:**

- täglich
- wöchentlich
- monatlich

**Default:** monatlich

### 2.18.8.4 Tag

Der Tag im Monat, an dem die Zwischenspeicherung vorgenommen wird. Nur beim Interval 'monatlich' von Bedeutung.

**Pfad Telnet:** /Setup/Accounting/Zeit-Schnappschuss

**Mögliche Werte:**

- 0 bis 31

**Default:** 1

### 2.18.8.5 Wochentag

Der Wochentag, an dem die Zwischenspeicherung vorgenommen wird. Nur beim Interval 'wöchentlich' von Bedeutung.

**Pfad Telnet:** /Setup/Accounting/Zeit-Schnappschuss

**Mögliche Werte:**

- 0 bis 7

**Default:** unbekannt

### 2.18.8.6 Stunde

Die Stunde, zu der die Zwischenspeicherung vorgenommen wird.

**Pfad Telnet:** /Setup/Accounting/Zeit-Schnappschuss

**Mögliche Werte:**

- 0 bis 23

**Default:** 0

### 2.18.8.7 Minute

Die Minute, zu der die Zwischenspeicherung vorgenommen wird

**Pfad Telnet:** /Setup/Accounting/Zeit-Schnappschuss

**Mögliche Werte:**

- 0 bis 59

**Default:** 0

## 2.18.9 Letzter Schnappschuss

Zeigt Ihnen den letzten Schnappschuss.

**SNMP-ID:** 2.18.9

**Pfad Telnet:** /Setup/Accounting

### 2.18.9.1 Username

Zeigt den Benutzernamen an.

**Pfad Telnet:** /Setup/Accounting/Letzter-Schnappschuss

### 2.18.9.3 Gegenstelle

Zeigt den Namen der Gegenstelle an.

**Pfad Telnet:** /Setup/Accounting/Letzter-Schnappschuss

### 2.18.9.4 Verbindungs-Typ

Zeigt den Verbindungs-Typ an (z. B. DSL-Verbindung)

**Pfad Telnet:** /Setup/Accounting/Letzter-Schnappschuss

### 2.18.9.5 Rx-KBytes

Zeigt die empfangenen Bytes an.

**Pfad Telnet:** /Setup/Accounting/Letzter-Schnappschuss

### 2.18.9.6 Tx-KBytes

Zeigt die gesendeten Bytes an

**Pfad Telnet:** /Setup/Accounting/Letzter-Schnappschuss

### 2.18.9.8 Gesamt-Zeit

Zeigt die Gesamtzeit der jeweiligen Verbindung an.

**Pfad Telnet:** /Setup/Accounting/Letzter-Schnappschuss

### 2.18.9.9 Verbindungen

Zeigt die Anzahl der Verbindungen an.

**Pfad Telnet:** /Setup/Accounting/Letzter-Schnappschuss

## 2.19 VPN

Dieses Menü enthält die Konfiguration des Virtual-Private-Network (VPN).

**SNMP-ID:** 2.19

**Pfad Telnet:** /Setup

## 2.19.11 AggrMode-IKE-Group-Default

Diese IKE-Gruppe wird für Aggressive-Mode-Verbindungen genutzt, wenn die Gegenstelle nicht anhand der IP-Adresse, sondern anhand einer später übermittelten Identität identifiziert werden kann.

**SNMP-ID:** 2.19.11

**Pfad Telnet:** /Setup/VPN

**Mögliche Werte:**

- MODP-768
- MODP-1024
- MODP-1536

**Default:** MODP-1024

## 2.19.10 AggrMode-Proposal-List-Default

Diese IKE-Proposal-Liste wird für Aggressive-Mode-Verbindungen genutzt, wenn die Gegenstelle nicht anhand der IP-Adresse, sondern anhand einer später übermittelten Identität identifiziert werden kann.

**SNMP-ID:** 2.19.10

**Pfad Telnet:** /Setup/VPN

**Mögliche Werte:**

- Auswahl aus der Liste der definierten IKE-Proposal-Listen.

**Default:** IKE_RSA_SIG

## 2.19.8 Aktiv

Schaltet das VPN-Modul ein bzw. aus.

**SNMP-ID:** 2.19.8

**Pfad Telnet:** /Setup/VPN

**Mögliche Werte:**

- Aktiviert
- Deaktiviert

**Default:** Deaktiviert

## 2.19.22 Erlaube-Entferntes-Netzwerk-Auswahl

Wenn die vereinfachte Einwahl mit Zertifikaten für ein Gerät in der Zentrale aktiviert ist, können die entfernten Router während der IKE-Verhandlung in Phase 2 selbst ein Netzwerk vorschlagen, dass für die Anbindung verwendet werden soll. Dieses Netzwerk wird z. B. bei der Einrichtung der VPN-Verbindung in den entfernten Router eingetragen. Das Gerät in der Zentrale akzeptiert das vorgeschlagene Netzwerk, wenn diese Option aktiviert ist. Darüber hinaus müssen die vom Client bei der Einwahl verwendeten Parameter mit den Defaultwerten des VPN-Routers übereinstimmen.

**SNMP-ID:** 2.19.22

**Pfad Telnet:** /Setup/VPN

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

Achten Sie bei der Konfiguration der einwählenden Gegenstellen darauf, dass jede Gegenstelle ein spezielles Netzwerk anfordert, damit es nicht zu Konflikten der Netzwerkadressen kommt.

## 2.19.25 Flexibler-ID-Vergleich

Der flexible Identitätsvergleich kann in der VPN-Konfiguration aktiviert bzw. deaktiviert werden.

**SNMP-ID:** 2.19.25

**Pfad Telnet:** /Setup/VPN

**Mögliche Werte:**

- ja
- nein

**Default:** nein

Der flexible Identitätsvergleich wird sowohl bei der Prüfung der (empfangenen) entfernten Identität als auch bei der Zertifikatsauswahl durch die lokale Identität eingesetzt.

## 2.19.15 legacy-dyn-VPN(LCOS5.0x)-support

Erlaubt den Fallback von DynVPNv2 auf DynVPNv1.

**SNMP-ID:** 2.19.15

**Pfad Telnet:** /Setup/VPN

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

## 2.19.14 MainMode-IKE-Group-Default

Diese IKE-Gruppe wird für Main-Mode-Verbindungen genutzt, wenn die Gegenstelle nicht anhand der IP-Adresse, sondern anhand einer später übermittelten Identität identifiziert werden kann.

**SNMP-ID:** 2.19.14

**Pfad Telnet:** /Setup/VPN

**Mögliche Werte:**

- MODP-768
- MODP-1024
- MODP-1536

**Default:** MODP-1024

## 2.19.13 MainMode-Proposal-List-Default

Diese IKE-Proposal-Liste wird für Main-Mode-Verbindungen genutzt, wenn die Gegenstelle nicht anhand der IP-Adresse, sondern anhand einer später übermittelten Identität identifiziert werden kann.

**SNMP-ID:** 2.19.13

**Pfad Telnet:** /Setup/VPN

**Mögliche Werte:**

- Auswahl aus der Liste der definierten IKE-Proposal-Listen.

**Default:** IKE_PRESH_KEY

## 2.19.24 Max-gleichzeitige-Verbindungen

Stellen Sie hier ein, wie viele VPN-Verbindungen das Gerät aufbauen darf.

**Pfad Telnet:** /Setup/Vpn/Max-gleichzeitige-Verbindungen

**Mögliche Werte:**

- Der Maximalwert ist durch die jeweilige Lizenz begrenzt.

**Default:** 0

Bei einem Wert von 0 darf das Gerät den durch die Lizenz begrenzten Maximalwert voll ausnutzen. Werte oberhalb der Lizenzgrenze werden ignoriert.

## 2.19.16 NAT-T-Aktiv

Aktiviert die Verwendung von NAT-Traversal. NAT Traversal überwindet die Probleme beim VPN-Verbindungsaufbau an den Endpunkten der VPN-Tunnel.

**SNMP-ID:** 2.19.16

**Pfad Telnet:** /Setup/VPN

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

NAT-T kann nur bei VPN-Verbindungen eingesetzt werden, die zur Authentifizierung ESP (Encapsulating Security Payload) verwenden. ESP berücksichtigt im Gegensatz zu AH (Authentication Header) bei der Ermittlung des Hashwertes zur Authentifizierung nicht den IP-Header der Datenpakete. Der vom Empfänger berechnete Hashwert entspricht daher dem in den Paketen eingetragenen Hashwert.

Achten Sie darauf, dass neben dem UDP-Port 500 auch der UDP-Port 4500 bei Verwendung von NAT-T in der Firewall freigeschaltet ist, wenn das LANCOM als NAT-Router zwischen den VPN-Endpunkten fungiert! Bei Verwendung des Firewall-Assistenten in LANconfig wird dieser Port automatisch freigeschaltet.

## 2.19.26 NAT-T-Port-fuer-Rekeying

Stellen Sie hier ein, ob bei einem Rekeying die IKE-Pakete an den Port 500 (nein) oder den Port 4500 (ja) geschickt werden.

**Pfad Telnet:** /Setup/Vpn/NAT-T-Port-fuer-Rekeying

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

## 2.19.20 QuickMode-PFS-Group-Default

Diese IPSec-Gruppe wird bei der vereinfachten Einwahl mit Zertifikaten genutzt.

**SNMP-ID:** 2.19.20

**Pfad Telnet:** /Setup/VPN

**Mögliche Werte:**

- Kein PFS
- MODP-768
- MODP-1024
- MODP-1536

**Default:** MODP-1024

## 2.19.19 QuickMode-Proposal-List-Default

Diese IPSec-Proposal-Liste bei der vereinfachten Einwahl mit Zertifikaten genutzt.

**SNMP-ID:** 2.19.19

**Pfad Telnet:** /Setup/VPN

**Mögliche Werte:**

- Auswahl aus der Liste der definierten IPSec-Proposal-Listen.

**Default:** ESP_TN

## 2.19.21 QuickMode-Shorthold-Zeit-Default

Diese Haltezeit wird für Verbindungen bei der vereinfachten Einwahl mit Zertifikaten genutzt.

**SNMP-ID:** 2.19.21

**Pfad Telnet:** /Setup/VPN

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

## 2.19.23 SA-Aufbau-gemeinsam

Die Basis für den Aufbau eines VPN-Tunnels zwischen zwei Netzwerken stellen die „Security Associations“ (SAs) dar. Der Aufbau der Security Associations wird normalerweise durch ein IP-Paket angestoßen, dass vom Quell- ins Zielnetz übertragen werden soll.

Der Aufbau der Security Associations wird normalerweise durch ein IP-Paket angestoßen, dass vom Quell- ins Zielnetz übertragen werden soll. Daher kann der Aufbau der Netzbeziehungen je nach Anwendung gezielt gesteuert werden.

**SNMP-ID:** 2.19.23

**Pfad Telnet:** /Setup/VPN

**Mögliche Werte:**

- Einzeln: Nur die explizit durch ein zu übertragenes Paket angesprochene SA wird aufgebaut.
- Gemeinsam: Alle im Gerät definierten SAs werden aufgebaut.
- Gemeinsam für KeepAlive: Alle definierten SAs werden aufgebaut, für deren Gegenstelle in der VPN-Verbindungsliste eine Haltezeit von '9999' eingestellt ist (Keep Alive).

**Default:** Einzeln

## 2.19.27 SSL- Encaps. erlaubt

Für den passiven Verbindungsaufbau zu einem VPN-Gerät von einer anderen VPN-Gegenstelle mit Hilfe der IPSec over HTTPS-Technologie (LANCOM-VPN-Gerät oder LANCOM Advanced VPN Client) aktivieren Sie die Option SSL-Encaps in den allgemeinen VPN-Einstellungen.

**SNMP-ID:** 2.19.27

**Pfad Telnet:** /Setup/VPN

**Mögliche Werte:**

- ja, nein

**Default:** nein

Der LANCOM Advanced VPN Client unterstützt einen automatischen Fallback auf IPSec over HTTPS. In dieser Einstellung versucht der VPN-Client zunächst eine Verbindung ohne die zusätzliche SSL-Kapselung aufzubauen. Falls diese Verbindung nicht aufgebaut werden kann, versucht das Gerät im zweiten Schritt eine Verbindung mit der zusätzlichen SSL-Kapselung aufzubauen.

## 2.19.17 Vereinfachtes-Zertifikats-RAS-Aktiv

Erlaubt die vereinfachte Einwahl mit Zertifikaten. Die Vereinfachung besteht darin, dass für ankommende Verbindungen eine gemeinsame Konfiguration vorgenommen werden kann, wenn die Zertifikate der Gegenstellen vom Herausgeber des im Gerät befindlichen Root-Zertifikats signiert sind. In diesem Fall muss keine Konfiguration pro Gegenstelle erfolgen. Die dafür nötige gemeinsame Konfiguration finden Sie bei den Einstellungen der Default-Parameter. Einzelne Gegenstellen können von dieser Funktionalitat nur ausgenommen werden, indem ihre Zertifikate mit Hilfe einer CRL (Certificate Revocation List) zurückgezogen werden.

**SNMP-ID:** 2.19.17

**Pfad Telnet:** /Setup/VPN

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

## 2.19.3 Isakmp

Dieses Menü enthält die Konfiguration des Isakmp.

**SNMP-ID:** 2.19.3

**Pfad Telnet:** /Setup/VPN

### 2.19.3.4 Timer

Diese Tabelle enthält Werte, die das Timing von IKE-Verhandlungen beeinflussen.

Die Werte werden bei jeder VPN-Vollkonfiguration (Aufsetzen aller VPN-Regeln) an den IKE-Job übergeben. Der IKE-Job liest diese Werte bei jeder Verwendung direkt aus seiner Konfiguration. Dadurch wird der Expiry-Timeout bei jeder neuen Verhandlung (inkl. Rekeying alter Verbindungen) sofort verwendet. Ebenso wird das Retry-Limit sofort verwendet, dieses sogar bei schon laufenen Wiederholungen von Verhandlungspaketen.

**SNMP-ID:** 2.19.3.4

**Pfad Telnet:** /Setup/VPN/Isakmp

#### 2.19.3.4.1 Retr-Lim

Das Retry-Limit gibt an, wie oft ein IKE-Verhandlungspaket maximal wiederholt wird, wenn keine Antwort darauf empfangen wird. Der Defaultwert ist 5. Die Zeitabstände der Wiederholungen sind derzeit nicht konfigurierbar und betragen 5, 7, 9, 11, 13, ... Sekunden. Die Gesamtdauer einer IKE-Verhandlung wird zusätzlich durch das Expiry-Limit beschränkt.

**SNMP-ID:** 2.19.3.4.1

**Pfad Telnet:** /Setup/VPN/Isakmp/Timer

**Mögliche Werte:**

- Maximal 5 Zeichen

**Default:** 5

#### 2.19.3.4.2 Retr-Tim

Diese Einstellungen sind nur aus Gründen der Kompatibilität zu früheren Firmware-Versionen enthalten. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

**SNMP-ID:** 2.19.3.4.2

**Pfad Telnet:** /Setup/VPN/Isakmp/Timer

#### 2.19.3.4.3 Retr-Tim-Usec

Diese Einstellungen sind nur aus Gründen der Kompatibilität zu früheren Firmware-Versionen enthalten. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

**SNMP-ID:** 2.19.3.4.3

**Pfad Telnet:** /Setup/VPN/Isakmp/Timer

#### 2.19.3.4.4 Retr-Tim-Max

Diese Einstellungen sind nur aus Gründen der Kompatibilität zu früheren Firmware-Versionen enthalten. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

**SNMP-ID:** 2.19.3.4.4

**Pfad Telnet:** /Setup/VPN/Isakmp/Timer

#### 2.19.3.4.5 Exp-Tim

Maximale Dauer einer IKE-Verhandlungs-Phase in Sekunden.

**SNMP-ID:** 2.19.3.4.5

**Pfad Telnet:** /Setup/VPN/Isakmp/Timer

**Mögliche Werte:**

- 0 bis 65535

**Default:** 30 Sekunden

Diese Einstellungen sind nur aus Gründen der Kompatibilität zu früheren Firmware-Versionen enthalten. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

#### 2.19.3.4.6 Idx.

Die Tabelle enthält nur eine Zeile, daher hat der Index nur den Wert '1'.

**SNMP-ID:** 2.19.3.4.6

**Pfad Telnet:** /Setup/VPN/Isakmp/Timer

## 2.19.4 Proposals

Dieses Menü enthält die Konfiguration der Proposals.

**SNMP-ID:** 2.19.4

**Pfad Telnet:** /Setup/VPN

### 2.19.4.9 IKE-Proposal-Listen

Hier können Sie IKE-Proposal-Listen anzeigen und hinzufügen.

**SNMP-ID:** 2.19.4.9

**Pfad Telnet:** /Setup/VPN/Proposals

#### 2.19.4.9.1 IKE-Proposal-Listen

Name für die Zusammenstellung von IKE-Proposals

**Pfad Telnet:** /Setup/VPN/Proposals/IKE-Proposal-Listen

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

#### 2.19.4.9.2 IKE-Proposal-1

Proposal, welches für diese Liste verwendet werden soll.

**Pfad Telnet:** /Setup/VPN/Proposals/IKE-Proposal-Listen

**Mögliche Werte:**

- Auswahl aus den definierten IKE-Proposals

**Default:** Leer

#### 2.19.4.9.3 IKE-Proposal-2

Proposal, welches für diese Liste verwendet werden soll.

**Pfad Telnet:** /Setup/VPN/Proposals/IKE-Proposal-Listen

**Mögliche Werte:**

- Auswahl aus den definierten IKE-Proposals

**Default:** Leer

#### 2.19.4.9.4 IKE-Proposal-3

Proposal, welches für diese Liste verwendet werden soll.

**Pfad Telnet:** /Setup/VPN/Proposals/IKE-Proposal-Listen

**Mögliche Werte:**

- Auswahl aus den definierten IKE-Proposals

**Default:** Leer

#### 2.19.4.9.5 IKE-Proposal-4

Proposal, welches für diese Liste verwendet werden soll.

**Pfad Telnet:** /Setup/VPN/Proposals/IKE-Proposal-Listen

**Mögliche Werte:**

- Auswahl aus den definierten IKE-Proposals

**Default:** Leer

#### 2.19.4.9.6 IKE-Proposal-5

Proposal, welches für diese Liste verwendet werden soll.

**Pfad Telnet:** /Setup/VPN/Proposals/IKE-Proposal-Listen

**Mögliche Werte:**

- Auswahl aus den definierten IKE-Proposals

**Default:** Leer

#### 2.19.4.9.7 IKE-Proposal-6

Proposal, welches für diese Liste verwendet werden soll.

**Pfad Telnet:** /Setup/VPN/Proposals/IKE-Proposal-Listen

**Mögliche Werte:**

- Auswahl aus den definierten IKE-Proposals

**Default:** Leer

#### 2.19.4.9.8 IKE-Proposal-7

Proposal, welches für diese Liste verwendet werden soll.

**Pfad Telnet:** /Setup/VPN/Proposals/IKE-Proposal-Listen

**Mögliche Werte:**

- Auswahl aus den definierten IKE-Proposals

**Default:** Leer

#### 2.19.4.9.9 IKE-Proposal-8

Proposal, welches für diese Liste verwendet werden soll.

**Pfad Telnet:** /Setup/VPN/Proposals/IKE-Proposal-Listen

**Mögliche Werte:**

- Auswahl aus den definierten IKE-Proposals

**Default:** Leer

### 2.19.4.10 IPSEC-Proposal-Listen

Kombinieren Sie hier die zuvor definierten Proposals zu Proposal-Listen.

**SNMP-ID:** 2.19.4.10

**Pfad Telnet:** /Setup/VPN/Proposals

#### 2.19.4.10.1 IPSEC-Proposal-Listen

Name für die Zusammenstellung von IPSec-Proposals

**Pfad Telnet:** /Setup/VPN/Proposals/IPSEC-Proposal-Listen

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

#### 2.19.4.10.2 IPSEC-Proposal-1

Proposal, welches für diese Liste verwendet werden soll.

**Pfad Telnet:** /Setup/VPN/Proposals/IPSEC-Proposal-Listen

**Mögliche Werte:**

- Auswahl aus den definierten IPSec-Proposals

**Default:** Leer

#### 2.19.4.10.3 IPSEC-Proposal-2

Proposal, welches für diese Liste verwendet werden soll.

**Pfad Telnet:** /Setup/VPN/Proposals/IPSEC-Proposal-Listen

**Mögliche Werte:**

- Auswahl aus den definierten IPSec-Proposals

**Default:** Leer

#### 2.19.4.10.4 IPSEC-Proposal-3

Proposal, welches für diese Liste verwendet werden soll.

**Pfad Telnet:** /Setup/VPN/Proposals/IPSEC-Proposal-Listen

**Mögliche Werte:**

- Auswahl aus den definierten IPSec-Proposals

**Default:** Leer

#### 2.19.4.10.5 IPSEC-Proposal-4

Proposal, welches für diese Liste verwendet werden soll.

**Pfad Telnet:** /Setup/VPN/Proposals/IPSEC-Proposal-Listen

**Mögliche Werte:**

- Auswahl aus den definierten IPSec-Proposals

**Default:** Leer

#### 2.19.4.10.6 IPSEC-Proposal-5

Proposal, welches für diese Liste verwendet werden soll.

**Pfad Telnet:** /Setup/VPN/Proposals/IPSEC-Proposal-Listen

**Mögliche Werte:**

- Auswahl aus den definierten IPSec-Proposals

**Default:** Leer

#### 2.19.4.10.7 IPSEC-Proposal-6

Proposal, welches für diese Liste verwendet werden soll.

**Pfad Telnet:** /Setup/VPN/Proposals/IPSEC-Proposal-Listen

**Mögliche Werte:**

- Auswahl aus den definierten IPSec-Proposals

**Default:** Leer

#### 2.19.4.10.8 IPSEC-Proposal-7

Proposal, welches für diese Liste verwendet werden soll.

**Pfad Telnet:** /Setup/VPN/Proposals/IPSEC-Proposal-Listen

**Mögliche Werte:**

- Auswahl aus den definierten IPSec-Proposals

**Default:** Leer

#### 2.19.4.10.9 IPSEC-Proposal-8

Proposal, welches für diese Liste verwendet werden soll.

**Pfad Telnet:** /Setup/VPN/Proposals/IPSEC-Proposal-Listen

**Mögliche Werte:**

- Auswahl aus den definierten IPSec-Proposals

**Default:** Leer

### 2.19.4.11 IKE

In dieser Tabelle können Sie Proposals zur Verwaltung der SA-Aushandlung definieren.

**SNMP-ID:** 2.19.4.11

**Pfad Telnet:** /Setup/VPN/Proposals

#### 2.19.4.11.1 Name

Name für die Kombination von IKE-Parametern, die als Proposal verwendet werden soll.

**SNMP-ID:** 2.19.4.11.1

**Pfad Telnet:** /Setup/VPN/Proposals/IKE

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

Der Internet Key Exchange (IKE) ist ein Authentisierungs- und Schlüsselaustauschprotokoll.

#### 2.19.4.11.2 IKE-Crypt-Alg

Verschlüsselungsalgorithmus für dieses Proposal

**SNMP-ID:** 2.19.4.11.2

**Pfad Telnet:** /Setup/VPN/Proposals/IKE

**Mögliche Werte:**

- AES
- Blowfish
- CAST128
- 3DES
- DES
- NULL

**Default:** AES-CBC

#### 2.19.4.11.3 IKE-Crypt-Keylen

Schlüssellänge für dieses Proposal

**SNMP-ID:** 2.19.4.11.3

**Pfad Telnet:** /Setup/VPN/Proposals/IKE

**Mögliche Werte:**

- 0 bis 65535

**Default:** 128

#### 2.19.4.11.4 IKE-Auth-Alg

Hash-Verfahren zur Abbildung der Verschlüsselung

**SNMP-ID:** 2.19.4.11.4

**Pfad Telnet:** /Setup/VPN/Proposals/IKE

**Mögliche Werte:**

- MD5
- SHA1

**Default:** MD5

#### 2.19.4.11.5 IKE-Auth-Mode

Authentifizierungsverfahren für dieses Proposal

**SNMP-ID:** 2.19.4.11.5

**Pfad Telnet:** /Setup/VPN/Proposals/IKE

**Mögliche Werte:**

- Preshared Key: Beim symmetrischen PSK-Verfahren muss der verwendete Schlüssel vorher beiden Seiten bekannt sein.
- RSA-Signature: Asymmetrisches Verfahren mit privatem und öffentlichem Schlüssel, benannt nach Rivest, Shamir Adleman.

**Default:** Preshared Key

#### 2.19.4.11.6 Lifetime-Sec

Gültigkeit der mit diesem Proposal ausgehandelten Verbindungen in Bezug auf die Verbindungsdauer.

**SNMP-ID:** 2.19.4.11.6

**Pfad Telnet:** /Setup/VPN/Proposals/IKE

**Mögliche Werte:**

- 0 bis 65535

**Default:** 8000 Sekunden

**Besondere Werte:** 0: Keine Einschränkung der Verbindungszeit.

#### 2.19.4.11.7 Lifetime-KB

Gültigkeit der mit diesem Proposal ausgehandelten Verbindungen in Bezug auf die übertragene Datenmenge.

**SNMP-ID:** 2.19.4.11.7

**Pfad Telnet:** /Setup/VPN/Proposals/IKE

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0 kBytes

**Besondere Werte:** 0: Keine Einschränkung des Datenvolumens

### 2.19.4.12 IPSEC

Hier können Sie Vorgaben für Verschlüsselung, Authentifizierung oder Kompression festlegen.

**SNMP-ID:** 2.19.4.12

**Pfad Telnet:** /Setup/VPN/Proposals

#### 2.19.4.12.1 Name

Name für die Kombination von IPSec-Parametern, die als Proposal verwendet werden soll.

**SNMP-ID:** 2.19.4.12.1

**Pfad Telnet:** /Setup/VPN/Proposals/IPSEC

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

IPSec steht für „IP Security Protocol“ und ist ursprünglich der Name einer Arbeitsgruppe innerhalb des Interessenverbandes IETF, der Internet Engineering Task Force. Diese Arbeitsgruppe hat über die Jahre ein Rahmenwerk für ein gesichertes IP-Protokoll entwickelt, das heute allgemein als IPSec bezeichnet wird.

#### 2.19.4.12.2 Encaps-Mode

Auswahl des Verbindungsmodus

**SNMP-ID:** 2.19.4.12.2

**Pfad Telnet:** /Setup/VPN/Proposals/IPSEC

**Mögliche Werte:**

- Transport: Im Transport-Modus wird der IP-Header des ursprünglichen Paketes unverändert gelassen und es werden ESP-Header, die verschlüsselten Daten und die beiden Trailer eingefügt. Der IP-Header enthält die unveränderte IP-Adresse. Der Transport-Modus kann daher nur zwischen zwei Endpunkten verwendet werden, beispielsweise zur Fernkonfiguration eines Routers. Zur Kopplung von Netzen über das Internet kann der Transport-Modus nicht eingesetzt werden – hier wird ein neuer IP-Header mit der öffentlichen IP-Adresse des Gegenübers benötigt. In diesen Fällen kommt ESP im Tunnel-Modus zum Einsatz.
- Tunnel: Im Tunnel-Modus wird das gesamte Paket inkl. dem ursprünglichen IP-Header am Tunnel-Eingang verschlüsselt und authentifiziert und mit ESP-Header und -Trailern versehen. Diesem neuen Paket wird ein neuer IP-Header vorangesetzt, diesmal mit der öffentlichen IP-Adresse des Empfängers am Tunnel-Ende.

**Default:** Tunnel

#### 2.19.4.12.3 ESP-Crypt-Alg

Verschlüsselungsalgorithmus für dieses Proposal

**SNMP-ID:** 2.19.4.12.3

**Pfad Telnet:** /Setup/VPN/Proposals/IPSEC

**Mögliche Werte:**

- AES
- Blowfish
- CAST128
- 3DES
- DES
- NULL

**Default:** AES-CBC

#### 2.19.4.12.4 ESP-Crypt-Keylen

Schlüssellänge für dieses Proposal

**SNMP-ID:** 2.19.4.12.4

**Pfad Telnet:** /Setup/VPN/Proposals/IPSEC

**Mögliche Werte:**

- 0 bis 65535

**Default:** 128

#### 2.19.4.12.5 ESP-Auth-Alg

ESP-Authentifizierungsverfahren für dieses Proposal

**SNMP-ID:** 2.19.4.12.5

**Pfad Telnet:** /Setup/VPN/Proposals/IPSEC

**Mögliche Werte:**

- HMAC-MD5
- HMAC-SHA1
- Keine Authentifizierung

**Default:** HMAC-MD5

#### 2.19.4.12.6 AH-Auth-Alg

AH-Authentifizierungsverfahren für dieses Proposal

**SNMP-ID:** 2.19.4.12.6

**Pfad Telnet:** /Setup/VPN/Proposals/IPSEC

**Mögliche Werte:**

- HMAC-MD5
- HMAC-SHA1
- Kein AH

**Default:** Kein AH

#### 2.19.4.12.7 IPCOMP-Alg

Kompressionsverfahren für dieses Proposal

**SNMP-ID:** 2.19.4.12.7

**Pfad Telnet:** /Setup/VPN/Proposals/IPSEC

**Mögliche Werte:**

- Kein IPCOMP
- Deflate
- LZS

**Default:** Kein IPCOMP

#### 2.19.4.12.8 Lifetime-Sec

Gültigkeit der mit diesem Proposal ausgehandelten Verbindungen in Bezug auf die Verbindungsdauer.

**SNMP-ID:** 2.19.4.12.8

**Pfad Telnet:** /Setup/VPN/Proposals/IPSEC

**Mögliche Werte:**

- 0 bis 65535

**Default:** 8000 Sekunden

**Besondere Werte:** 0: Keine Einschränkung der Verbindungszeit.

#### 2.19.4.12.9 Lifetime-KB

Gültigkeit der mit diesem Proposal ausgehandelten Verbindungen in Bezug auf die übertragene Datenmenge.

**SNMP-ID:** 2.19.4.12.9

**Pfad Telnet:** /Setup/VPN/Proposals/IPSEC

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0 kBytes

**Besondere Werte:** 0: Keine Einschränkung des Datenvolumens

## 2.19.5 Zertifikate-Schluessel

Dieses Menü enthält die Konfiguration der Zertifikate und Schlüssel.

**SNMP-ID:** 2.19.5

**Pfad Telnet:** /Setup/VPN

### 2.19.5.3 IKE-Keys

Hier werden die gemeinsamen Schlüssel für die Authentifizierung nach dem Preshared-Key-Verfahren und die Identitäten für die Authentifizierung nach dem Preshared-Key- und dem RSA-Signature-Verfahren eingegeben.

**Pfad Telnet:** /Setup/VPN/Zertifikate-Schluessel

#### 2.19.5.3.1 Name

Name für die Kombination von Identitäten und Schlüsseln

**Pfad Telnet:** /Setup/VPN/Zertifikate-Schluessel/IKE-Keys

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

#### 2.19.5.3.2 Remote-Identity

Entfernte Identität, für die der eingetragene Schlüssel gelten soll.

**Pfad Telnet:** /Setup/VPN/Zertifikate-Schluessel/IKE-Keys

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

#### 2.19.5.3.3 Shared-Sec

Schlüssel, der für diese Kombination gelten soll.

**Pfad Telnet:** /Setup/VPN/Zertifikate-Schluessel/IKE-Keys

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

#### 2.19.5.3.4 Shared-Sec-File

[obsolet, nicht verwendet: Datei mit PSK]

**Pfad Telnet:** /Setup/VPN/Zertifikate-Schluessel/IKE-Keys

#### 2.19.5.3.5 Remote-ID-Type

Typ der entfernten Identität, für die der eingetragene Schlüssel gelten soll.

**Pfad Telnet:** /Setup/VPN/Zertifikate-Schluessel/IKE-Keys

**Mögliche Werte:**

- Keine Identität
- IP-Adresse
- Domänen-Name (FQDN)
- E-Mail-Adresse (FQUN)
- ASN.1-Distinguished Name

**Default:** Keine Identität

#### 2.19.5.3.6 Local-ID-Type

Typ der lokalen Identität, für die der eingetragene Schlüssel gelten soll.

**Pfad Telnet:** /Setup/VPN/Zertifikate-Schluessel/IKE-Keys

**Mögliche Werte:**

- Keine Identität
- IP-Adresse
- Domänen-Name (FQDN)
- E-Mail-Adresse (FQUN)
- ASN.1-Distinguished Name

**Default:** Keine Identität

#### 2.19.5.3.7 Local-Identity

Lokale Identität, für die der eingetragene Schlüssel gelten soll.

**Pfad Telnet:** /Setup/VPN/Zertifikate-Schluessel/IKE-Keys

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

## 2.19.7 Layer

Definieren Sie hier weitere Parameter für die einzelnen VPN-Verbindungen.

**SNMP-ID:** 2.19.7

**Pfad Telnet:** /Setup/VPN

### 2.19.7.1 Name

Name für die Kombination der Verbindungs-Parameter

**SNMP-ID:** 2.19.7.1

**Pfad Telnet:** /Setup/VPN/Layer

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

### 2.19.7.3 PFS-Grp

Perfect Forward Secrecy (PFS) ist ein Sicherheitsmerkmal von Verschlüsselungsverfahren. Die PFS-Gruppe gibt an, wie lang der Diffie-Hellmann Key ist, der zur Verschlüsselung der IKE-Verhandlung verwendet wird.

**SNMP-ID:** 2.19.7.3

**Pfad Telnet:** /Setup/VPN/Layer

**Mögliche Werte:**

- Kein PFS
- MODP-768
- MODP-1024

- MODP-1536

**Default:** MODP-1024

### 2.19.7.4 IKE-Grp

Die IKE-Gruppe gibt an, wie lang der Diffie-Hellmann Key ist, der zur Verschlüsselung der IKE-Verhandlung verwendet wird.

**SNMP-ID:** 2.19.7.4

**Pfad Telnet:** /Setup/VPN/Layer

**Mögliche Werte:**

- MODP-768
- MODP-1024
- MODP-1536

**Default:** MODP-1024

### 2.19.7.5 IKE-Prop-Liste

IKE-Proposal-Liste für diese Verbindung.

**SNMP-ID:** 2.19.7.5

**Pfad Telnet:** /Setup/VPN/Layer

**Mögliche Werte:**

- Auswahl aus der Liste der definierten IKE-Proposal-Listen.

**Default:** Leer

### 2.19.7.6 IPSEC-Prop-Liste

IKE-Schlüssel für diese Verbindung.

**SNMP-ID:** 2.19.7.6

**Pfad Telnet:** /Setup/VPN/Layer

**Mögliche Werte:**

- Auswahl aus der Liste der definierten IKE-Schlüssel.

**Default:** Leer

### 2.19.7.7 IKE-Key

IPSec-Proposal-Liste für diese Verbindung.

**SNMP-ID:** 2.19.7.7

**Pfad Telnet:** /Setup/VPN/Layer

**Mögliche Werte:**

- Auswahl aus der Liste der definierten IPSec-Proposal-Listen.

**Default:** Leer

## 2.19.9 VPN-Gegenstellen

In dieser Tabelle definieren Sie die VPN-Verbindungen, die Ihr Gerät aufbauen soll.

**SNMP-ID:** 2.19.9

**Pfad Telnet:** /Setup/VPN

### 2.19.9.1 Gegenstelle

Name der VPN-Verbindung.

**SNMP-ID:** 2.19.9.1

**Pfad Telnet:** /Setup/VPN/VPN-Gegenstellen

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen

**Default:** Leer

### 2.19.9.10 DPD-Inakt-Timeout

Die Dead Peer Detection wird bei der Einwahl von VPN-Clients in ein VPN-Gateway oder bei Verbindungen von 2 VPN-Gateways eingesetzt. Damit soll sichergestellt werden, das eine Gegenstelle ausgebucht wird, wenn die VPN-Verbindung z. B. durch kurzzeitigen Ausfall der Internetverbindung gestört wurde. Ohne eine entsprechende Leitungsüberwachung würde das VPN-Gateway den Client oder das andere VPN-Gateway weiter in der Liste der eingebuchten Gegenstellen führen. Eine erneute Einwahl der Gegenstelle würde damit verhindert, weil z. B. beim LANCOM Advanced VPN Client eine erneute Einwahl mit der gleichen Seriennummer nicht möglich ist.

Bei der Dead-Peer-Detection tauschen Gateway und Gegenstelle während der Verbindung regelmäßig „Keep-Alive"-Pakete aus. Bleiben die Antworten aus, bucht das Gateway die Gegenstelle aus und ermöglicht so nach wiederherstellen der VPN-Verbindung eine erneute Anmeldung mit der gleichen Identity. Für VPN-Clients wird die DPD-Zeit üblicherweise auf 60 Sekunden eingestellt.

**SNMP-ID:** 2.19.9.10

**Pfad Telnet:** /Setup/VPN/VPN-Gegenstellen

**Mögliche Werte:**

- 0 bis 9999 numerische Zeichen

**Default:** 0

Ohne Leitungsüberwachung würde z. B. die Einwahl eines Benutzers mit gleicher "Identity" – also gleichem Usernamen – verhindert, da der entsprechende Benutzer weiterhin in der Liste der eingebuchten Gegenstellen geführt würde.

### 2.19.9.11 IKE-CFG

Bei der Konfiguration von VPN-Einwahlzugängen kann alternativ zur festen Vergabe der IP-Adressen für die einwählenden Gegenstellen auch ein Pool von IP-Adressen angegeben werden. In den Einträgen der Verbindungsliste wird dazu der "IKE-CFG"-Modus angegeben.

**SNMP-ID:** 2.19.9.11

**Pfad Telnet:** /Setup/VPN/VPN-Gegenstellen

**Mögliche Werte:**

- Aus: Ist der IKE-CFG-Modus ausgeschaltet, werden keine IP-Adressen für die Verbindung zugewiesen. Auf beiden Seiten der VPN-Strecke muss fest konfiguriert sein, welche IP-Adressen für diese Verbindung zu verwenden sind.
- Client: In dieser Einstellung fungiert das Gerät als Client für diese VPN-Verbindung und fordert eine IP-Adresse für die Verbindung von der Gegenstelle (Server) an. Das Gerät verhält sich also so ähnlich wie ein VPN-Client.
- Server: In dieser Einstellung fungiert das Gerät als Server für diese VPN-Verbindung. Für die Zuweisung der IP-Adresse an den Client gibt es zwei Möglichkeiten:
- Wenn die Gegenstelle in der Routing-Tabelle eingetragen ist, wird ihr die dort konfigurierte IP-Adresse zugewiesen.
- Wenn die Gegenstelle nicht in der Routing-Tabelle eingetragen ist, wird eine freie IP-Adresse aus dem IP-Pool für die Einwahlzugänge entnommen.

**Default:** Aus

In der Einstellung als Server muss die Gegenstelle als IKE-CFG-Client konfiguriert sein und so vom Server eine IP-Adresse für die Verbindung anfordern. Für die Einwahl mit einem LANCOM Advanced VPN Client aktivieren Sie im Verbindungsprofil die Option "IKE Config Mode verwenden".

### 2.19.9.12 XAUTH

Aktiviert die Verwendung von XAUTH für die gewählte VPN-Gegenstelle.

**SNMP-ID:** 2.19.9.12

**Pfad Telnet:** /Setup/VPN/VPN-Gegenstellen

**Mögliche Werte:**

- Client: In der Betriebsart als XAUTH-Client startet das Gerät die erste Phase der IKE-Verhandlung (Main Mode oder Aggressive Mode) und wartet dann auf den Authentifizierungs-Request vom XAUTH-Server. Auf diesen Request antwortet der XAUTH-Client mit dem Benutzernamen und dem Kennwort aus dem Eintrag der PPP-Tabelle, in dem die PPP-Gegenstelle der hier definierten VPN-Gegenstelle entspricht. Zu der VPN-Gegenstelle muss es also eine gleichnamige PPP-Gegenstelle geben. Der in der PPP-Tabelle definierte Benutzername weicht üblicherweise von dem Gegenstellennamen ab.
- Server: In der Betriebsart als XAUTH-Server startet das Gerät nach erfolgreicher Verhandlung der ersten IKE-Verhandlung die Authentifizierung mit einem Request an den XAUTH-Client, der daraufhin mit seinem Benutzernamen und Kennwort antwortet. Der XAUTH-Server sucht den übermittelten Benutzernamen in den Gegenstellennamen der PPP-Tabelle und prüft bei Übereinstimmung das Kennwort. Der Benutzername für diesen Eintrag in der PPP-Tabelle wird nicht verwendet.
- Aus: Bei der Verbindung zu dieser Gegenstelle wird keine XAUTH-Authentifizierung durchgeführt.

**Default:** Aus

Wenn die XAUTH-Authentifizierung für eine VPN-Gegenstelle aktiviert ist, muss die Option IKE-CFG auf den gleichen Wert eingestellt werden.

### 2.19.9.13 SSL-Encaps.

Mit dieser Option aktivieren Sie die Nutzung der IPsec over HTTPS-Technologie beim aktiven Verbindungsaufbau zu dieser Gegenstelle.

**SNMP-ID:** 2.19.9.13

**Pfad Telnet:** /Setup/VPN/VPN-Gegenstellen

**Mögliche Werte:**

- ja, nein

**Default:** nein

Bitte beachten Sie, dass bei eingeschalteter IPsec over HTTPS-Option die VPN-Verbindung nur aufgebaut werden kann, wenn die Gegenstelle diese Technologie ebenfalls unterstützt und die Annahme von passiven VPN-Verbindungen mit IPsec over HTTPS bei der Gegenstelle aktiviert ist.

### 2.19.9.15 Rtg-Tag

Routing-Tags werden im LANCOM genutzt, um neben der IP-Adresse weitere Kriterien zur Auswahl der Zielroute auswerten zu können. Aus der Routing-Tabelle werden nur die Routen mit übereinstimmendem Routing-Tag verwendet. Hier kann für jede VPN-Verbindung das Routing-Tag angegeben werden, das verwendet werden soll, um die Route zum entfernten Gateway zu ermitteln.

**SNMP-ID:** 2.19.9.15

**Pfad Telnet:** /Setup/VPN/VPN-Gegenstellen

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.9.2 Extranet-Adresse

Ist hier eine IP-Adresse angegeben, werden die IP-Adressen der lokalen Stationen hinter dieser IP-Adresse maskiert. Dies ist nur für spezielle Szenarien nötig.

**SNMP-ID:** 2.19.9.2

**Pfad Telnet:** /Setup/VPN/VPN-Gegenstellen

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** Leer

### 2.19.9.4 Layer

Kombination von Verbindungs-Parametern (PFS-, IKE- und IPSec-Parameter), die für diese Verbindung verwendet werden sollen.

**SNMP-ID:** 2.19.9.4

**Pfad Telnet:** /Setup/VPN/VPN-Gegenstellen

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Verbindungs-Parameter

**Default:** Leer

### 2.19.9.5 dynamisch

LANCOM Dynamic VPN ist eine Technik, die den Aufbau von VPN-Tunneln auch zu solchen Gegenstellen ermöglicht, die keine statische, sondern nur eine dynamische IP-Adresse besitzen.

**SNMP-ID:** 2.19.9.5

**Pfad Telnet:** /Setup/VPN/VPN-Gegenstellen

**Mögliche Werte:**

- Kein dynamisches VPN
- Dynamisches VPN: Es wird eine Verbindung aufgebaut, um IP-Adressen zu übermitteln

- Dynamisches VPN: IP-Adressen werden nach Möglichkeit ohne Verbindungsaufbau übermittelt:
- Dynamisches VPN: Ein ICMP-Paket wird an die Gegenstelle gesendet um die IP-Adresse zu übermitteln
- Dynamisches VPN: Ein UDP-Paket wird an die Gegenstelle gesendet um die IP-Adresse zu übermitteln

**Default:** Kein dynamisches VPN

### 2.19.9.6 SH-Zeit

Geben Sie an, nach wieviel Sekunden die Verbindung zu dieser Gegenstelle getrennt werden soll, wenn in dieser Zeit keine Daten mehr übertragen worden sind.

**SNMP-ID:** 2.19.9.6

**Pfad Telnet:** /Setup/VPN/VPN-Gegenstellen

**Mögliche Werte:**

- 0 bis 9999

**Default:** 0

**Besondere Werte:** Der Wert 9999 sorgt für einen sofortigen Verbindungsaufbau ohne zeitliche Begrenzung.

### 2.19.9.7 IKE-Exchange

Auswahl des IKE-Exchange-Modus

**SNMP-ID:** 2.19.9.7

**Pfad Telnet:** /Setup/VPN/VPN-Gegenstellen

**Mögliche Werte:**

- Main Mode
- Aggressive Mode

**Default:** Main Mode

Beim Main Mode werden in der IKE-Verhandlungsphase deutlich mehr Nachrichten ausgetauscht als im Aggressive Mode. Der Main Mode ist daher wesentlich sicherer als der Aggressive Mode.

### 2.19.9.8 Entferntes-Gw

DNS-Name oder IP-Adresse des entfernten Gateways, über das die VPN-Verbindung aufgebaut werden soll.

**SNMP-ID:** 2.19.9.8

**Pfad Telnet:** /Setup/VPN/VPN-Gegenstellen

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

### 2.19.9.9 Regelerzegung

Ein-/Ausschalter und Art der VPN-Regelerzeugung

**SNMP-ID:** 2.19.9.9

**Pfad Telnet:** /Setup/VPN/VPN-Gegenstellen

**Mögliche Werte:**

- Aus: Es wird keine VPN-Regel für die Gegenstelle erzeugt.

- Automatisch: Automatisch erzeugte VPN-Regeln verbinden die lokalen IP-Netze mit den in der Routing-Tabelle für die Gegenstelle eingetragenen IP-Netzen.
- Manuell: VPN-Regeln werden nur für die in der Firewall-Konfiguration „manuell" angegebenen IP-Netzbeziehungen für die Gegenstelle angelegt.

**Default:** Automatisch

## 2.19.12 Zusaetzliche-Gateway-Liste

In dieser Tabelle wird für jede Gegenstelle eine Liste der möglichen Gateways angegeben.

**SNMP-ID:** 2.19.12

**Pfad Telnet:** /Setup/VPN

### 2.19.12.1 Gegenstelle

Name der VPN-Verbindung, für welche die hier definierten zusätzlichen Gateways gelten sollen.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- Auswahl aus der Liste der definierten VPN-Verbindungen.

**Default:** Leer

### 2.19.12.10 Anfangen-mit

Auswahl des Gateways, über das zuerst der Aufbau der VPN-Verrbindung versucht werden soll.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- Erstem: Beginnt mit dem ersten Eintrag in der Liste.
- Zufaelligem: Wählt zufällig einen Eintrag aus der Liste.
- Zuletzt-verwendetem: Beginnt mit dem Eintrag, über den zuletzt eine Verbindung erfolgreich aufgebaut werden konnte.

**Default:** Zuletzt-verwendetem

### 2.19.12.2 Entferntes-Gateway-1

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.11 Rtg-Tag-1

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.3 Entferntes-Gateway-2

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.12 Rtg-Tag-2

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.4 Entferntes-Gateway-3

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.13 Rtg-Tag-3

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.5 Entferntes-Gateway-4

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.14 Rtg-Tag-4

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.6 Entferntes-Gateway-5

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.15 Rtg-Tag-5

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.7 Entferntes-Gateway-6

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.16 Rtg-Tag-6

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.8 Entferntes-Gateway-7

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.17 Rtg-Tag-7

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.9 Entferntes-Gateway-8

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.18 Rtg-Tag-8

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.19 Entferntes-Gateway-9

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

### 2.19.12.27 Rtg-Tag-9

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.20 Entferntes-Gateway-10

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.28 Rtg-Tag-10

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.21 Entferntes-Gateway-11

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.29 Rtg-Tag-11

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.22 Entferntes-Gateway-12

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.30 Rtg-Tag-12

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.23 Entferntes-Gateway-13

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.31 Rtg-Tag-13

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.24 Entferntes-Gateway-14

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.32 Rtg-Tag-14

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.25 Entferntes-Gateway-15

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.33 Rtg-Tag-15

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.26 Entferntes-Gateway-16

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.34 Rtg-Tag-16

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/VPN/Zusaetzliche-Gateway-Liste

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.35 Gateway-17

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-17

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.36 Rtg-Tag-17

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-17

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.37 Gateway-18

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-18

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.38 Rtg-Tag-18

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-18

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.39 Gateway-19

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-19

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.40 Rtg-Tag-19

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-19

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.41 Gateway-20

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-20

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.42 Rtg-Tag-20

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-20

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.43 Gateway-21

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-21

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.44 Rtg-Tag-21

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-21

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.45 Gateway-22

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-22

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.46 Rtg-Tag-22

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-22

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.47 Gateway-23

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-23

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.48 Rtg-Tag-23

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-23

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.49 Gateway-24

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-24

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.50 Rtg-Tag-24

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-24

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.51 Gateway-25

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-25

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.52 Rtg-Tag-25

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-25

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.53 Gateway-26

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-26

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.54 Rtg-Tag-26

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-26

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.55 Gateway-27

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-27

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.56 Rtg-Tag-27

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-27

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.57 Gateway-28

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-28

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.58 Rtg-Tag-28

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-28

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.59 Gateway-29

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-29

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.60 Rtg-Tag-29

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-29

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.61 Gateway-30

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-30

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.62 Rtg-Tag-30

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-30

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.63 Gateway-31

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-31

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.64 Rtg-Tag-31

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-31

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

### 2.19.12.65 Gateway-32

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-32

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** Leer

### 2.19.12.66 Rtg-Tag-32

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

**Pfad Telnet:** /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-32

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

## 2.20 LAN-Bridge

Dieses Menü enthält die Einstellungen für die LAN-Bridge.

**SNMP-ID:** 2.20

**Pfad Telnet:** /Setup

## 2.20.12 Alterungs-Zeit

Wenn ein Client eine IP-Adresse bei einem DHCP-Server anfordert, kann er eine Gültigkeitsdauer für diese Adresse anfordern. Der Wert der maximalen Gültigkeit kontrolliert die maximale Gültigkeitsdauer, die ein Client anfordern darf. Wenn ein Client eine IP-Adresse anfordert, ohne eine Gültigkeitsdauer für diese Adresse zu fordern, wird dieser Adresse als Gültigkeitsdauer der Wert der Standard Gültigkeit zugewiesen.

**SNMP-ID:** 2.20.12

**Pfad Telnet:** /Setup/LAN-Bridge

**Mögliche Werte:**

- 1 bis 99.999 Minuten

**Default:** max. Gültigkeit: 6.000 Min., Standard Gültigkeit: 500 Min.

## 2.20.2 Bridge-Prioritaet

Dieser Wert legt die Priorität der Bridge im LAN fest. Sie beeinflussen damit, welche Bridge das Spanning- Tree-Protokoll bevorzugt als Root-Bridge verwendet. Es handelt sich hier um einen 16-Bit-Wert (0...65535), wobei höhere Werte eine niedrigere Priorität bedeuten. Ändern Sie den voreingestellten Wert nur dann, wenn Sie eine bestimmte Bridge bevorzugen. Auch mit gleichen Werten funktioniert das Auswahlverfahren, da das Gerät die MAC-Adresse der Bridge bei gleicher Priorität zur Entscheidung heranzieht.

**Pfad Telnet:** /Setup/LAN-Bridge/Bridge-Prioritaet

**Mögliche Werte:**

- maximal 5 numerische Zeichen

**Default:** 32768

Obwohl für die Konfiguration dieses Parameters ein ganzer 16-Bit Wert zur Verfügung steht, sollte bei neueren Versionen des Rapid-, bzw. Multiple-Spanning-Tree Protokolles darauf geachtet werden, den Prioritätswert nur in Schritten von 4096 zu verändern, da hier die unteren 12-Bit für andere Zwecke verwendet werden und deshalb von künftigen Firmware-Releases vielleicht ignoriert werden könnten.

## 2.20.7 Forward-Delay

Dieser Wert bestimmt die Zeit (in Sekunden), die mindestens vergeht, bevor ein Port von 'listening' nach 'learning' bzw. von 'learning' nach 'forwarding' wechseln darf. Seit es beim Rapid-Spanning-Tree jedoch eine Methode gibt, um festzustellen, wann ein Port in den 'Forwarding-Zustand' versetzt werden kann ohne lange zu warten, hat diese Einstellung in vielen Fällen keinen Effekt mehr.

**SNMP-ID:** 2.20.7

**Pfad Telnet:** /Setup/LAN-Bridge/Forward-Delay

**Mögliche Werte:**

- maximal 5 numerische Zeichen

**Default:** 6

## 2.20.6 Hello-Time

Dieser Parameter legt fest, in welchem zeitlichen Abstand in Sekunden ein als Root-Bridge ausgewähltes Gerät Informationen ins LAN schickt.

**SNMP-ID:** 2.20.6

**Pfad Telnet:** /Setup/LAN-Bridge/Hello-Time

**Mögliche Werte**:

- maximal 5 numerische Zeichen

**Default**: 2

## 2.20.8 Isolierter-Modus

Hier können die Verbindungen, zum Beispiel zwischen Layer-2 Forwarding und den LAN Schnittstellen an- oder ausgeschaltet werden.

**SNMP-ID:** 2.20.8

**Pfad Telnet:** /Setup/LAN-Bridge

**Mögliche Werte:**

- Bridge oder Router (Isolierter Modus)

**Default:** Bridge

Beachten Sie, dass andere konfigurierte Funktionen der Verbindung (wie zum Beispiel Spanning Tree, Packet Filters) bestehen bleiben / unabhängig davon, ob die Schnittstellen an- oder ausgeschaltet sind.

## 2.20.5 Max-Age

Dieser Wert bestimmt die Zeit (in Sekunden), nach der eine Bridge über Spanning Tree empfangene Nachrichten als 'veraltet' verwirft. Damitt legt man fest, wie schnell der Spanning-Tree Algorithmus auf Änderungen z. B. durch fortgefallene Bridges reagiert. Es handelt sich hier um einen 16-Bit-Wert (0...65535).

**SNMP-ID:** 2.20.5

**Pfad Telnet:** /Setup/LAN-Bridge/Max-Age

**Mögliche Werte:**

- maximal 5 numerische Zeichen

**Default:** 20

## 2.20.1 Protokoll-Version

Wählen Sie hier das gewünschte Protokoll aus. Je nach Wahl verwendet das Gerät entweder das Classic- oder das Rapid-Protokoll, welche in der IEEE 802.1D-1998 chapter 8, bzw. IEEE 802.1D-2004 chapter 17 definiert sind.

**Pfad Telnet:** /Setup/LAN-Bridge/Protokoll-Version

**Mögliche Werte:**

- Klassisch
- Rapid

**Default:** Klassisch

## 2.20.4 Verkapselungs-Tabelle

In dieser Tabelle können Sie Verkapselungen hinzufügen.

**SNMP-ID:** 2.20.4

**Pfad Telnet:** /Setup/LAN-Bridge

### 2.20.4.1 Protokoll

Ein Protokoll wird als 16-bit Protokoll ausgewiesen, und in ein Ethernet II/SNAP Feld gebracht. Der Protokoll Typ ist eine Hexadezimalzahl von 0001 bis ffff. Auch wenn die Tabelle leer ist, implizieren einige Protokolle eine Annahme, die in der Tabelle als SNAP (namely, IPX und AppleTalk) aufgelistet sind. Das kann durch die Protokoll Einstellung zu Ethernet II überschrieben werden.

**Pfad Telnet:** /Setup/LAN-Bridge/Verkapselungs-Tabelle

### 2.20.4.2 Verkapselung

Hier können Sie angeben, ob die Datenpakete bei der Übertragung mit einem Ethernet-Header versehen werden sollen oder nicht. Normalerweise sollten Sie hier "Transparent" auswählen. Nur wenn Sie einen Layer zur Verwendung mit der Bridge zusammenstellen, sollten Sie "Ethernet" auswählen.

**Pfad Telnet:** /Setup/LAN-Bridge/Verkapselungs-Tabelle

**Mögliche Werte:**

- Transparent
- Ethernet

**Default:** Transparent

## 2.20.10 Protokoll-Tabelle

Hier können Sie Protokolle zur Verwendung durch die LAN-Bridge hinzufügen.

**SNMP-ID:** 2.20.10

**Pfad Telnet:** /Setup/LAN-Bridge

### 2.20.10.1 Name

Dieser Name sollte die Regel beschreiben. Beachten Sie, dass es sich hier gleichzeitig um die Inhaltsspalte (index column) der Tabelle handelt, d.h. der Tabelleninhalt ist eine Reihe (String).

**Pfad Telnet:** /Setup/LAN-Bridge/Protokoll-Tabelle

**Mögliche Werte:**

- max. 15 Zeichen

**Default:** leer

### 2.20.10.10 IP-Netzwerk

Wenn der Wert im ersten Feld ungleich 0.0.0.0 ist, trifft eine Regel auf ein Paket zu, wenn es sich um ein IPv4 Paket handelt und entweder die Quell- oder Zieladresse des Pakets im IP-Netzwerk vorkommt und durch diese beiden Werte definiert wird.

**Pfad Telnet:** /Setup/LAN-Bridge/Protokoll-Tabelle

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0.

### 2.20.10.11 IP-Netzmaske

Wenn der Wert im ersten Feld ungleich 0.0.0.0 ist, trifft eine Regel auf ein Paket zu, wenn es sich um ein IPv4 Paket handelt und entweder die Quell- oder Zieladresse des Pakets im IP-Netzwerk vorkommt und durch diese beiden Werte definiert wird.

**Pfad Telnet:** /Setup/LAN-Bridge/Protokoll-Tabelle

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0.

### 2.20.10.12 DHCP-Src-MAC

meine Übersetzung: Diese Einstellungsregel hängt von der Quelle der MAC-Adresse ab, da diese ihre IP-Adresse über DHCP zugewiesen bekommt.

Aus anderer Quelle (Aurelia): DHCP-Tracking auf einer bestimmten (W)LAN-Schnittstelle findet nur statt, wenn Protokollfilter für die Schnittstelle definiert wurden, die den Parameter "Per DHCP zugewiesene IP" auf Ja oder Nein eingestellt haben. Für eine Filterregel kann zusätzlich ein Netz spezifiziert werden. Wenn eine Regel allerdings den Parameter "Per DHCP zugewiesene IP" auf Ja eingestellt hat, wird ein eventuell angegebenes Netz ignoriert.

**Pfad Telnet:** /Setup/LAN-Bridge/Protokoll-Tabelle

**Mögliche Werte:**

- Irrelevant
- Nein
- Ja

**Default:** Irrelevant

### 2.20.10.2 Protokoll

Hier wird die Kennung des Protokolls eingegeben. Die Kennung ist eine 4-stellige Hexadezimalzahl, die jedes Protokoll eindeutig kennzeichnet. Einige häufig vorkommende Protokolle sind z. B. 0800, 0806 für IP und ARP (Internet), E0E0, 8137 für IPX (Novell Netware), F0F0 für NetBEUI (Windows Netzwerk) oder 809B, 80F3 für Apple Talk (Apple Netzwerk). Wenn Sie das Protokoll-Feld auf Null setzen, betrifft diese Regel alle Pakete. Weitere Protokolle entnehmen Sie bitte der Dokumentation.

**Pfad Telnet:** /Setup/LAN-Bridge/Protokoll-Tabelle

**Mögliche Werte:**

- 4-stellige Hexadezimalzahl

**Default:** leer

### 2.20.10.3 Unterprotokoll

Geben Sie hier das Unter-Protokoll ein. Gängige Unterprotokolle innerhalb des IP-Protokolls (0800) sind z. B. 1 ICMP, 6 TCP, 17 UDP, 50 ESP (IPSec). Für ARP-Pakete gibt dieses Feld den ARP-Rahmen-Typ an (ARP request/reply, RARP request/reply). Wenn dieser Wert ungleich 0 ist, trifft die Regel nur zu, wenn es sich um ein IPv4 Paket handelt und das IP-Protokoll (UDP, TCP, ICMP,...) auf den gegebenen Wert passt, oder wenn es ein ARP Paket ist und der gegebene Wert mit dem ARP-Typ übereinstimmt. Wenn das Protokoll-Feld gesetzt ist, jedoch das Unterprotokoll-Feld auf Null steht, trifft diese Regel auf alle Pakete des angegebenen Protokolls zu, z. B. auf alle IP-Pakete für Protokoll 0800. Hinweis: Weitere Informationen finden Sie unter der URL www.iana.org, Rubrik "Protocol Number Assignment Services", Dokumente "Protocol Numbers" und "Port Numbers".

**Pfad Telnet:** /Setup/LAN-Bridge/Protokoll-Tabelle

**Mögliche Werte:**

- max. 65.535

**Default:** 0

### 2.20.10.4 Port

Geben Sie hier für TCP- oder UDP-Protokolle den Port-Nummern-Bereich an. Beispielsweise entspricht der UDP-Port 500 dem bei IPSec verwendeten IKE.

Wenn dieser Wert ungleich 0 ist, trifft die Regel nur zu, wenn es sich um ein IPv4 TCP oder ein UDP-Paket handelt oder die Quelle des Ziel-TCP/UDP-Ports in einem Bereich liegt, der durch diese beiden Werte definiert wird.

Falls Sie als End-Port eine Null angeben, gilt die Regel nur für den Anfangs-Port. Der Portnummern-Vergleich wird sowohl beim Empfangs- als auch beim Ziel-Port vorgenommen und eine Regel trifft zu, wenn auch nur einer der beiden im angegebenen Bereich liegt. Wenn das Protokoll- und das Unter-Protokoll-Feld gesetzt sind, jedoch die Port-Felder auf Null stehen, trifft diese Regel auf alle Pakete des angegebenen UnterProtokolls zu, z. B. auf alle Pakete für Protokoll 0800/6. Hinweis: Weitere Informationen finden Sie unter der URL www.iana.org, Rubrik "Protocol Number Assignment Services", Dokumente "Protocol Numbers" und "Port Numbers".

**Pfad Telnet:** /Setup/LAN-Bridge/Protokoll-Tabelle

**Mögliche Werte:**

- max. 65.535

**Default:** 0

### 2.20.10.5 Port-Ende

Geben Sie hier für TCP- oder UDP-Protokolle den Port-Nummern-Bereich an. Beispielsweise entspricht der UDP-Port 500 dem bei IPSec verwendeten IKE.

Wenn dieser Wert ungleich 0 ist, trifft die Regel nur zu, wenn es sich um ein IPv4 TCP oder ein UDP-Paket handelt oder die Quelle des Ziel-TCP/UDP-Ports in einem Bereich liegt, der durch diese beiden Werte definiert wird.

Falls Sie als End-Port eine Null angeben, gilt die Regel nur für den Anfangs-Port. Der Portnummern-Vergleich wird sowohl beim Empfangs- als auch beim Ziel-Port vorgenommen und eine Regel trifft zu, wenn auch nur einer der beiden im angegebenen Bereich liegt. Wenn das Protokoll- und das Unter-Protokoll-Feld gesetzt sind, jedoch die Port-Felder auf Null stehen, trifft diese Regel auf alle Pakete des angegebenen UnterProtokolls zu, z. B. auf alle Pakete für Protokoll 0800/6. Hinweis: Weitere Informationen finden Sie unter der URL www.iana.org, Rubrik "Protocol Number Assignment Services", Dokumente "Protocol Numbers" und "Port Numbers".

**Pfad Telnet:** /Setup/LAN-Bridge/Protokoll-Tabelle

**Mögliche Werte:**

- max. 65.535

**Default:** 0

### 2.20.10.6 Ifc-Liste

Diese Liste enthält die LAN-Interfaces, für welche die Regel angewendet wird. Die Syntax der Schnittstellen-Liste ist in Ergänzungen/Nachträgen/Anhängen angegeben.

In Abhängigkeit von den tatsächlich vorhandenen Interfaces können folgende vordefinierte Interface-beschreibende Bezeichner in einem Komma-separierten Ausdruck verwendet werden, um die betroffenen Interfaces zu spezifizieren:

- LAN-1,
- WLAN-1, WLAN-1-2, WLAN-1-3, WLAN-1-4, WLAN-1-5, WLAN-1-6, WLAN-1-7, WLAN-1-8, WLAN-2, WLAN-2-2, WLAN-2-3, WLAN-2-4, WLAN-2-5, WLAN-2-6, WLAN-2-7, WLAN-2-8,
- P2P-n-m ('n' bezeichnet die Schnittstelle des WLANs und 'm' die Nummer der P2P-Verbindung auf diesem WLAN).

Numerisch aufeinanderfolgende Interface-Bezeichner können durch folgende Notation verkürzt beschrieben werden: P2P-4~P2P-10. Wird hier kein Interface spezifiziert, wird die gewählte Aktion auch nie ausgeführt.

**Pfad Telnet:** /Setup/LAN-Bridge/Protokoll-Tabelle

**Mögliche Werte:**

- alle LAN-Interfaces
- DMZ-Interfaces
- die logischen WLAN-Netze und die Point-to-Point-Strecken im WLAN

**Default:** leer

### 2.20.10.7 Aktion

Hier können Sie eine Aktion auswählen, die mit einem Paket durchgeführt wird, das dieser Regel entspricht. Mögliche Aktionen sind Übertragen, Verwerfen oder Umleiten. Im Falle einer Umleitung muss im darauffolgenden Feld angegeben werden, zu welcher IP-Adresse das Paket umgeleitet werden soll. Die Umleitungseigenschaft ist nur für Pakete möglich, die TCP, UDP oder ICMP "echo requests" unterstützen. Das Gerät kann die Ziel-MAC- und IP-Adresse verändern, bevor das Paket weitergeleitet und wird so eine Eingabe in die Connection-Tabelle vornehmen, die eine Übersetzung der möglichen Antworten erlaubt.

**Pfad Telnet:** /Setup/LAN-Bridge/Protokoll-Tabelle

**Mögliche Werte:**

- Übertragen
- Verwerfen
- Umleiten

**Default:** Pakete verwerfen

### 2.20.10.8 Umleite-IP-Adresse

Falls die Regel eine Umleitungsregel darstellt, muss in diesem Feld angegeben werden, zu welcher IP-Adresse die passenden Pakete umgeleitet werden sollen.

**Pfad Telnet:** /Setup/LAN-Bridge/Protokoll-Tabelle

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0.

### 2.20.10.9 Ziel-MAC-Adr.

Hier wird die physikalische Adresse (MAC) einer Ziel-WLAN-Station eingegeben. Jede Netzwerkkarte hat eine eigene weltweit eindeutige MAC-Adresse. Diese Adresse ist eine 12stellige Hexadezimalzahl (z. B. 00A057010203). Sie finden diese Adresse meistens als Aufdruck auf der Netzwerkkarte selbst. Wenn Sie keine MAC-Adresse (oder 0) spezifizieren, betrifft diese Regel alle Pakete.

**Pfad Telnet:** /Setup/LAN-Bridge/Protokoll-Tabelle

**Mögliche Werte:**

- 12-stellige Hexadezimalzahl

**Default:** leer

## 2.20.11 Port-Daten

In dieser Tabelle kann man weitere Bridge-Parameter pro Port einstellen.

**SNMP-ID:** 2.20.11

**Pfad Telnet:** /Setup/LAN-Bridge

### 2.20.11.2 Port

Auswahl des Ports, für den die Spanning-Tree-Parameter eingestellt werden sollen.

**SNMP-ID:** 2.20.11.2

**Pfad Telnet:** /Setup/LAN-Bridge/Port-Daten

**Mögliche Werte:**

- Auswahl aus der Liste der logischen Schnittstellen des Geräts, z. B. LAN-1, WLAN-1 oder P2P-1-1

### 2.20.11.3 aktiv

Hier können Sie einen Port komplett sperren, d.h. der Port wird nie den Status disabled (gesperrt) verlassen.

**SNMP-ID:** 2.20.11.3

**Pfad Telnet:** /Setup/LAN-Bridge/Port-Daten

**Mögliche Werte:**

- aktiv
- inaktiv

**Default:** aktiviert

### 2.20.11.5 Bridge-Gruppe

Ordnet das logische Interface einer Bridge-Gruppe zu und ermöglicht so das Bridging von/zu dieser logischen Interface über die LAN-Bridge. Durch die Zuordnung zu einer gemeinsamen Bridge-Gruppe können mehrere logische Interfaces gemeinsam angesprochen werden und wirken so für den LANCOM Wireless wie ein einzelnes Interface – z. B. für die Nutzung im Zusammenhang mit Advanced Routing and Forwarding.

**SNMP-ID:** 2.20.11.5

**Pfad Telnet:** /Setup/LAN-Bridge/Port-Daten

**Mögliche Werte:**

- BRG-1 bis BRG-8
- keine

**Default:** BRG - 1

**Besondere Werte:** Wird das Interface über die Einstellung 'keine' aus allen Bridge-Gruppen entfernt, so findet keine Übertragung über die LAN-Bridge zwischen LAN und WLAN statt (isolierter Modus). In dieser Einstellung ist eine Datenübertragung zwischen LAN und WLAN für dieses Interface nur über den Router möglich.

Voraussetzung für die Datenübertragung von/zu einem logischen interface über die LAN-Bridge ist die Deaktivierung des globalen „Isolierten Modus“, der für die gesamte LAN-Bridge gilt. Außerdem muss das logische Interface einer Bridge-Gruppe zugeordnet sein – in der Einstellung 'keine' ist keine Übertragung über die LAN-Bridge möglich.

### 2.20.11.6 DHCP-Limit

Anzahl der Clients, die über DHCP zugewiesen werden können. Bei Überschreiten des Limits wird der jeweils älteste Eintrag verworfen. Dies kann in Kombination mit der Protokoll-Filter-Tabelle genutzt werden, um den Zugang auf ein logisches Interface zu begrenzen.

**SNMP-ID:** 2.20.11.6

**Pfad Telnet:** /Setup/LAN-Bridge/Port-Daten

**Mögliche Werte:**

- 0 bis 255

**Default:** 0

### 2.20.11.7 Point-To-Point-Port

Dieser Wert beschreibt die in der IEEE 802.1D definierte "adminPointToPointMAC"-Einstellmöglichkeit. Standardmäßig wird die "Point-to-Point"-Einstellung der LAN-Schnittstelle automatisch aufgrund der Technologie und des momentanen Status hergeleitet:

Ein Ethernet Port wird als P2P-Port angenommen, wenn er im Full-Duplex-Modus betrieben wird.

Ein Token Ring Port wird als P2P-Port angenommen, wenn er im Full-Duplex-Modus betrieben wird.

Eine WLAN SSID wird niemals als P2PPort betrachtet.

Eine WLAN P2P-Verbindung wird immer als P2P-Port angenommen.

Es ist jedoch möglich diese automatisch getroffene Einstellung zu revidieren, falls diese z. B. nicht brauchbar für die vorliegende Konfiguration erscheint. Schnittstellen im "Point-to-Point"-Modus haben besondere Fähigkeiten, die benutzt werden können um z. B. im Rapid-Spanning-Tree-Verfahren die Port-Status-Wechsel zu beschleunigen.

**SNMP-ID:** 2.20.11.7

**Pfad Telnet:** /Setup/LAN-Bridge/Port-Daten

**Mögliche Werte:**

- automatisch
- ein
- aus

**Default:** automatisch

## 2.20.13 Prioritaets-Zuordnung

Ordnen Sie über diese Tabelle jedem zu sendenden IP-Paket anhand eines ToS/DSCP-Wertes eine User-Priority gemäß 802.1D zu. Das Gerät nutzt die User-Priority z. B. im WLAN bei aktiviertem QoS, um Pakete einzelnen Access Categories zuzuordnen (Voice/Video/Best-Effort/Background).

**Pfad Telnet:** /Setup/LAN-Bridge/Prioritaets-Zuordnung

### 2.20.13.1 Name

Geben Sie hier einen Namen für eine Kombination von DSCP-Wert und Priorität an.

**Pfad Telnet:** /Setup/LAN-Bridge/Prioritaets-Zuordnung/Name

**Mögliche Werte:**

- maximal 16 alphanumerische Zeichen

**Default:** leer

### 2.20.13.2 DSCP-Wert

Geben Sie hier den DSCP-Wert an, der für diese Prioritätszuordnung verwendet wird.

**Pfad Telnet:** /Setup/LAN-Bridge/Prioritaets-Zuordnung/DSCP-Wert

**Mögliche Werte:**

- Numerische Zeichen von 0 bis 255

**Default:** 0

### 2.20.13.3 Prioritaet

Geben Sie hier die Priorität an, die für diese Prioritätszuordnung verwendet wird.

**Pfad Telnet:** /Setup/LAN-Bridge/Prioritaets-Zuordnung/Prioritaet

**Mögliche Werte:**

- Best-Effort
- Background
- Two
- Excellent-Erffort
- Controlled-Latency
- Video
- Voice
- Network-Control

**Default:** Best-Effort

## 2.20.20 Spannning-Tree

Dieses Menü enthält die Einstellungen des Spanning-Tree.

**SNMP-ID:** 2.20.20

**Pfad Telnet:** /Setup/LAN-Bridge

### 2.20.20.1 Aktiv

Hier können Sie die Unterstützung für Spanning-Tree ein- und ausschalten. Bei ausgeschaltetem Spanning-Tree verschickt der Router keine Spanning-Tree-Pakete und leitet empfangene Spanning-Tree-Pakete weiter, anstatt sie selber zu verarbeiten.

**SNMP-ID:** 2.20.20.1

**Pfad Telnet:** /Setup/LAN-Bridge/Spanning-Tree

**Mögliche Werte:**

- aktiv
- inaktiv

**Default:** deaktiviert

### 2.20.20.2 Bridge-Priotitaet

Dieser Wert legt die Priorität der Bridge im LAN fest. Man kann damit beeeinflußen, welche Bridge vom Spanning-Tree-Protokoll bevorzugt zur Root-Bridge gemacht wird. Es handelt sich hier um einen 16-Bit-Wert (0…65535), wobei höhere Werte eine niedrigere Priorität bedeuten. Eine Änderung des voreingestellten Wertes sollte nur erfolgen, wenn eine bestimmte Bridge bevorzugt werden soll. Auch mit gleichen Werten funktioniert das Auswahlverfahren, da die MAC-Adresse der Bridge bei gleicher Priorität zur Entscheidung herangezogen wird. Obwohl für die Konfiguration eines Parameters ein ganzer 16-Bit Wert zur Verfügung steht, sollte bei neueren Versionen des Rapid- bzw. Multiple-Spanning-Tree Protokolls darauf geachtet werden, den Prioritätswert nur in Schritten von 4096 zu verändern, da hier die unteren 12-Bit für andere Zwecke verwendet werden und deshalb von künftigen Firmware-Releases vielleicht ignoriert werden könnten.

**SNMP-ID:** 2.20.20.2

**Pfad Telnet:** /Setup/LAN-Bridge/Spanning-Tree

**Mögliche Werte:**

- max. 65.535

**Default:** 32768

### 2.20.20.7 Forward-Delay

Bestimmt die Zeit (in Sekunden) die mindestens vergehen muss, bevor ein Port von "listening" auf "learning" bzw. von "learning" auf "forwarding" wechseln darf. Seit es beim Rapid-Spanning-Tree jedoch eine Methode gibt um festzustellen, wann ein Port in den "Forwarding-Zustand" versetzt werden kann ohne lange zu warten, hat diese Einstellung in vielen Fällen keinen Effekt mehr." Ändern Sie diesen Wert ohne ausreichendes Wissen über Spanning-Trees nicht, da er das Risiko einer vorübergehenden Schleife im Netzwerk beeinflusst.

**SNMP-ID:** 2.20.20.7

**Pfad Telnet:** /Setup/LAN-Bridge/Spanning-Tree

**Mögliche Werte:**

- max. 32768 Sekunden

**Default:** 6 Sekunden

### 2.20.20.6 12 Sekunden

Die Hello-Zeit legt fest, in welchem Intervall (in Sekunden) die Root-Bridge Informationen ins LAN schickt. Beachte, dass die Non-Root-Bridge Werte der Root-Bridge übernehmen kann. Daher kann der Wert, abhängig von der Struktur des Netzwerks ignoriert werden.

**SNMP-ID:** 2.20.20.6

**Pfad Telnet:** /Setup/LAN-Bridge/Spanning-Tree

**Mögliche Werte:**

- max. 32768 Sekunden

**Default:** 2 Sekunden

### 2.20.20.5 Max-Age

Dieser Wert bestimmt die Zeit (in Sekunden) nach der eine Bridge über Spanning Tree empfangene Nachrichten als "veraltet" verwirft. Man legt damit folglich fest, wie schnell der Spanning-Tree Algorithmus auf Änderungen z. B. durch fortgefallene Bridges reagiert.

**SNMP-ID:** 2.20.20.5

**Pfad Telnet:** /Setup/LAN-Bridge/Spanning-Tree

**Mögliche Werte:**

- max. 65535 Sekunden

**Default:** 20 Sekunden

### 2.20.20.14 Pfadkosten-Berechnung

Hier kann eingestellt werden, nach welchem Protokoll die Pfadkosten berechnet werden. Während beim Rapid-Spanning-Tree Verfahren der volle 32-Bit Wertebereich ausgenutzt wird, findet beim Classic-Algorithmus nur ein 16-Bit Wertebereich Anwendung. Das Rapid-Spanning-Tree Verfahren ist aber nur sinnvoll, wenn es von allen Bridges im Netzwerk unterstützt wird und auch bei allen konsistent konfiguriert ist.

**SNMP-ID:** 2.20.20.14

**Pfad Telnet:** /Setup/LAN-Bridge/Spanning-Tree

**Mögliche Werte:**

- classic
- rapid

**Default:** classic

### 2.20.20.12 Protokoll-Version

Hier kann das Protokoll gewählt werden. Je nach Wahl wird entweder das Classic- oder das Rapid-Protokoll verwendet, welche in der IEE 802.1D-1998 chapter 8 bzw. in der IEEE 802.1D-2004 chapter 17 definiert ist.

**SNMP-ID:** 2.20.20.12

**Pfad Telnet:** /Setup/LAN-Bridge/Spanning-Tree

**Mögliche Werte:**

- classic
- rapid

**Default:** classic

Beachten Sie die Aufwärtskompatibilität dieses Protokolls. Wird eine Komponente erkannt die kein Rapid-Spanning-Tree unterstützt, werden automatisch Classic-Spannning-Tree Datenelemente und Methoden verwendet.

### 2.20.20.13 Transmit-Hold-Count

Bestimmt die Anzahl BPDUs (Bridge-Protocol-Data-Units), die bei der Verwendung von Rapid-Spanning-Tree gesendet werden dürfen, bevor eine Sekunde Pause eingelegt wird. (Bei Classic-Spanning-Tree hat dieser Wert keinen Einfluss.)

**SNMP-ID:** 2.20.20.13

**Pfad Telnet:** /Setup/LAN-Bridge/Spanning-Tree

**Mögliche Werte:**

- max. 999

**Default:** 6

### 2.20.20.11 Port-Daten

In dieser Tabelle kann man weitere Spanning-Tree-Parameter pro Port einstellen.

**SNMP-ID:** 2.20.20.11

**Pfad Telnet:** /Setup/LAN-Bridge/Spanning-Tree

#### 2.20.20.11.2 Port

Der Name der LAN-Schnittstelle.

**Pfad Telnet:** /Setup/LAN-Bridge/Spanning-Tree/Port-Daten

#### 2.20.20.11.4 Priorität

Die Priorität des Ports, vorliegend als 8-Bit Wert. Wenn mehr als ein Port verfügbar ist als Pfad zu einem LAN, und die Pfade zu beiden Ports die gleiche Länge haben, dann fungiert dieser Wert als Entscheidungsregel um einen Port auszuwählen. Wenn zwei Ports die gleiche Priorität haben, dann wird der Port mit der kleineren Nummer ausgewählt.

**Pfad Telnet:** /Setup/LAN-Bridge/Spanning-Tree/Port-Daten

**Mögliche Werte:**

- max. 255

**Default:** 128

Für Rapid-Spanning-Tree benutzt das Gerät nur die oberen 4 Bits dieses Wertes, z. B. wenn ein Wert sich in 16 Schritten erhöht und erniedrigt. Niedriger Werte bringen eine höhere Priorität.

#### 2.20.20.11.6 Kanten-Port

Ein Port kann als Edge-Port gekennzeichnet werden

**Pfad Telnet:** /Setup/LAN-Bridge/Spanning-Tree/Port-Daten

**Mögliche Werte:**

- an
- aus

**Default:** Kennzeichnung aus

#### 2.20.20.11.7 Pfadkosten-Uebersteuerung

Gibt die Pfadkosten-Beeinflussung an.

**Pfad Telnet:** /Setup/LAN-Bridge/Spanning-Tree/Port-Daten

**Mögliche Werte:**

- max. 4.294.967.295

**Default:** 0

## 2.20.30 IGMP-Snooping

**Pfad Telnet:** /Setup/LAN-Bridge/IGMP-Snooping

**Webconfig englisch:** LCOS menu tree/Setup/LAN-Bridge/IGMP-Snooping

### 2.20.30.6 Anfrage-Antwort-Intervall

Intervall in Sekunden, beeinflusst das Timing zwischen den IGMP-Anfragen und dem Altern der Router-Ports bzw. Mitgliedschaften.

Intervall in Sekunden, in dem ein Multicast-fähiger Router (oder ein simulierter Querier) Antworten auf seine IGMP-Anfragen erwartet. Diese regelmäßigen Abfragen beeinflussen den Zeitpunkt, nach dem die Mitgliedschaft in bestimmten Multicast-Gruppen “altern” und gelöscht werden.

**Pfad Telnet:** /Setup/LAN-Bridge/IGMP-Snooping

**Webconfig englisch:** LCOS menu tree/Setup/LAN-Bridge/IGMP-Snooping

**Mögliche Werte:**

- Zahl aus 10 Ziffern größer als 0

**Default:** 10

Das Anfrage-Antwort-Intervall muss kleiner als das Anfrage-Intervall sein.

### 2.20.30.5 Anfrage-Intervall

Intervall in Sekunden, in dem ein Multicast-fähiger Router (oder ein simulierter Querier) IGMP-Anfragen an die Multicast-Adresse 224.0.0.1 schickt und damit Rückmeldungen der Stationen über die Mitgliedschaft in Multicast-Gruppen auslöst. Diese regelmäßigen Abfragen beeinflussen den Zeitpunkt, nach dem die Mitgliedschaft in bestimmten Multicast-Gruppen “altern” und gelöscht werden.

Ein Querier sendet nach der Anfangsphase IGMP-Anfragen in diesem Intervall.

Ein Querier kehrt zurück in den Querier-Status nach einer Zeit von “Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)”.

Ein Router-Port verliert seine Eigenschaften nach einer Alterungszeit von “Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)”.

**Pfad Telnet:** /Setup/LAN-Bridge/IGMP-Snooping

**Webconfig englisch:** LCOS menu tree/Setup/LAN-Bridge/IGMP-Snooping

**Mögliche Werte:**

- Zahl aus 10 Ziffern größer als 0

**Default:** 125

Das Anfrage-Intervall muss größer als das Anfrage-Antwort-Intervall sein.

### 2.20.30.1 In-Betrieb

Aktiviert oder deaktiviert IGMP Snooping für das Gerät und alle definierten Querier-Instanzen. Ohne IGMP Snooping verhält sich die Bridge wie ein einfacher Switch und sendet alle Multicast auf alle Ports weiter.

**Pfad Telnet:** /Setup/LAN-Bridge/IGMP-Snooping

**Webconfig englisch:** LCOS menu tree/Setup/LAN-Bridge/IGMP-Snooping

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

Wenn diese Funktion deaktiviert ist, werden alle IP-Multicast-Pakete auf alle Ports gesendet. Bei einer Änderung des Betriebszustandes wird die IGMP-Snooping-Funktion vollständig zurückgesetzt, d.h. alle dynamische gelernten Werte (Mitgliedschaften, Router-Port-Eigenschaften) werden gelöscht.

### 2.20.30.7 Robustheit

Dieser Wert bestimmt die Robustheit des IGMP-Protokolls. Diese Option toleriert den Paketverlust von IGMP-Anfragen gegenüber den Join-Nachrichten.

**Pfad Telnet:** /Setup/LAN-Bridge/IGMP-Snooping

**Webconfig englisch:** LCOS menu tree/Setup/LAN-Bridge/IGMP-Snooping

**Mögliche Werte:**

- Zahl aus 10 Ziffern größer als 0

**Default:** 2

### 2.20.30.3 Unregistrierte-Datenpakete-Behandlung

Diese Option definiert die Verarbeitung von Multicast-Paketen mit Ziel-Adressen außerhalb des reservierten Adress-Bereiches "224.0.0.x", für die weder dynamisch gelernte noch statisch konfigurierte Mitgliedschaften vorhanden sind.

**Pfad Telnet:** /Setup/LAN-Bridge/IGMP-Snooping

**Webconfig englisch:** LCOS menu tree/Setup/LAN-Bridge/IGMP-Snooping

**Mögliche Werte:**

- Nur-Router-Ports: Sendet diese Pakete an alle Router-Ports.
- Fluten: Sendet diese Pakete an alle Ports.
- Verwerfen: Verwirft diese Pakete.

**Default:** Nur-Router-Ports

### 2.20.30.9 Werbe-Intervall

Das Intervall in Sekunden, in dem die Geräte Pakete aussenden, mit denen sie sich als Multicast-fähige Router bekanntmachen. Aufgrund dieser Information können andere IGMP Snooping-fähige Geräte schneller lernen, welche ihrer Ports als Router-Ports verwendet werden sollen. Beim Aktivieren von Ports kann ein Switch z. B. eine entsprechende

Anfrage nach Multicast-Routern versenden, die der Router mit einer solchen Bekanntmachung beantworten kann. Diese Methode ist je nach Situation ggf. deutlich schneller als die alternative Lernmöglichkeit über die IGMP-Anfragen.

**Pfad Telnet:** /Setup/LAN-Bridge/IGMP-Snooping

**Webconfig englisch:** LCOS menu tree/Setup/LAN-Bridge/IGMP-Snooping

**Mögliche Werte:**

- 4 bis 180 Sekunden

**Default:** 20

## 2.20.30.2 Port-Einstellungen

In dieser Tabelle werden die Port-bezogenen Einstellungen für IGMP Snooping vorgenommen.

**Pfad Telnet:** /Setup/LAN-Bridge/IGMP-Snooping

### 2.20.30.2.1 Port

Auf diesen Port beziehen sich die Einstellungen.

**Pfad Telnet:** /Setup/LAN-Bridge/IGMP-Snooping/Port-Einstellungen/Port

**Mögliche Werte:**

- Auswahl aus der Liste der im Gerät verfügbaren Ports

### 2.20.30.2.2 Router-Port

Diese Option definiert das Verhalten des Ports.

**Pfad Telnet:** /Setup/LAN-Bridge/IGMP-Snooping/Port-Einstellungen/Router-Port

**Mögliche Werte:**

- Ja: Dieser Port verhält sich immer wie ein Router-Port, unabhängig von den IGMP-Anfragen oder Router-Meldungen, die auf diesem Port evtl. empfangen werden.
- Nein: Dieser Port verhält sich nie wie ein Router-Port, unabhängig von den IGMP-Anfragen oder Router-Meldungen, die auf diesem Port evtl. empfangen werden.
- Auto: Dieser Port verhält sich wie ein Router-Port, wenn eine IGMP-Anfragen oder Router-Meldung empfangen wurde. Der Port verliert diese Eigenschaft wieder, wenn für die Dauer von "Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)" keine entsprechenden Pakete empfangen wurden.

**Default:** Auto

## 2.20.30.4 Simulierte-Anfrager

Diese Tabelle enthält alle im Gerät definierten simulierten Querier. Diese Einheiten werden eingesetzt, wenn kein Multicast-Router im Netzwerk vorhanden ist, aber dennoch die Funktionen des IGMP Snooping benötigt werden. Um die Querier auf bestimmte Bridge-Gruppen oder VLANs einzuschränken, können mehrere unabhängige Querier definiert werden, welche dann die entsprechenden VLAN-IDs nutzen.

**Pfad Telnet:** /Setup/LAN-Bridge/IGMP-Snooping

**Webconfig englisch:** LCOS menu tree/Setup/LAN-Bridge/IGMP-Snooping

**Name**

Name der Querier-Instanz.

Mögliche Werte:

- 8 alphanumerische Zeichen.

Default: Leer

**In-Betrieb**

Aktiviert oder deaktiviert die Querier-Instanz.

Mögliche Werte:

- Ja
- Nein

Default: Nein

**Bridge-Gruppe**

Schränkt die Querier-Instanz auf eine bestimmte Bridge-Gruppe ein.

Mögliche Werte:

- Auswahl aus der Liste der verfügbaren Bridge-Gruppen, keine.

Default: keine

Besondere Werte: Wenn “keine” Bridge-Gruppe gewählt wird, werden die IGMP-Anfragen auf allen Brigde-Gruppen ausgegeben.

**VLAN-Id**

Schränkt die Querier-Instanz auf ein bestimmtes VLAN ein.

Mögliche Werte:

- 0 bis 4096.

Default: 0

Besondere Werte: Wenn “0” als VLAN gewählt wird, werden die IGMP-Anfragen ohne VLAN-Tag ausgegeben. Dieser Wert ist daher nur sinnvoll, wenn die Verwendung von VLAN generell deaktiviert ist.

#### 2.20.30.4.1 Name

Name der Querier-Instanz.

**Pfad Telnet:** /Setup/LAN-Bridge/IGMP-Snooping/Simulierte-Anfrager/Name

**Mögliche Werte:**

- 8 alphanumerische Zeichen.

**Default:** Leer

#### 2.20.30.4.2 In-Betrieb

Aktiviert oder deaktiviert die Querier-Instanz.

**Pfad Telnet:** /Setup/LAN-Bridge/IGMP-Snooping/Simulierte-Anfrager/In-Betrieb

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

#### 2.20.30.4.3 Bridge-Gruppe

Schränkt die Querier-Instanz auf eine bestimmte Bridge-Gruppe ein.

**Pfad Telnet:** /Setup/LAN-Bridge/IGMP-Snooping/Simulierte-Anfrager/Bridge-Gruppe

**Mögliche Werte:**

- Auswahl aus der Liste der verfügbaren Bridge-Gruppen
- keine.

**Besondere Werte:** Wenn “keine” Bridge-Gruppe gewählt wird, werden die IGMP-Anfragen auf allen Brigde-Gruppen ausgegeben.

**Default:** keine

#### 2.20.30.4.4 VLAN-Id

Schränkt die Querier-Instanz auf ein bestimmtes VLAN ein.

**Pfad Telnet:** /Setup/LAN-Bridge/IGMP-Snooping/Simulierte-Anfrager/VLAN-Id

**Mögliche Werte**:

- 0 bis 4096

**Besondere Werte:** Wenn “0” als VLAN gewählt wird, werden die IGMP-Anfragen ohne VLAN-Tag ausgegeben. Dieser Wert ist daher nur sinnvoll, wenn die Verwendung von VLAN generell deaktiviert ist.

**Default:** 0

### 2.20.30.8 Statische-Mitglieder

Diese Tabelle erlaubt die manuelle Definition von Mitgliedschaften, die z. B. nicht automatisch gelernt werden können oder sollen.

**Pfad Telnet:** /Setup/LAN-Bridge/IGMP-Snooping

**Adresse**

Die IP-Adresse der manuell definierten Multicast-Gruppe.

Mögliche Werte:

- Gültige IP-Multicast-Adresse

Default: Leer

**VLAN-Id**

Die VLAN-ID, auf welche diese statische Mitgliedschaft angewendet werden soll. Für eine IP-Multicast-Adresse können durchaus mehrere Einträge mit unterschiedlichen VLAN-IDs gemacht werden.

Mögliche Werte:

- 0 bis 4096

Default: 0

Besondere Werte: Wenn “0” als VLAN gewählt wird, werden die IGMP-Anfragen ohne VLAN-Tag ausgegeben. Dieser Wert ist daher nur sinnvoll, wenn die Verwendung von VLAN generell deaktiviert ist.

**Lernen-erlauben**

Mit dieser Option wird das automatische Lernen von Mitgliedschaften für diese Multicast-Gruppe aktiviert. Wenn das automatische Lernen deaktiviert ist, werden die Pakete nur über die für die Multicast-Gruppe manuell definierten Ports verschickt.

Mögliche Werte:

- Ja
- Nein

Default: Ja

**Statische-Mitglieder**

An diese Ports werden die Pakete mit der entsprechenden IP-Multicast-Adresse immer zugestellt, unabhängig von empfangenen Join-Nachrichten.

Mögliche Werte:

- Kommaseparierte Liste der gewünschten Ports, maximal 215 alphanumerische Zeichen

Default: Leer

#### 2.20.30.8.1 Adresse

Die IP-Adresse der manuell definierten Multicast-Gruppe.

**Pfad Telnet:** /Setup/LAN-Bridge/IGMP-Snooping/Statische-Mitglieder/Adresse

**Mögliche Werte:**

- Gültige IP-Multicast-Adresse

**Default:** Leer

#### 2.20.30.8.2 Statische-Mitglieder

An diese Ports werden die Pakete mit der entsprechenden IP-Multicast-Adresse immer zugestellt, unabhängig von empfangenen Join-Nachrichten.

**Pfad Telnet:** /Setup/LAN-Bridge/IGMP-Snooping/Statische-Mitglieder/Statische-Mitglieder

**Mögliche Werte:**

- Kommaseparierte Liste der gewünschten Ports, maximal 215 alphanumerische Zeichen

**Default:** Leer

#### 2.20.30.8.3 VLAN-Id

Die VLAN-ID, auf welche diese statische Mitgliedschaft angewendet werden soll. Für eine IP-Multicast-Adresse können durchaus mehrere Einträge mit unterschiedlichen VLAN-IDs gemacht werden.

**Pfad Telnet:** /Setup/LAN-Bridge/IGMP-Snooping/Statische-Mitglieder/VLAN-Id

**Mögliche Werte:**

- 0 bis 4096

**Besondere Werte:** Wenn “0” als VLAN gewählt wird, werden die IGMP-Anfragen ohne VLAN-Tag ausgegeben. Dieser Wert ist daher nur sinnvoll, wenn die Verwendung von VLAN generell deaktiviert ist.

**Default:** 0

#### 2.20.30.8.4 Lernen-erlauben

Mit dieser Option wird das automatische Lernen von Mitgliedschaften für diese Multicast-Gruppe aktiviert. Wenn das automatische Lernen deaktiviert ist, werden die Pakete nur über die für die Multicast-Gruppe manuell definierten Ports verschickt.

**Pfad Telnet:** /Setup/LAN-Bridge/IGMP-Snooping/Statische-Mitglieder/Lernen-erlauben

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

# 2.21 HTTP

Dieses Menü enthält die Einstellungen des HTTP.

**SNMP-ID:** 2.21

**Pfad Telnet:** /Setup

## 2.21.2 Seitenueberschriften

Mit dieser Einstellung wählen Sie aus, ob bei der Darstellung der HTTP-Seiten des Public Spot Überschriften als Texte oder als Bilder angezeigt werden.

**SNMP-ID:** 2.21.2

**Pfad Telnet:** /Setup/HTTP

**Mögliche Werte:**

- Bilder
- Texte

**Default:** Bilder

Die Einstellungen für die Seitenüberschriften werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

## 2.21.1 Dokumentenwurzel

Dieser Parameter definiert den Pfad zu einem Verzeichnis, in dem die Hilfe für WEBconfig lokal gespeichert ist.

**SNMP-ID:** 2.21.1

**Pfad Telnet:** /Setup/HTTP/Dokumentenwurzel

**Mögliche Werte:**

- maximal 99 alphanumerische Zeichen

**Default:** leer

Dieser Parameter ist für die zukünftige, lokale Nutzung der WEBconfig-Hilfe vorgesehen. In aktuellen Firmware-Versionen ist dieser Parameter ohne Funktion.

## 2.21.6 Fehlerseiten-Stil

Normale Fehlerseite oder Bluescreen

**SNMP-ID:** 2.21.6

**Pfad Telnet:** /Setup/HTTP

**Mögliche Werte:**

- Standard
- Nifty

## 2.21.15 HTTP-Kompression

Zur schnelleren Anzeige werden die Inhalte von WEBconfig komprimiert. Für Browser, welche die Kompression nicht unterstützen, kann die Kompression deaktiviert werden.

**SNMP-ID:** 2.21.15

**Pfad Telnet:** /Setup/HTTP

**Mögliche Werte:**

- Aktiviert
- Deaktiviert
- Nur_für_WAN

**Default:** Aktiviert

## 2.21.9 Max.-Tunnel-Verbindungen

max. Anzahl der gleichzeitig aktiven HTTP-Tunnel.

**SNMP-ID:** 2.21.9

**Pfad Telnet:** /Setup/HTTP

**Mögliche Werte:**

- max. 255 Tunnel.

**Default:** 3

## 2.21.7 Port

Port für die HTTP-Server-Verbindung

**SNMP-ID:** 2.21.7

**Pfad Telnet:** /Setup/HTTP

**Mögliche Werte:**

- max. 5 Zeichen

**Default:** 80

## 2.21.3 Schrift-Familie

Schrift-Familie zur Darstellung der Weboberfläche.

**SNMP-ID:** 2.21.3

**Pfad Telnet:** /Setup/HTTP

**Mögliche Werte:**

- max. 39 Zeichen

**Default:**

- helvetica
- sans-serif

## 2.21.5 Seitenueberschriften

Wählen Sie hier aus, ob der Public Spot die Überschriften in den Standard-Seiten als Text oder als Grafiken anzeigt.

**Pfad Telnet:** /Setup/HTTP/Seitenueberschriften

**Mögliche Werte:**

- Bilder
- Texte

**Default:** Bilder

## 2.21.11 Sitzungs-Timeout

Gültigkeitsdauer der Webconfig-Sitzung ohne Benutzeraktivität in Sekunden. Nach Ablauf dieser Zeit wird erneut das Kennwort abgefragt.

**SNMP-ID:** 2.21.11

**Pfad Telnet:** /Setup/HTTP

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 600

## 2.21.8 SSL-Port

Port für die HTTPS-Server-Verbindung

**SNMP-ID:** 2.21.8

**Pfad Telnet:** /Setup/HTTP

**Mögliche Werte:**

- max. 5 Zeichen

**Default:** 443

## 2.21.13 Standard-Design

Wählt das Design, das standardmäßig für die Anzeige von WEBconfig verwendet wird.

**SNMP-ID:** 2.21.13

**Pfad Telnet:** /Setup/HTTP

**Mögliche Werte:**

- Normales_Design
- Design_für_kleine_Auflösungen
- Design_mit_hohem_Kontrast

**Default:** Normales_Design

## 2.21.10 Tunnel-Idle-Timeout

Lebensdauer eines Tunnels ohne Aktivität. Nach Ablauf dieser Zeit wird der Tunnel automatisch geschlossen, wenn darüber keine Daten übertragen werden.

**SNMP-ID:** 2.21.10

**Pfad Telnet:** /Setup/HTTP

**Mögliche Werte:**

- max. 4294967295 Sekunden.

**Default:** 300

## 2.21.18 SSL-Versions

Mit dieser Einstellung wählen Sie die Verwendung der aktuellen Verschlüsselungs-Protokolle für HTTPS-Verbindungen aus.

Bitte beachten Sie, dass die hier eingestellten Verschlüsselungsprotokolle nur bei HTTPS-Verbindungen eingesetzt werden. Bei anderen Protokollen sind die angebotenen Verschlüsselungsverfahren fest eingestellt:

- EAP/TLS/TTLS/PEAP ist fest TLS 1.0 eingestellt
- CAPWAP ist fest DTLS 1.0 eingestellt (was auf TLS 1.1 aufsetzt)
- Telnet/SSL ist fest auf 'SSL 3.0+TLS 1.0 + TLS 1.1 + TLS 1.2' eingestellt
- RADSEC ist fest auf 'SSL 3.0+TLS 1.0' eingestellt

**SNMP-ID:**

2.21.18

**Pfad Telnet:**

**Setup** > **HTTP** > **SSL-Versions**

**Mögliche Werte:**

SSLv3

TLSv1

TLSv1.1

TLSv1.2

**Default:**

SSLv3

TLSv1

## 2.21.14 Geräteinformation-anzeigen

In dieser Tabelle wird definiert, welche Systeminformationen auf der Seite Systeminformation/Gerätestatus in Webconfig angezeigt werden.

**SNMP-ID:** 2.21.14

**Pfad Telnet:** /Setup/HTTP

### 2.21.14.1 Geräte-Information

Auswahl der Geräteinformationen, die im Webconfig angezeigt werden sollen.

**Pfad Telnet:** /Setup/HTTP/Geräteinformation-anzeigen

**Mögliche Werte:**

- CPU
- Speicher

- Ethernet-Ports
- Durchsatz(Ethernet)
- UMTS/Modem-Schnittstelle
- Router
- Firewall
- DHCP
- DNS
- VPN
- ADSL
- ISDN
- DSLoL
- Uhrzeit
- IP-Adressen

**Default:** CPU

### 2.21.14.2 Position

Index für die Reihenfolge der Anzeige der Geräteinformationen.

**Pfad Telnet:** /Setup/HTTP/Geräteinformation-anzeigen

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

## 2.21.16 Server-Ports-offen-halten

In diesem Menü finden Sie die Parameter zum Einschränken des Zugriffs auf Web-Server-Dienste.

**Pfad Telnet:** /Setup/HTTP/Server-Ports-offen-halten

### 2.21.16.1 Ifc.

Wählen Sie hier den Zugangsweg aus, für den Sie den Zugang zu den Web-Server-Diensten einstellen möchten.

**Pfad Telnet:** /Setup/HTTP/Server-Ports-offen-halten/Ifc.

**Mögliche Werte:**

- Alle im Gerät verfügbaren Zugangswege (je nach Modell z. B. LAN, WAN, WLAN).

**Default:** Leer

### 2.21.16.2 Server-Ports-offen-halten

Der Zugriff auf ein Gerät über HTTP für die Konfiguration kann generell erlaubt, nicht erlaubt oder auf nur lesen eingeschränkt werden. Unabhängig davon kann der Zugriff auf die Web-Server-Dienste separat geregelt werden, z. B. um die Kommunikation von CAPWAP, SSL-VPN oder SCEP-CA über HTTP(S) zu ermöglichen, auch wenn der HTTP(S)-Zugang generell nicht erlaubt ist.

Für jeden Zugriffsweg (je nach Gerät LAN, WAN, WLAN) stellen Sie hier das Zugriffsrecht von Web-Server-Diensten des Gerätes auf den HTTP-Server-Port ein.

**Pfad Telnet:** /Setup/HTTP/Server-Ports-offen-halten/Server-Ports-offen-halten

**Mögliche Werte:**

- Automatisch: Der HTTP-Server-Port ist offen, solange ein Dienst angemeldet ist (z. B. CAPWAP). Ist kein Dienst mehr angemeldet, wird der Server-Port geschlossen.
- Aktiviert: Der HTTP-Server-Port ist immer offen, auch wenn der Zugriff auf die Konfiguration über HTTP nicht erlaubt ist. Hiermit kann der direkte Konfigurationszugriff unterbunden werden, jedoch die automatische Konfiguration von APs über einen WLAN-Controller weiterhin erlaubt werden.
- Deaktiviert: Der HTTP-Server-Port ist geschlossen, so dass kein Dienst den Web-Server benutzen kann. Wenn der Zugriff auf die Konfiguration über HTTP erlaubt ist, wird mit der entsprechenden Meldung quittiert, dass der Web-Server nicht erreichbar ist.

**Default:** Automatisch

## 2.21.20 Rollout-Wizard

Dieses Menü enthält die Einstellungen des Rollout-Wizards.

**SNMP-ID:** 2.21.20

**Pfad Telnet:** /Setup/HTTP

### 2.21.20.6 Aktionen-Renumerieren

Wie schon angeführt, werden Variablen und Aktionen in der Reihenfolge Ihres Index angezeigt bzw. abgearbeitet. Manchmal muss zwischen zwei Variablen/Aktionen mit benachbartem Index ein neuer Eintrag eingeführt werden. Mit dieser Aktion können die Indizes automatisch mit einem bestimmten Abstand zwischen den Einträgen neu vergeben werden.

Bei der Ausführung können als Argumente der Startwert und das Inkrement angegeben werden. Die Aktion nummeriert die Einträge neu, beginnend mit dem Startwert mit dem als Inkrement gewählten Abstand. Werden Startwert und Inkrement nicht angegeben, so wird für beides automatisch der Wert 10 verwendet. Ohne Argumente verwendet die Aktion daher die Indizes 10, 20, 30, 40 usw.

**SNMP-ID:** 2.21.20.6

**Pfad Telnet:** /Setup/HTTP/Rollout-Wizard

### 2.21.20.1 In-Betrieb

Schaltet den Rollout-Assistenten ein oder aus. Nach dem Einschalten wird der Assistent auf der Startseite von WEBconfig angeboten.

**SNMP-ID:** 2.21.20.1

**Pfad Telnet:** /Setup/HTTP/Rollout-Wizard

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

### 2.21.20.2 Titel

Name für den Rollout-Assistenten, wie er auf der Startseite von WEBconfig angezeigt wird.

**SNMP-ID:** 2.21.20.2

**Pfad Telnet:** /Setup/HTTP/Rollout-Wizard

**Mögliche Werte:**

- max. 50 Zeichen

**Default:** Rollout

### 2.21.20.5 Variablen-Renumerieren

Wie schon angeführt, werden Variablen und Aktionen in der Reihenfolge Ihres Index angezeigt bzw. abgearbeitet. Manchmal muss zwischen zwei Variablen/Aktionen mit benachbartem Index ein neuer Eintrag eingeführt werden. Mit dieser Aktion können die Indizes automatisch mit einem bestimmten Abstand zwischen den Einträgen neu vergeben werden.

Bei der Ausführung können als Argumente der Startwert und das Inkrement angegeben werden. Die Aktion nummeriert die Einträge neu, beginnend mit dem Startwert mit dem als Inkrement gewählten Abstand. Werden Startwert und Inkrement nicht angegeben, so wird für beides automatisch der Wert 10 verwendet. Ohne Argumente verwendet die Aktion daher die Indizes 10, 20, 30, 40 usw.

**SNMP-ID:** 2.21.20.5

**Pfad Telnet:** /Setup/HTTP/Rollout-Wizard

### 2.21.20.7 Verbindungsstatus-anzeigen-fuer

Bei der ersten Seite wird der Status der Verbidnung angezeigt.

**SNMP-ID:** 2.21.20.7

**Pfad Telnet:** /Setup/HTTP/Rollout-Wizard

### 2.21.20.1 Benutze-Zusatzpruefungen

Diese Option aktiviert einige Konsistenz-Tests, die interne Aspekte des Assistenten püfen.

Die Ausführung der Zusatzprüfungen ist sehr zeitaufwändig. Aktivieren Sie diese Option nur während der Entwicklung des Assistenten und deaktivieren Sie diese Option für den normalen Betrieb.

**SNMP-ID:** 2.21.20.8

**Pfad Telnet:** /Setup/HTTP/Rollout-Wizard

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

### 2.21.20.3 Variablen

In dieser Tabelle werden die Variablen für den Rollout-Assistenten definiert.

**SNMP-ID:** 2.21.20.3

**Pfad Telnet:** /Setup/HTTP/Rollout-Wizard

#### 2.21.20.3.1 Index

Index für die Variable. Die Variablen werden in der Anzeige des Rollout-Assistenten in aufsteigender Reihenfolge angezeigt.

**Pfad Telnet:** /Setup/HTTP/Rollout-Wizard/Variablen

**Mögliche Werte:**

- 1 bis 232 - 1

**Default:** 0

#### 2.21.20.3.2 Ident

Eindeutiger Identifier zur Kennzeichnung von Variablen, die bei der Ausführung von Aktionen referenziert werden. Die Angabe eines Identifiers ist nicht erforderlich bei Feldern, in die keine Daten vom Anwender eingetragen werden (z. B. Label).

**Pfad Telnet:** /Setup/HTTP/Rollout-Wizard/Variablen

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

#### 2.21.20.3.3 Titel

Name der Variablen, wie er im Rollout-Assistenten von WEBconfig angezeigt wird.

**Pfad Telnet:** /Setup/HTTP/Rollout-Wizard/Variablen

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

#### 2.21.20.3.4 Typ

Ty der Variable.

**Pfad Telnet:** /Setup/HTTP/Rollout-Wizard/Variablen

**Mögliche Werte:**

- Label: Text zur Anzeige von weiteren Erklärungen der anderen Variablen. Min-Wert und Max-Wert haben für diese Einträge keine weitere Bedeutung.
- Integer: Erlaubt die Eingabe einer positiven Integer-Zahl von 0 bis 232 - 1. Mit der Angabe von Min-Wert und Max-Wert kann der Eingabebereich eingeschränkt werden, außerdem kann ein Vorgabewert (Default) definiert werden. Dabei muss der Vorgabewert als Zahl innerhalb der Min- und Max-Werte eingetragen werden.
- String: Erlaubt die Eingabe eines Textes. Mit der Angabe von Min-Wert und Max-Wert kann die Länge des Textes eingeschränkt werden, außerdem kann ein Vorgabewert (Default) definiert werden. Dabei muss der Vorgabe-Text innerhalb der maximalen Länge liegen, längere Texte werden abgeschnitten.
- Passwort: Erlaubt die Eingabe eines Passwortes, welches bei der Eingabe nicht angezeigt wird. Die Eingabe des Passwortes muss wiederholt werden. Der Rollout-Asstsistent führt keine Aktionen aus, wenn die Eingabe der Passwörter nicht übereinstimmt.
- Haken: Einfache Option, die ein- oder ausgeschaltet sein kann. Min-Wert und Max-Wert haben für diese Einträge keine weitere Bedeutung. Haken sind standardmäßig eingeschaltet, wenn der Vorgabewert nicht leer ist.

**Default:** 0

#### 2.21.20.3.5 Min-Wert

Minimalwert der aktuellen Variablen (bei Typ Integer) bzw. minimale Anzahl der möglichen Zeichen (bei Typ String oder Passwort).

**Pfad Telnet:** /Setup/HTTP/Rollout-Wizard/Variablen

**Mögliche Werte:**

- 0 bis 232 - 1

**Default:** 0

#### 2.21.20.3.6 Max-Wert

Maximalwert der aktuellen Variablen (bei Typ Integer) bzw. maximale Anzahl der möglichen Zeichen (bei Typ String oder Passwort).

**Pfad Telnet:** /Setup/HTTP/Rollout-Wizard/Variablen

**Mögliche Werte:**

- 0 bis 232 - 1

**Default:** 0

#### 2.21.20.3.7 Vorgabewert

Vorgabewert der aktuellen Variablen.

**Pfad Telnet:** /Setup/HTTP/Rollout-Wizard/Variablen

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

### 2.21.20.4 Aktionen

In dieser Tabelle werden die Aktionen für den Rollout-Assistenten definiert.

**SNMP-ID:** 2.21.20.4

**Pfad Telnet:** /Setup/HTTP/Rollout-Wizard

#### 2.21.20.4.1 Index

Index für die Aktion. Die Aktionen werden bei der Ausführung des Rollout-Assistenten in aufsteigender Reihenfolge abgearbeitet.

**Pfad Telnet:** /Setup/HTTP/Rollout-Wizard/Aktionen

**Mögliche Werte:**

- 1 bis 232 - 1

**Default:** 0

#### 2.21.20.4.2 Aktion

Aktion, die vom Rollout-Assistenten nach der Eingabe der Benutzerdaten ausgeführt werden soll.

**Pfad Telnet:** /Setup/HTTP/Rollout-Wizard/Aktionen

**Mögliche Werte:**

- Aktionen werden wie Cron-Befehle in der Syntax [Protokoll:] Argument eingetragen. Wenn kein Protokoll angegeben ist, wird 'exec:' verwendet.

**Default:** Leer

**Besondere Werte:** exec: Führt einen beliebigen Befehl aus, wie er auf der Telnet-Ebene zur Konfiguration eines LANCOM verwendet wird. Das folgende Beispiel setzt den Namen des Gerätes auf 'MyLANCOM':

exec: set /setup/name MyLANCOM

mailto: Erlaubt das Versenden einer E-Mail mit Angabe von Adressat, Betreff und Body, z. B.:

mailto:admin@mylancom.de?subject=Rollout?body=LANCOM fertig eingerichtet

http und https: Erlaubt das Aufrufen einer Webseite, z. B. um dort eine Aktion auszuführen:

<http:|https:>//[user[:pass]@]hostname[:port]/...

Variablen in den Aktionen: Bei der Ausführung von Aktionen können die mit dem Rollout-Assistenten definierten Variablen referenziert werden. Dazu wird der Identifier der Variable geführt von einem Prozentzeichen in die Aktion eingesetzt. Der Identifier muss dabei in geschweifte Klammern gesetzt werden, wenn weitere Zeichen in der Aktion enthalten sind. Das folgende Beispiel setzt den Namen des Gerätes auf das Format 'Standort (Filiale)', wenn als Variable mit dem Identifier 'Location' der Standort des Gerätes abgefragt wird:

exec: set /setup/name %{Location}(Filiale)

Bei Variablen vom Typ Integer oder String wird der jeweilige Wert aufgrund der Benutzereingabe verwendet. Bei Variablen vom Typ Haken wird '1' (eingeschaltet) bzw. '0' (ausgeschaltet) verwendet.

Wenn der Ausdruck der Aktion Leerzeichen enthält, muss der Ausdruck in Anführungszeichen eingefasst werden.

Zur Nutzung der Mail-Funktion muss in dem Gerät ein SMTP-Konto eingerichtet sein.

#### 2.21.20.4.3 Beschreibung

Kommentar zu der Aktion.

**Pfad Telnet:** /Setup/HTTP/Rollout-Wizard/Aktionen

**Mögliche Werte:**

- max. 251 Zeichen

**Default:** Leer

## 2.21.30 Datei-Server

Dieses Menü beinhaltet die Einstellungen zum Fileserver für externe USB-Medien.

**SNMP-ID:** 2.21.30

**Pfad Telnet:** /Setup/HTTP/Datei-Server

### 2.21.30.2 In-Betrieb

Aktivieren oder deaktivieren Sie mit diesem Parameter den File-Server für USB-Medien.

**Pfad Telnet:** /Setup/HTTP/Datei-Server/In-Betrieb

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

### 2.21.30.1 Oeffentliches-Unterverzeichnis

Dieses Verzeichnis ist das root-Verzeichnis auf einem USB-Medium. Das Gerät ignoriert alle anderen Dateien auf dem USB-Medium .

**Pfad Telnet:** /Setup/HTTP/Datei-Server/Oeffentliches-Unterverzeichnis

**Mögliche Werte:**

- maximal 64 alphanumerische Zeichen

**Default:** public_html

# 2.22 SYSLOG

Dieses Menü enthält die Einstellungen des SYSLOGs.

**SNMP-ID:** 2.22

**Pfad Telnet:** /Setup

## 2.22.1 Aktiv

Aktiviert den Versand von Informationen über Systemereignisse an die konfigurierten SYSLOG-Clients.

**SNMP-ID:** 2.22.1

**Pfad Telnet:** /Setup/SYSLOG

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

## 2.22.5 Meldungs-Tabellen-Reihenfolge

Bestimmen Sie hier die Reihenfolge in der die Meldungs-Tabellen angezeigt werden.

**SNMP-ID:** 2.22.5

**Pfad Telnet:** /Setup/SYSLOG

**Mögliche Werte:**

- oldest on top
- newest-on-top

**Default:** oldest-on-top

## 2.22.4 Port

Port, der für den Versand der SYSLOG-Nachichten verwendet wird.

**SNMP-ID:** 2.22.4

**Pfad Telnet:** /Setup/SYSLOG

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 514

## 2.22.2 Tabelle-SYSLOG

In dieser Tabelle werden die SYSLOG-Clients definiert.

**SNMP-ID:** 2.22.2

**Pfad Telnet:** /Setup/SYSLOG

### 2.22.2.1 Idx.

Position des Eintrags in der Tabelle.

**SNMP-ID:** 2.22.2.1

**Pfad Telnet:** /Setup/SYSLOG/Tabelle-SYSLOG

**Mögliche Werte:**

- max. 4 Zeichen

**Default:** Leer

### 2.22.2.2 IP-Adresse

IP-Adresse des SYSLOG-Clients.

**SNMP-ID:** 2.22.2.2

**Pfad Telnet:** /Setup/SYSLOG/Tabelle-SYSLOG

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.22.2.3 Quelle

Quelle, die zum Versenden einer Meldung führt. Jede Quelle wird durch einen bestimmten Code dargestellt.

**SNMP-ID:** 2.22.2.3

**Pfad Telnet:** /Setup/SYSLOG/Tabelle-SYSLOG

**Mögliche Werte:**

- Systemzeit: 01
- Konsolen-Logins: 02
- Systemzeit: 04
- Logins: 08
- Verbindungen: 10
- Accounting: 20
- Verwaltung: 40
- Router: 80

**Default:** 00

**Besondere Werte:** 00: Es wird keine Quelle spezifiziert.

### 2.22.2.4 Level

SYSLOG-Level, mit dem die Meldung verschickt wird. Jedes Level wird durch einen bestimmten Code dargestellt.

**SNMP-ID:** 2.22.2.4

**Pfad Telnet:** /Setup/SYSLOG/Tabelle-SYSLOG

**Mögliche Werte:**

- Alarm: 01
- Fehler: 02
- Warning: 04

- Information: 08
- Debug: 10

**Default:** 00

**Besondere Werte:** 00: Es wird kein Level spezifiziert.

#### 2.22.2.6 Loopback-Addr.

Absenderadresse, die in den die SYSLOG-Meldung eingetragen wird. Auf SYSLOG-Meldungen werden keine Antworten erwartet.

**SNMP-ID:** 2.22.2.6

**Pfad Telnet:** /Setup/SYSLOG/Tabelle-SYSLOG

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

**Default:** Leer

### 2.22.3 Facility-Mapper

In dieser Tabelle werden die Zuordnungen von SYSLOG-Quellen zu Facilities definiert.

**SNMP-ID:** 2.22.3

**Pfad Telnet:** /Setup/SYSLOG

#### 2.22.3.1 Quelle

Zuordnung der Quellen zu bestimmten Facilities.

**SNMP-ID:** 2.22.3.1

**Pfad Telnet:** /Setup/SYSLOG/Facility-Mapper

**Mögliche Werte:**

- System
- Logins
- Systemzeit
- Konsolen-Logins
- Verbindungen
- Accounting
- Verwaltung
- Router

#### 2.22.3.2 Facility

Zuordnung der Quellen zu bestimmten Facilities.

**SNMP-ID:** 2.22.3.2

**Pfad Telnet:** /Setup/SYSLOG/Facility-Mapper

**Mögliche Werte:**

- KERNEL
- AUTH
- CRON
- AUTHPRIV
- LOCAL0
- LOCAL1
- LOCAL2
- LOCAL3

# 2.23 Schnittstellen

Dieses Menü enthält die Einstellungen der Schnittstellen.

**SNMP-ID:** 2.23

**Pfad Telnet:** /Setup

## 2.23.19 PCM-SYNC-SOURCE

Dieser ISDN-S0-Bus wird zur Synchronisierung der übrigen Busse verwendet. Wenn 'Automatisch' ausgewählt ist, wird auf den ersten im TE-Modus laufenden S0-Bus synchronisiert. Wenn Sie einen falschen SO-Bus auswählen, kann es zu Übertragungs-Störungen (Knack-Geräusche) kommen.

**Pfad Telnet:** /Setup/Schnittstellen/PCM-SYNC-SOURCE

**Mögliche Werte:**

- Auto
- S0-1
- S0-2

**Default:** Auto

Die Auswahlmöglichkeit der Parameter hängt von der jeweiligen Austattung Ihres Gerätes ab.

## 2.23.18 Permanente-L1-Aktivierung

Mit dieser Option aktivieren Sie die permanente Aktivierung des ISDN-Busses.

Wenn diese Option deaktiviert ist, schaltet das Gerät den ISDN-Bus ab, wenn er für 30 Sekunden nicht verwendet wird. Dieses Verfahren trägt dazu bei, in der Vermittlingsstelle (z. B. in einer übergeordneten TK-Anlage) Strom zu sparen.

Aktivieren Sie diese Option dann, wenn die übergeordnete TK-Anlage nicht korrekt auf die automatische Deaktivierung/Aktivierung des angeschlossenen Geräts reagiert.

**Pfad Telnet:** /Setup/Schnittstellen/Permanente-L1-Aktivierung

**Mögliche Werte Telnet:**

- deaktiviert
- nur-Sync-Quelle
- Alle-TE-Schnittstellen

**Default:** deaktiviert

## 2.23.1 S0

Hier können Sie für diese Schnittstelle Ihres Gerätes weitere Einstellungen vornehmen.

**SNMP-ID:** 2.23.1

**Pfad Telnet:** /Setup/Schnittstellen

### 2.23.1.1 Ifc

Auswahl der ISDN-Schnittstelle, auf die sich die Einstellungen beziehen.

**SNMP-ID:** 2.23.1.1

**Pfad Telnet:** /Setup/Schnittstellen/S0/Ifc

**Mögliche Werte:**

- Auswahl aus den im Gerät verfügbaren ISDN-Schnittstellen, z. B. S0-1 oder S0-2

### 2.23.1.13 Max-pass-Verb

Mit dieser Einstellung können Sie die Anzahl der Verbindungen beschränken, die über dieses Interface aufgebaut werden. So können Sie beispielsweise sicherstellen, dass für andere Geräte immer eine Leitung verfügbar bleibt.

**Pfad Telnet:** /Setup/Schnittstellen/S0/Max-pass-Verb

**Mögliche Werte:**

- keine
- eine
- zwei

**Default:** zwei

### 2.23.1.14 Max-akt-Verb

Mit dieser Einstellung können Sie die Anzahl der Verbindungen beschränken, die über dieses Interface aufgebaut werden. So können Sie beispielsweise sicherstellen, dass für andere Geräte immer eine Leitung verfügbar bleibt.

**Pfad Telnet:** /Setup/Schnittstellen/S0/Max-akt-Verb

**Mögliche Werte:**

- keine
- eine
- zwei

**Default:** zwei

### 2.23.1.2 Protokoll

Wählen Sie hier das D-Kanal-Protokoll für dieses Interface aus.

**Pfad Telnet:** /Setup/Schnittstellen/S0/Protokoll

**Mögliche Werte:**

- nein
- DSS1
- 1TR6
- P2P-DSS1

- GRP0
- Auto

**Default:** Auto

### 2.23.1.7 FV-B-Kanal

Stellen Sie den Festverbindungskanal ein, der bei einer Festverbindung des Typs **Gruppe 0** benutzt werden soll.

**Pfad Telnet:** /Setup/Schnittstellen/S0/FV-B-Kanal

**Mögliche Werte:**

- kein
- B1
- B2

**Default:** kein

### 2.23.1.9 Anwahl-Praefix

Geben Sie hier eine Nummer ein, die jeder Rufnummer bei abgehenden Rufen vorangestellt werden soll.

Wenn Ihr Gerät beispielsweise an einer Telefonanlage betrieben wird, welche die Vorwahl einer Amtskennzahl erfordert, dann sollten Sie diese hier eintragen.

**Pfad Telnet:** /Setup/Schnittstellen/S0/Anwahl-Praefix

**Mögliche Werte:**

- max. 8 Zeichen

**Default**: leer

## 2.23.4 DSL

Hier finden Sie die Einstellungen für das DSL-Interface.

**SNMP-ID:** 2.23.4

**Pfad Telnet:** /Setup/Schnittstellen

### 2.23.4.1 Ifc

Auswahl der Schnittstelle, auf die sich die Einstellungen beziehen.

**SNMP-ID:** 2.23.4.1

**Pfad Telnet:** /Setup/Schnittstellen/S0/Ifc

**Mögliche Werte:**

- Auswahl aus den im Gerät verfügbaren ISDN-Schnittstellen, z. B. S0-1 oder S0-2
- ADSL
- VDSL
- Auswahl aus den im Gerät verfügbaren DSL-Schnittstellen, z. B. DSL-1 oder DSL-2
- UMTS

Die Auswahlmöglichkeiten hängen von der jeweiligen Ausstattung Ihres Gerätes aus.

### 2.23.4.16 Upstream-Rate

Hier können Sie die Brutto-Upstreamrate für diese Schnittstelle bestimmen. Die hier eingegebene Datenmenge (kbit/s) limitiert die vom Gerät abgehenden Datenströme.

**Pfad Telnet:** /Setup/Schnittstellen/DSL/Upstream-Rate

**Mögliche Werte:**

- maximal 6 numerische Zeichen

**Default:** leer

**Besondere Werte:** 0: keine Limitierung der übertragenen Datenmenge

### 2.23.4.17 Ext.-Overhead

Der externe Overhead ergibt sich aus den Daten, die das Modem selbst noch vor jedes Paket setzt. Bei PPPoE-Verbindungen sind das 4 Byte für den LLC-Header und 8 Byte für den AAL-5-Trailer. Da das Modem zudem keine "angebrochenen" ATM-Zellen verschicken kann, muss im Schnitt noch eine halbe ATM-Zelle (= 24 Bytes) aufgeschlagen werden. Somit ergibt sich ein Gesamt-Overhead von 36 Bytes pro übertragenem Paket.

**Pfad Telnet:** /Setup/Schnittstellen/S0/Ext.-Overhead

**Mögliche Werte:**

- maximal 3 numerische Zeichen

**Default:** leer

### 2.23.4.18 Downstream-Rate

Die Downstreamrate wird in Kilobit angegeben und enthält alles, was den Router über das WAN-Ethernet erreicht. So beträgt z. B. auf einem T-DSL Anschluss mit garantierten 768 kbit Downstream die vom Modem ausgehandelte Upstreamrate 864 kbit. Diese beinhalten allerdings noch einen für diese Verbindung typischen Overhead, welcher sich aus der Verwendung von ATM als Transportprotokoll des Modems ergibt. Bereinigt man die 864 kbit um den Overhead, der sich aus dem Aufbau einer ATM-Zelle ergibt (48 Byte Nutzdaten bei 53 Byte Zellenlänge), so erhält man 864 *48 /53 = 792 kbit Brutto-Downstreamrate, welche auf dem Ethernet vom Modem zum Router übertragen werden. Sind die vom Modem ausgehandelten Datenraten nicht bekannt, so kann man aus den garantierten Datenraten durch Multiplikation mit 56/55 die Brutto-Datenraten annähern.

**Pfad Telnet:** /Setup/Schnittstellen/DSL/Downstream-Rate

**Mögliche Werte:**

- maximal 6 numerische Zeichen

**Default:** leer

**Besondere Werte:** 0: keine Beschränkung des empfangenen Datenverkehrs

### 2.23.4.2 Aktiv

Hier können Sie einstellen, ob die Schnittstelle aktiv ist oder nicht.

**SNMP-ID:** 2.23.4.2

**Pfad Telnet:** /Setup/Schnittstellen/DSL/Aktiv

**Mögliche Werte:**

- nein
- ja

**Default:** nein

### 2.23.4.23 LAN-Ifc

Wählen Sie an welches LAN-Interface das DSLoL-Interface gebunden ist.

**Pfad Telnet:** /Setup/Schnittstellen/DSLoL-Schnittstellen/LAN-Ifc

**Mögliche Werte:**

- LAN-1
- WLAN-1
- P2P-1-1
- P2P-1-2
- P2P-1-3
- P2P-1-4
- P2P-1-5
- P2P-1-6
- WLAN-1-2
- WLAN-1-3
- WLAN-1-4
- WLAN-1-5
- WLAN-1-6
- WLAN-1-7
- WLAN-1-8
- BRG-1
- BRG-2
- BRG-3
- BRG-4
- BRG-5
- BRG-6
- BRG-7
- BRG-8
- beliebig

**Default:** LAN-1

### 2.23.4.6 Mode

Wählen Sie hier den Modus, wie das WAN-Interface genutzt wird. Im Automatik-Modus werden alle PPPoE-Frames sowie alle Datenpakete, die zu einer über das DSLoL-Interface aufgebauten Verbindung gehören (Konfiguriert in der IP-Parameter-Liste), über das DSLoL-Interface (WAN) weitergeleitet. Alle anderen Datenpakete werden als normale LAN-Pakete behandelt. Im Exclusiv-Modus wird das LAN-Interface ausschließlich als WAN-Interface benutzt.

**Pfad Telnet:** /Setup/Schnittstellen/DSLoL-Interface/Mode

**Mögliche Werte:**

- Auto
- Exklusiv

**Default:** Auto

## 2.23.6 ADSL-Interface

Hier finden Sie die Einstellungen für das ADSL-Interface.

**Pfad Telnet:** /Setup/Schnittstellen/ADSL-Interface

### 2.23.6.1 Ifc

Wählen Sie hier die betreffende Schnittstelle aus.

**Pfad Telnet:** /Setup/Schnittstellen/ADSL-Interface/Ifc

**Mögliche Werte:**

- ADSL
- S0-1
- DSL-1
- DSL-2
- DSL-3
- UMTS

Die Auswahlmöglichkeiten hängen von der jeweiligen Austattung Ihres Gerätes ab.

### 2.23.6.2 Protokoll

Wählen Sie hier das Protokoll aus, das Sie für diese Schnittstelle verwenden möchten.

Beim ADSL-Multimode werden reihum die Protokolle G.DMT, T1.413 und G.Lite versucht. Beim Auto-Modus wird zuerst versucht mit dem ADSL2+-Protokoll eine Verbindung aufzubauen. Kann damit keine Verbindung aufgebaut werden findet ein Fallback über ADSL2 nach G.Dmt statt.

**Pfad Telnet:** /Setup/Schnittstellen/ADSL-Interface/Protokoll

**Mögliche Werte:**

- nein
- Auto
- ADSL2+
- ADSL2
- ADSL-Multimode
- Annex-M-Auto
- G.Dmt
- T1.413

**Default:** nein

### 2.23.6.25 Powermanagement

Aktivieren Sie das Powermanagement, um die Leistungsaufnahme des integrierten ADSL-Modems zu senken.

Der L2-Modus greift nur in die Vermittlungsstelle ein.

Der L3-Modus ermöglicht eine Reduzierung der Leistungsaufnahme in der Vermittlungsstelle und im ADSL-Gerät. Dazu schaltet sich das Gerät in einen Sleep-Modus, wenn die Verbindung für eine definierte Zeit nicht aktiv ist. Sobald die Verbindung wieder aktiviert wird, benötigt das ADSL-Gerät einige Sekunden für die Initialisierung und Rückkehr in den Betriebsmodus.

**Pfad Telnet:** /Setup/Schnittstellen/ADSL-Interface/Powermanagement

**Mögliche Werte Telnet:**

- Deaktiviert
- L2-erlaubt

- L3-und-L2-erlaubt

**Default:** L2-erlaubt

### 2.23.6.26 Linecode

Stellen Sie hier die Funtionsweise des Linecodes ein. Wenn Sie 'Auto wählen', dann erfolgt ein automatisches Weiterschalten zum nächsten Protokoll der ADSL-Protokollliste eines Line-Codes bzw. bei Erreichen deren Endes zum nächsten Line-Code:

- wenn kein Signal auf der Leitung erkannt wird
- nach 3 Minuten ohne Sync bei ADSL2+
- nach 1,5 Minuten ohne Sync bei ADSL
- beim ersten Sync-Verlust nach dem Weiterschalten auf einen neuen Line-Code

Weitergeschaltet wird nur zu Line-Codes, die das aktuell ausgewählte Protokoll unterstützen. Wird ein Protokoll ausgewählt, das der aktuelle Line-Code nicht beherrscht, wird auf den nächsten passenden Line-Code weitergeschaltet.

Eine kontinuierliche Bewertung der Leitungsqualität findet nicht statt. Es wird im Automatik-Modus (Protokoll und/oder Line-Code) lediglich die Anzahl der Leitungsfehler innerhalb der Überwachungszeit geprüft. Standardmäßig ist ein Leitungsfehler in 24 Stunden zugelassen. Wird die zulässige Anzahl überschritten, erfolgt eine Weiterschaltung zum nächsten Protokoll bzw. Line-Code.

Wird die Anzahl der zulässigen Leitungsfehler innerhalb der Überwachungszeit nicht erreicht, wird der aktuell verwendete Line-Code "festgeschrieben", und hier entsprechend fest eingetragen. Gleichzeitig wird damit der Automatik-Modus für den Line-Code deaktiviert. Die Überwachungszeit beginnt erst eine Minute nach dem Boot bzw. nach einem Wechsel von Line-Code oder Protokoll.

**Pfad Telnet:** /Setup/Schnittstellen/ADSL-Interface/Linecode

**Mögliche Werte:**

- Auto
- Annex-A
- Annex-B
- ADSL-A
- ADSL2+A
- ADSL-B
- ADSL2+B

**Default:** Auto

## 2.23.7 Modem-Mobilfunk

Hier finden Sie die Einstellungen für das Mobilfunk-Modem.

**SNMP-ID:** 2.23.7

**Pfad Telnet:** /Setup/Schnittstellen

### 2.23.7.1 Ifc

Wählen Sie hier das Interface aus, das Sie konfigurieren möchten.

**Pfad Telnet:** /Setup/Schnittstellen/Modem-Mobilfunk/Ifc

**Mögliche Werte**:

- DSL-1
- EXT
- ADSL

- S0-1
- DSL-1
- DSL-2
- DSL-3
- UMTS

Die Auswahlmöglichkeiten hängen von der Ausstattung Ihres Gerätes ab.

### 2.23.7.2 Aktiv

Wählen Sie hier, auf welche Weise die Schnittstelle aktiv ist.

**Pfad Telnet:** /Setup/Schnittstellen/Modem-Mobilfunk/Aktiv

**Mögliche Werte**:

- Nein
- Modem
- UMTS-GPRS

**Default**: Nein

### 2.23.7.21 Datenrate

Wählen Sie hier die Datenrate, mit der Datenströme in Kilobyte pro Sekunde übertragen werden.

**Pfad Telnet:** /Setup/Schnittstellen/Modem-Mobilfunk/Datenrate

**Mögliche Werte Telnet:**

- 19200
- 38400
- 57600
- 115200

**Default**: 115200

### 2.23.7.22 Profil

Wählen Sie hier das Profil, das für die UMTS-Schnittstelle verwendet werden soll.

**Pfad Telnet:** /Setup/Schnittstellen/Modem-Mobilfunk/Profil

**Mögliche Werte:**

- maximal 16 alphanumerische Zeichen

**Default:** leer

## 2.23.8 VDSL

Für jede der im Gerät verfügbaren VDSL-Schnittstellen enthält diese Tabelle einen Eintrag mit der Auswahl des verwendeten Protokolls.

**SNMP-ID:** 2.23.8

**Pfad Telnet:** /Setup/Interfaces/

### 2.23.8.1 Ifc

Wählen Sie hier eine VDSL-Schnittstelle zur Konfiguration aus.

**SNMP-ID:** 2.23.8.1

**Pfad Telnet:** /Setup/Interfaces/VDSL

**Mögliche Werte:**

- Auswahl aus den im Gerät verfügbaren VDSL-Schnittstellen.

### 2.23.8.2 Protokoll

Wählen Sie hier das Protokoll für die VDSL-Schnittstelle aus.

**SNMP-ID:** 2.23.8.2

**Pfad Telnet:** /Setup/Interfaces/VDSL

**Mögliche Werte:**

- Auto: VDSL und sämtliche ADSL-Modi
- VDSL: Nur VDSL
- ADSL: Sämtliche ADSL-Modi
- ADSL2+: Nur ADSL2+ (G.992.5)
- ADSL2: Nur ADSL2 (G.992.3)
- ADSL1: G.DMT (G.992.1) und bei Annex-A auch T1.413

**Default:** Auto

## 2.23.20 WLAN

Dieses Menü enthält die Einstellungen für kabellose Netzwerke (WLAN)

**SNMP-ID:** 2.23.20

**Pfad Telnet:** /Setup/Schnittstellen

### 2.23.20.1 Netzwerk

Hier können Sie für jedes logische Wireless-LAN-Netzwerk (MultiSSID) Ihres Gerätes weitere Netzwerk-Einstellungen vornehmen.

**SNMP-ID:** 2.23.20.1

**Pfad Telnet:** /Setup/Schnittstellen/WLAN

#### 2.23.20.1.1 Ifc

Auswahl aus den logischen WLAN-Schnittstellen.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Netzwerk

**Mögliche Werte:**

- Auswahl aus den verfügbaren logischen WLAN-Netzwerken.

#### 2.23.20.1.10 Maximum-Stationen

Legen Sie hier die maximale Anzahl der Clients fest, die sich bei diesem Access Point in dieses Netzwerk einbuchen dürfen. Weitere Clients, die sich über diese Anzahl hinaus anmelden wollen, werden abgelehnt.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Netzwerk

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

**Besondere Werte:** 0 = Limitierung ausgeschaltet

#### 2.23.20.1.11 Cl.-Brg.-Support

Während mit der Adress-Anpassung (’Adress-Anpassung’ Æ Seite 480) nur die MAC-Adresse eines einzigen angeschlossenen Gerätes für den Access Point sichtbar gemacht werden kann, werden über die Client-Bridge-Unterstützung alle MAC-Adressen der Stationen im LAN hinter der Clientstationen transparent an den Access Point übertragen.

Dazu werden in dieser Betriebsart nicht die beim Client-Modus üblichen drei MAC-Adressen verwendet (in diesem Beispiel für Server, Access Point und Clientstation), sondern wie bei Punkt-zu-Punkt-Verbindungen vier Adressen (zusätzlich die MAC-Adresse der Station im LAN der Clientstation). Die volltransparente Anbindung eines LANs an der Clientstation ermöglicht die gezielte Übertragung der Datenpakete im WLAN und damit Funktionen wie TFTP-Downloads, die über einen Broadcast angestoßen werden.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Netzwerk

**Mögliche Werte:**

- Ja: Aktiviert die Client-Bridge-Unterstützung für dieses logische WLAN.
- Nein: Deaktiviert die Client-Bridge-Unterstützung für dieses logische WLAN.
- Exklusiv: Akzeptiert nur Clients, die ebenfalls den Client-Bridge-Modus unterstützen.

**Default:** Nein

Der Client-Bridge-Modus kann ausschließlich zwischen zwei LANCOM-Geräten verwendet werden.

#### 2.23.20.1.12 RADIUS-Accounting

Schaltet Accounting über einen RADIUS-Server auf diesem Netz ein oder aus

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Netzwerk

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

#### 2.23.20.1.13 Inter-Stations-Verkehr

Je nach Anwendungsfall ist es gewünscht oder eben auch nicht erwünscht, dass die an einem Access Point angeschlossenen WLAN-Clients mit anderen Clients kommunizieren. Für jedes logische WLAN kann separat eingestellt werden, ob die Clients in dieser SSID untereinander Daten austauschen können.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Netzwerk

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

#### 2.23.20.1.14 APSD

Aktiviert den Stromsparmodus APSD für dieses logische WLAN-Netzwerk.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Netzwerk

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

Bitte beachten Sie, dass zur Nutzung der Funktion APSD in einem logischen WLAN auf dem Gerät das QoS aktiviert sein muss. Die Mechanismen des QoS werden bei APSD verwendet, um den Strombedarf der Anwendungen zu optimieren.

#### 2.23.20.1.15 Aironet-Erweiterungen

Aktiviert Aironet-Erweiterungen für dieses logische Wireless LAN.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Netzwerk/Aironet-Erweiterungen

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

#### 2.23.20.1.2 Netzwerkname

Stellen Sie für jedes benötigte logische Funknetzwerk eine eindeutige SSID (den Netzwerknamen) ein. Nur solche WLAN-Clients, die über die gleiche SSID verfügen, können sich in diesem Funknetzwerk anmelden.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Netzwerk

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** BLANK

#### 2.23.20.1.4 Closed-Network

Sie können Ihr Funk-LAN entweder in einem öffentlichen oder in einem privaten Modus betreiben. Ein Funk-LAN im öffentlichen Modus kann von Mobilstationen in der Umgebung ohne weiteres kontaktiert werden. Durch Aktivieren der Closed-Network-Funktion versetzen Sie Ihr Funk-LAN in einen privaten Modus. In dieser Betriebsart sind Mobilstationen ohne Kenntnis des Netzwerknamens (SSID) von der Teilnahme am Funk-LAN ausgeschlossen.

Schalten Sie den 'Closed-Network-Modus' ein, wenn Sie verhindern möchten, dass sich WLAN-Clients mit der SSID 'Any' in Ihrem Funknetzwerk anmelden.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Netzwerk

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

#### 2.23.20.1.8 Aktiv

Schaltet das logische WLAN separat ein- oder aus.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Netzwerk

**Mögliche Werte:**

- Ein
- Aus

**Default:** Ein

#### 2.23.20.1.9 MAC-Filter

In der MAC-Filterliste werden die MAC-Adressen der Clients hinterlegt, die sich bei einem Access Point einbuchen dürfen. Mit dem Schalter 'MAC-Filter aktiviert' kann die Verwendung der MAC-Filterliste gezielt für einzelne logische Netzwerke ausgeschaltet werden.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Netzwerk

**Mögliche Werte:**

- Ein
- Aus

**Default:** Ein

Die Verwendung der MAC-Filterliste ist auf jeden Fall erforderlich für logische Netzwerke, in denen sich die Clients mit einer individuellen Passphrase über LEPS anmelden. Die bei LEPS verwendete Passphrase wird ebenfalls in der MAC-Filterliste eingetragen. Für die Anmeldung mit einer individuellen Passphrase wird daher immer die MAC-Filterliste beachtet, auch wenn diese Option hier deaktiviert ist.

### 2.23.20.2 Uebertragung

Hier können Sie für jedes logische Wireless-LAN-Netzwerk (MultiSSID) Ihres Gerätes weitere Übertragungs-Einstellungen vornehmen.

**SNMP-ID:** 2.23.20.2

**Pfad Telnet:** /Setup/Schnittstellen/WLAN

#### 2.23.20.2.1 Ifc

Öffnet die Einstellungen für die logischen WLAN-Netzwerke

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Uebertragung

**Mögliche Werte:**

- Auswahl aus den verfügbaren logischen WLAN-Netzwerken.

#### 2.23.20.2.10 Min.-Frag.-Laenge

Paket-Fragmentlänge, unterhalb der Fragmente verworfen werden

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Uebertragung

**Mögliche Werte:**

- 0 bis 2347

**Default:** 16

#### 2.23.20.2.11 Soft-Retries

Wenn ein Paket von der Hardware nicht verschickt werden konnte, wird mit der Anzahl der Soft-Retries festgelegt, wie oft der gesamte Sendeversuch wiederholt werden soll.

Die Gesamtzahl der Versuche ist also (Soft-Retries + 1) * Hard-Retries.

Der Vorteil von Soft-Retries auf Kosten von Hard-Retries ist, dass aufgrund des Raten-Adaptionalgorithmus die nächste Serie von Hard-Retries direkt mit einer niedrigeren Rate beginnt.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Uebertragung

**Mögliche Werte:**

- 0 bis 999

**Default:** 0

#### 2.23.20.2.12 Hard-Retries

Dieser Wert gibt an, wie oft die Hardware versuchen soll, Pakete zu verschicken, bevor sie als Tx-Fehler gemeldet werden. Kleinere Werte ermöglichen es so, dass ein nicht zu versendendes Paket den Sender weniger lange blockiert.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Uebertragung

**Mögliche Werte:**

- 0 bis 15

**Default:** 10

#### 2.23.20.2.13 Kurzes-Guard-Intervall

In der Standardeinstellung wird das Guard-Intervall automatisch optimal eingestellt. Wenn die momentanen Betriebsbedingungen es zulassen wird ein kurzes Intervall zugelassen.

Weiterhin haben Sie die Möglichkeit diese Automatik abzuschalten, um das kurze Guard-Intervall bewusst zu verhindern.

Das Guard-Intervall dient grob gesagt dazu die Störanfälligkeit bei Mehrträgerverfahren (OFDM) durch Intersymbolinterferenz (ISI) zu minimieren.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Uebertragung/Kurzes-Guard-Intervall

**Mögliche Werte:**

- aktiviert
- deaktiviert

**Default:** aktiviert

#### 2.23.20.2.14 Max.-Spatiale-Stroeme

Die Spatial-Streams fügen der bisherigen Frequenz-Zeit-Matrix vom Prinzip her eine 3. Dimension, den Raum hinzu. Mehrere Antennen verhelfen dem Empfänger zu räumlichen Informationen, was zur Steigerung der Übertragungsrate (Spatial-Multiplexing) genutzt werden kann. Dabei werden mehrere Datenströme parallel in einem Funkkanal übertragen. Gleichzeitig können auch mehrere Sende- und Empfangsantennen verwendet werden. Dadurch verbessert sich die Leistung des ganzen Funksystems erheblich.

In der Standardeinstellung werden die Spatial-Streams automatisch eingestellt, um das Funksystem optimal zu nutzen.

Weiterhin haben Sie die Möglichkeit die Spatial-Streams auf einen oder zwei einzustellen um das Funksystem beispielsweise bewusst geringer zu belasten.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Uebertragung/Max.-Spatiale-Stroeme

**Mögliche Werte:**

- automatisch
- einer
- zwei

**Default:** automatisch

#### 2.23.20.2.15 Sende-Aggregate

Hier finden Sie die Einstellungen für die Frame-Aggregation. Frame-Aggregation ist als offizieller Standard und herstellerunabhängig im 802.11n Standard vorgesehen. Er gleicht dem seit längerem bekannten Burst-Modus.

Bei Frame-Aggregation wird das WLAN-Frame soweit verlängert, dass mehrere Ethernet-Pakete hinein passen. Mit diesem Verfahren wird die Wartezeit zwischen den Datenpaketen verkürzt und der Durchsatz gesteigert. Der Overhead wird reduziert und kann für die Übertragung der Daten genutzt werden.

Mit der zunehmenden Länge der Frames steigt aber auch die Wahrscheinlichkeit, dass durch Funkstörung die Pakete nochmal gesendet werden müssen. Außerdem müssen andere Stationen länger auf einen freien Kanal warten und sie müssen die Datenpakete sammeln bis mehrere auf einmal gesendet werden können. In der Standardeinstellung ist die Frame-Aggregation eingeschaltet. Wenn Sie den Datendurchsatz dieser Station erhöhen möchten und andere auf diesem Medium nicht von Bedeutung sind, ist dies sinnvoll. .

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Uebertragung/Sende-Aggregate

**Mögliche Werte:**

- ja
- nein

**Default:** ja

#### 2.23.20.2.16 Min.-HT-MCS

MCS (Modulation Coding Scheme) dient der automatischen Geschwindigkeitsanpassung und definiert im 802.11n-Standard eine Reihe von Variablen, die beispielsweise die Anzahl der Spatial-Streams, Modulation und die Datenrate eines jeden Datenstroms festlegen.

In der Standardeinstellung wählt die Station automatisch die für den jeweiligen Stream optimalen MCS entsprechend den derzeitigen Kanalbedingungen aus. Wenn sich während des Betriebs beispielsweise Interferenzen durch Bewegung des Senders oder Abschwächung des Signals ergeben und sich dadurch die jeweiligen Kanalbedingungen ändern, wird das MCS dynamisch an die neuen Bedingungen angepasst.

Weiterhin haben Sie die Möglichkeit die MCS bewusst auf einen konstanten Wert einzustellen. Das kann für den Testbetrieb hilfreich sein oder bei Chaotischen Umgebungsbedingungen ein unnötiges Parametrieren vermeiden, wenn sowieso kein optimaler Betriebspunkt zu erwarten ist.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Uebertragung/Min.-HT-MCS

**Mögliche Werte:**

- automatisch
- MCS 0/8
- MCS 1/9
- MCS 2/10
- MCS 3/11
- MCS 4/12
- MCS 5/13
- MCS 6/14
- MCS 7/15

**Default:** automatisch

#### 2.23.20.2.17 Max.-HT-MCS

MCS (Modulation Coding Scheme) dient der automatischen Geschwindigkeitsanpassung und definiert im 802.11n-Standard eine Reihe von Variablen, die beispielsweise die Anzahl der Spatial-Streams, Modulation und die Datenrate eines jeden Datenstroms festlegen.

In der Standardeinstellung wählt die Station automatisch die für den jeweiligen Stream optimalen MCS entsprechend den derzeitigen Kanalbedingungen aus. Wenn sich während des Betriebs beispielsweise Interferenzen durch Bewegung des Senders oder Abschwächung des Signals ergeben und sich dadurch die jeweiligen Kanalbedingungen ändern, wird das MCS dynamisch an die neuen Bedingungen angepasst.

Weiterhin haben Sie die Möglichkeit die MCS bewusst auf einen konstanten Wert einzustellen. Das kann für den Testbetrieb hilfreich sein oder bei Chaotischen Umgebungsbedingungen ein unnötiges Parametrieren vermeiden, wenn sowieso kein optimaler Betriebspunkt zu erwarten ist.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Uebertragung/Max.-HT-MCS

**Mögliche Werte:**

- automatisch
- MCS 0/8
- MCS 1/9
- MCS 2/10
- MCS 3/11
- MCS 4/12
- MCS 5/13
- MCS 6/14
- MCS 7/15

**Default:** automatisch

#### 2.23.20.2.18 Min.-Spatiale-Stroeme

Die Spatial-Streams fügen der bisherigen Frequenz-Zeit-Matrix vom Prinzip her eine 3. Dimension, den Raum hinzu. Mehrere Antennen verhelfen dem Empfänger zu räumlichen Informationen, was zur Steigerung der Übertragungsrate (Spatial-Multiplexing) genutzt werden kann. Dabei werden mehrere Datenströme parallel in einem Funkkanal übertragen. Gleichzeitig können auch mehrere Sende- und Empfangsantennen verwendet werden. Dadurch verbessert sich die Leistung des ganzen Funksystems erheblich.

In der Standardeinstellung werden die Spatial-Streams automatisch eingestellt, um das Funksystem optimal zu nutzen.

Weiterhin haben Sie die Möglichkeit die Spatial-Streams auf einen oder zwei einzustellen um das Funksystem beispielsweise bewusst geringer zu belasten.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Uebertragung/Min.-Spatiale-Stroeme

**Mögliche Werte:**

- automatisch
- einer
- zwei

**Default:** automatisch

#### 2.23.20.2.19 EAPOL-Rate

Legen Sie hier die Datenrate für die Übertragung der EAPOL-Pakete fest.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Uebertragung

**Mögliche Werte:**

- Wie-Daten

Auswahl aus den angebotenen Geschwindigkeiten:

- 1M
- 2M
- 5.5M

- 11M
- 6M
- 9M
- 12M
- 18M
- 24M
- 36M
- 48M
- 54M
- T-12M
- T-18M
- T-24M
- T-36M
- T-48M
- T-72M
- T-96M
- T-108M

**Default:** Wie-Daten

**Besondere Werte:** Wie-Daten überträgt die EAPOL-Daten mit der gleichen Datenrate wie die Nutzdaten.

#### 2.23.20.2.2 Paketgroesse

Bei kleinen Datenpaketen ist die Gefahr für Übertragungsfehler geringer als bei großen Paketen, allerdings steigt auch der Anteil der Header-Informationen am Datenverkehr, die effektive Nutzlast sinkt also. Erhöhen Sie den voreingestellten Wert nur, wenn das Funknetzwerk überwiegend frei von Störungen ist und nur wenig Übertragungsfehler auftreten. Reduzieren Sie den Wert entsprechend, um die Übertragungsfehler zu vermeiden.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Uebertragung

**Mögliche Werte:**

- 500 bis 1600 (nur gerade Werte)

**Default:** 1600

#### 2.23.20.2.20 Max.-Aggr.-Paket-Anzahl

Dieser Parameter definiert, wie viele Pakete maximal zu einem Aggregat zusammengepackt werden dürfen. Die Aggregierung bei WLAN-Übertragungen nach IEEE 802.11n fasst mehrere Datenpakete zu einem großen Paket zusammen, reduziert so den Overhead und beschleunigt die Übertragung.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Uebertragung/Max.-Aggr.-Paket-Anzahl

**Mögliche Werte:**

- maximal 2 numerische Zeichen

**Default:** 16

#### 2.23.20.2.21 ProbeRsp-Retries

Dies ist die Anzahl der Hard-Retries für Probe-Responses, also Antworten, die ein Access Point als Antwort auf einen Probe-Request von einem Client schickt.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Uebertragung

**Mögliche Werte:**

- 0 bis 15

**Default:** 3

Werte größer als 15 werden wie 15 behandelt.

#### 2.23.20.2.3 Min-Tx-Rate

Der Access Point handelt mit den angeschlossenen WLAN-Clients die Geschwindigkeit für die Datenübertragung normalerweise fortlaufend dynamisch aus. Dabei passt der Access Point die Übertragungsgeschwindigkeit an die Empfangslage aus. Alternativ können Sie hier die minimale Übertragungsgeschwindigkeit fest vorgeben, wenn Sie die dynamische Geschwindigkeitsanpassung verhindern wollen.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Uebertragung

**Mögliche Werte:**

- Automatisch
- Auswahl aus den angebotenen Geschwindigkeiten

**Default:** Automatisch

#### 2.23.20.2.4 Basis-Rate

Die eingestellte Broadcastgeschwindgkeit sollte es auch unter ungünstigen Bedingungen erlauben, die langsamsten Clients im WLAN zu erreichen. Stellen Sie hier nur dann eine höhere Geschwindigkeit ein, wenn alle Clients in diesem logischen WLAN auch „schneller" zu erreichen sind.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Uebertragung

**Mögliche Werte:**

- Auswahl aus den angebotenen Geschwindigkeiten

**Default:** 2 Mbit/s

#### 2.23.20.2.6 RTS-Schwelle

Mit dem RTS-Schwellwert wird das Phänomen der „Hidden-Station" durch Verwendung des RTS/CTS-Protokolls vermieden.

Eine Kollision bei den recht kurzen RTS-Paketen ist sehr unwahrscheinlich, die Verwendung von RTS/CTS erhöht aber dennoch den Overhead. Der Einsatz dieses Verfahrens lohnt sich daher nur für längere Datenpakete, bei denen Kollisionen wahrscheinlich sind. Mit dem RTS-Schwellwert wird eingestellt, ab welcher Paketlänge das RTS/CTS eingesetzt werden soll. Der passende Werte ist in der jeweiligen Umgebung im Versuch zu ermitteln.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Uebertragung

**Mögliche Werte:**

- 512 bis 2347

**Default:** 2347

#### 2.23.20.2.7 11b-Praeambel

Normalerweise handeln die Clients im 802.11b-Modus die Länge der zu verwendenden Präambel mit dem Access Point selbst aus. Stellen Sie hier die „lange Präambel" nur dann fest ein, wenn die Clients diese feste Einstellung verlangen.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Uebertragung

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

#### 2.23.20.2.9 Max-Tx-Rate

Der Access Point handelt mit den angeschlossenen WLAN-Clients die Geschwindigkeit für die Datenübertragung normalerweise fortlaufend dynamisch aus. Dabei passt der Access Point die Übertragungsgeschwindigkeit an die Empfangslage aus. Alternativ können Sie hier die maximale Übertragungsgeschwindigkeit fest vorgeben, wenn Sie die dynamische Geschwindigkeitsanpassung verhindern wollen.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Uebertragung

**Mögliche Werte:**

- Automatisch
- Auswahl aus den angebotenen Geschwindigkeiten

**Default:** Automatisch

### 2.23.20.3 Verschluesselung

Hier können Sie für jedes logische Wireless-LAN-Netzwerk (MultiSSID) Ihres Gerätes spezifische Verschlüsselungs-Einstellungen vornehmen.

**SNMP-ID:** 2.23.20.3

**Pfad Telnet:** /Setup/Schnittstellen/WLAN

#### 2.23.20.3.1 Ifc

Öffnet die WPA- / Einzel-WEP-Einstellungen für die logischen WLAN-Netzwerke

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Verschluesselung

**Mögliche Werte:**

- Auswahl aus den verfügbaren logischen WLAN-Netzwerken.

#### 2.23.20.3.10 Client-EAP-Methode

LANCOM Wireless Router und Access Points in der Betriebsart als WLAN-Client können sich über EAP/802.1X bei einem anderen Access Point authentifizieren. Zur Aktivierung der EAP/802.1X-Authentifizierung im Client-Modus wird bei den Verschlüsselungsmethoden für das erste logische WLAN-Netzwerk die Client-EAP-Methode ausgewählt.

Beachten Sie, dass die gewählte Client-EAP-Methodezu den Einstellungen des Access Points passen muss, bei dem sich der LANCOM Access Point einbuchen will.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Verschluesselung

**Mögliche Werte:**

- TLS
- TTLS/PAP
- TTLS/CHAP
- TTLS/MSCHAP
- TTLS/MSCHAPv2
- TTLS/MD5
- PEAP/MSCHAPv2

**Default:** TLS

Beachten Sie neben der Einstellung der Client-EAP-Methode auch die entsprechende Einstellung der Betriebsart als WLAN-Client.

#### 2.23.20.3.11 WPA-Rekeying-Zyklus

Angabe, wie oft der WPA-Key-Handshake während einer bestehenden Verbindung wiederholt werden soll (Rekeying)

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Verschluesselung

**Mögliche Werte:**

- 0 bis 4294967295 s

**Default:** 0

**Besondere Werte:** 0 = Rekeying deaktiviert

#### 2.23.20.3.12 WPA1-Sitzungsschluessel

Wählen Sie hier die Verfahren aus, welche zur Generierung der WPA-Sitzungs- bzw -Gruppen-Schlüssel angeboten werden sollen. Es können das Temporal Key Integrity Protokoll (TKIP), der Advanced Encryption Standard (AES) oder beide angeboten werden.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Verschluesselung

**Mögliche Werte:**

- TKIP
- AES
- TKIP/AES

**Default:** TKIP

#### 2.23.20.3.13 WPA2-Sitzungsschluessel

Wählen Sie hier die Verfahren aus, welche zur Generierung der WPA-Sitzungs- bzw -Gruppen-Schlüssel angeboten werden sollen. Es können das Temporal Key Integrity Protokoll (TKIP), der Advanced Encryption Standard (AES) oder beide angeboten werden.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Verschluesselung

**Mögliche Werte:**

- TKIP
- AES
- TKIP/AES

**Default:** AES

### 2.23.20.3.2 Verschluesselung

Aktiviert die Verschlüsselung für dieses logische WLAN

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Verschluesselung

**Mögliche Werte:**

- Ein
- Aus

**Default:** Ein

### 2.23.20.3.3 Vorgabeschluessel

Wählt den WEP-Schlüssel aus, mit dem die von diesem logischen WLAN gesendeten Pakete verschlüsselt werden.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Verschluesselung

**Mögliche Werte:**

- Schlüssel 1
- Schlüssel 2
- Schlüssel 3
- Schlüssel 4

**Default:** Schlüssel 1

Schlüssel 1 gilt nur für das aktuelle logische WLAN, Schlüssel 2 bis 4 sind als Gruppenschlüssel für alle logischen WLANs der gleichen physikalischen Schnittstelle gültig.

#### 2.23.20.3.4 Methode

Wählt das Verschlüsselungs-Verfahren bzw. bei WEP die Schlüssellange aus, die bei der Verschlüsselung von Datenpaketen auf dem Wireless-LAN verwendet wird.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Verschluesselung

**Mögliche Werte:**

- 802-11i-(WPA)-PSK
- WEP-156 (128 Bit)
- WEP-128 (104 Bit)
- WEP-64 (40 Bit)
- 802-11i-(WPA)-802.1x
- WEP-156 (128 Bit)-802.1x
- WEP-128 (104 Bit)-802.1x
- WEP-64 (40 Bit)-802.1x

**Default:** WEP-128 (104 Bit)

Beachten Sie, dass nicht jedes Verschlüsselungs-Verfahren von jeder Wireless-Karte unterstützt wird.

#### 2.23.20.3.5 Authentifizierung

Für die Nutzung von WEP kann das Verschlüsselungsverfahren ausgewählt werden.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Verschluesselung

**Mögliche Werte:**

- Open-System: Beim Open-System-Authentifizierungsverfahren werden grundsätzlich alle Clients angenommen. Es findet keine Authentifizierung statt. Die Daten müssen von den WLAN-Clients immer korrekt verschlüsselt übertragen werden, um von der Basisstation weitergeleitet zu werden.
- Shared-Key: Beim Shared-Key-Authentifizierungsverfahren muss der WLAN-Client zunächst ein vom Server geliefertes Datenpaket korrekt verschlüsselt zurücksenden, um authentifiziert zu werden. Erst danach werden von ihm verschlüsselte Daten akzeptiert und weitergeleitet. Dadurch steht einem Angreifer allerdings ein Datenpaket in seiner unverschlüsselten und in seiner verschlüsselten Form zur Verfügung, wodurch der Schlüssel selbst angreifbar wird.

**Default:** Open-System

Aufgrund der Sicherheitsaspekte wird grundsätzlich das Open-System-Authentifizierungsverfahren empfohlen.

#### 2.23.20.3.6 Schluessel

Sie können die Schlüssel oder Passphrases als ASCII-Zeichenkette eingeben. Bei WEP ist alternativ die Eingabe einer Hexadezimalzahl durch ein vorangestelltes 'Ox' möglich.

Folgende Langen ergeben sich für die verwendeten Formate:

Verfahren Länge

WPA-PSK 8 bis 63 ASCII-Zeichen

WEP152 (128 bit) 16 ASCII-oder 32 HEX-Zeichen

WEP128 (104 bit) 13 ASCII-oder 26 HEX-Zeichen

WEP64 (40 bit) 5 ASCII-oder 10 HEX-Zeichen

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Verschluesselung

**Mögliche Werte:**

- ASCII-Zeichenkette oder Hexadezimalzahl

**Default:** Leer

Bei Verwendung von 802.1x im AP-Modus verweist der hier eingetragene Name auf den zu verwendenden RADIUS-Server.

Bei Verwendung von 802.1x im Client-Modus und PEAP oder TTLS als Client-EAP-Methode werden hier die Zugangsdaten (user:password) hinterlegt.

#### 2.23.20.3.9 WPA-Version

Mit dieser WPA-Version werden die Daten in diesem logischen WLAN verschlüsselt.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Verschluesselung

**Mögliche Werte:**

- WPA1
- WPA2
- WPA1/2

**Default:** WPA1/2

### 2.23.20.4 Gruppen-Schluessel

Hier definieren Sie für jedes physikalische Wireless-LAN-Interface Ihres Gerätes die WEP-Gruppen-Schlüssel 2 bis 4, die von allen darauf aufgespannten logischen Wireless-LAN-Netzen gemeinsam genutzt werden.

**SNMP-ID:** 2.23.20.4

**Pfad Telnet:** /Setup/Schnittstellen/WLAN

Wenn 802.1x/EAP aktiviert ist werden die Gruppenschlüssel von 802.1x/EAP verwendet und stehen damit nicht mehr für die WEP-Verschlüsselung zur Verfügung.

#### 2.23.20.4.1 Ifc

Öffnet die WEP-Gruppen-Schlüssel für die physikalische WLAN-Schnittstelle.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Gruppen-Schluessel

**Mögliche Werte:**

- Auswahl aus den verfügbaren physikalischen WLAN-Schnittstellen.

#### 2.23.20.4.3 Schluessel-2

WEP-Gruppenschlüssel 2

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Gruppen-Schluessel

**Mögliche Werte:**

- Sie können den Schlüssel als ASCII-Zeichenkette oder Hexadezimalzahl (mit vorangestelltem 'Ox') eintragen
- Folgende Langen ergeben sich für die verwendeten Formate:
- Verfahren Länge
- WEP152 (128 bit) 16 ASCII-oder 32 HEX-Zeichen
- WEP128 (104 bit) 13 ASCII-oder 26 HEX-Zeichen
- WEP64 (40 bit) 5 ASCII-oder 10 HEX-Zeichen

**Default:** Leer

#### 2.23.20.4.4 Schluessel-3

WEP-Gruppenschlüssel 3

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Gruppen-Schluessel

**Mögliche Werte:**

- Sie können den Schlüssel als ASCII-Zeichenkette oder Hexadezimalzahl (mit vorangestelltem 'Ox') eintragen
- Folgende Langen ergeben sich für die verwendeten Formate:
- Verfahren Länge
- WEP152 (128 bit) 16 ASCII-oder 32 HEX-Zeichen
- WEP128 (104 bit) 13 ASCII-oder 26 HEX-Zeichen
- WEP64 (40 bit) 5 ASCII-oder 10 HEX-Zeichen

**Default:** Leer

#### 2.23.20.4.5 Schluessel-4

WEP-Gruppenschlüssel 4

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Gruppen-Schluessel

**Mögliche Werte:**

- Sie können den Schlüssel als ASCII-Zeichenkette oder Hexadezimalzahl (mit vorangestelltem 'Ox') eintragen
- Folgende Langen ergeben sich für die verwendeten Formate:
- Verfahren Länge
- WEP152 (128 bit) 16 ASCII-oder 32 HEX-Zeichen
- WEP128 (104 bit) 13 ASCII-oder 26 HEX-Zeichen
- WEP64 (40 bit) 5 ASCII-oder 10 HEX-Zeichen

**Default:** Leer

#### 2.23.20.4.7 Schluessel-Typ-2

Wählt die Schlüssellänge, die für den WEP-Gruppenschlüssel 2 verwendet werden soll.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Gruppen-Schluessel

**Mögliche Werte:**

- WEP-156 (128 Bit)
- WEP-128 (104 Bit)
- WEP-64 (40 Bit)

**Default:** WEP-64 (40 Bit)

#### 2.23.20.4.8 Schluessel-Typ-3

Wählt die Schlüssellänge, die für den WEP-Gruppenschlüssel 3 verwendet werden soll.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Gruppen-Schluessel

**Mögliche Werte:**

- WEP-156 (128 Bit)
- WEP-128 (104 Bit)
- WEP-64 (40 Bit)

**Default:** WEP-64 (40 Bit)

#### 2.23.20.4.9 Schluessel-Typ-4

Wählt die Schlüssellänge, die für den WEP-Gruppenschlüssel 4 verwendet werden soll.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Gruppen-Schluessel

**Mögliche Werte:**

- WEP-156 (128 Bit)
- WEP-128 (104 Bit)
- WEP-64 (40 Bit)

**Default:** WEP-64 (40 Bit)

### 2.23.20.5 Interpoint-Einstellungen

Hier können Sie wichtige Parameter für die Kommunikation zwischen Basisstationen vornehmen, bzw. das Verhalten für diese festlegen.

**SNMP-ID:** 2.23.20.5

**Pfad Telnet:** /Setup/Schnittstellen/WLAN

#### 2.23.20.5.1 Ifc

Öffnet die Einstellungen für die physikalische WLAN-Schnittstelle.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Interpoint-Gegenstellen

**Mögliche Werte:**

- Auswahl aus den verfügbaren physikalischen WLAN-Schnittstellen.

#### 2.23.20.5.10 Kanalwahlverfahren

Bei der automatischen Suche nach einem freien WLAN-Kanal kann es im 5 GHz-Band zu gleichzeitigen Sendeversuchen mehrerer Access Points kommen, die sich in der Folge gegenseitig nicht finden. Diese Pattsituationen kann mit dem geeigneten „Kanalwahlverfahren“ verhindert werden.

Es ist daher empfehlenswert, im 5 GHz-Band jeweils einen zentralen Access Point als 'Master' und alle anderen Punkt-zu-Punkt-Partner als 'Slave' zu konfigurieren. Auch im 2,4 GHz-Band bei aktivierter automatischer Kanalsuche erleichtert diese Einstellung den Aufbau von Punkt-zu-Punkt-Verbindungen.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Interpoint-Gegenstellen

**Mögliche Werte:**

- Master: Dieser Access Point übernimmt die Führung bei der Auswahl eines freien WLAN-Kanals.
- Slave: Alle anderen Access Points suchen solange, bis sie einen sendenden Master gefunden haben.

**Default:** Master

Für die Verschlüsselung von Punkt-zu-Punkt-Verbindungen mit 802.11i/WPA ist die korrekte Konfiguration der Kanalwahlverfahren zwingend erforderlich.

#### 2.23.20.5.11 Link-Verlust-Timeout

Zeit in Sekunden, nach der ein (DFS-)Slave eine Verbindung zum Master als verloren betrachtet, wenn keine Beacons empfangen werden,

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Interpoint-Gegenstellen

**Mögliche Werte:**

- 0 bis 4294967295 Sekunden

**Default:** 4

#### 2.23.20.5.12 Key-Handshake-Rolle

Legt fest, ob bei Verwendung von WPA diese Seite als Authenticator oder Supplicant arbeiten soll. Im Default-Modus ist der Master einer Strecke Authenticator, im Auto-Modus ist die Seite mit der niedrigeren MAC-Adresse Authenticator

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Interpoint-Gegenstellen

**Mögliche Werte:**

- Default
- Auto

**Default:** Default

#### 2.23.20.5.13 Lokaler-Name

Geben Sie hier einen im WLAN eindeutigen Namen für diese physikalische WLAN-Schnittstelle ein. Dieser Name kann auf anderen WLAN-Geraten genutzt werden, um diese Basisstation über Punkt-zu-Punkt anzubinden.

Sie können dieses Feld frei lassen, wenn das Gerat nur eine WLAN-Schnittstelle hat und bereits ein im WLAN eindeutiger Geräte-Name konfiguriert ist oder die übrigen Basisstation diese Schnittstelle aber die MAC-Adresse des WLAN-Adapters identifizieren.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Interpoint-Gegenstellen

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** Leer

### 2.23.20.5.2 Freigeben

Das Verhalten eines Access Points beim Datenaustausch mit anderen Access Points wird in der „Punkt-zu-Punkt-Betriebsart" festgelegt.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Interpoint-Gegenstellen

**Mögliche Werte:**

- Aus: Der Access Point kann nur mit mobilen Clients kommunizieren
- An: Der Access Point kann mit anderen Basis-Stationen und mit mobilen Clients kommunizieren
- Exklusiv: Der Access Point kann nur mit anderen Basis-Stationen kommunizieren

**Default:** Aus

#### 2.23.20.5.9 Isolierter-Modus

Erlaubt oder verbietet die Übertragung von Paketen zwischen P2P-Links auf der gleichen WLAN-Schnittstelle (Kompatibilitätseinstellung für LCOS-Versionen vor 2.70)

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Interpoint-Gegenstellen

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

### 2.23.20.6 Client-Einstellungen

Wenn Sie ihr LANCOM Wireless-Gerät im Client-Modus betreiben, können Sie detaillierte Einstellung an dessen Verhalten vornehmen.

**SNMP-ID:** 2.23.20.6

**Pfad Telnet:** /Setup/Schnittstellen/WLAN

#### 2.23.20.6.1 Ifc

Öffnet die Einstellungen für die physikalische WLAN-Schnittstelle.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Client-Einstellungen

**Mögliche Werte:**

- Auswahl aus den verfügbaren physikalischen WLAN-Schnittstellen.

#### 2.23.20.6.10 Rx-Limit

Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients.

Ein Client übermittelt seine eigene Einstellung bei der Anmeldung an die Basisstation. Diese bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Client-Einstellungen

**Mögliche Werte:**

- 0 bis 4294967296 (2^32)

**Default:** 0

**Besondere Werte:** 0: keine Begrenzung

Die Bedeutung der Werte Rx und Tx ist abhängig von der Betriebsart des Gerätes. In diesem Fall als Access Point steht Rx für „Daten senden“ und Tx für „Daten empfangen“.

#### 2.23.20.6.12 Auswahl-Vorrang

Wählen Sie hier aus, wie diese Schnittstelle verwendet werden soll.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Client-Einstellungen/WLAN-1

**Mögliche Werte:**

- Signalstärke: Wählt das Profil, dessen WLAN aktuell das stärkste Signal bietet. In dieser Einstellung wechselt das WLAN-Modul im Client-Modus automatisch in ein anderes WLAN, sobald diese ein stärkeres Signal bietet.
- Profil: Wählt aus den verfügbaren WLANs das zu verwendende Profil in der Reihenfolge der definierten Einträge (WLAN-Index, z. B. WLAN-1, WLAN-1-2 etc.), auch wenn ein anderes WLAN ein stärkeres Signal bietet. In dieser

Einstellung wechselt das WLAN-Modul im Client-Modus automatisch in ein anderes WLAN, sobald ein WLAN mit einem niedrigeren WLAN-Index erkannt wird (unabhängig von der Signalstärke dieses WLANs).

**Default:** Signalstärke

#### 2.23.20.6.3 Verbindung-halten

Mit dieser Option hält die Client-Station die Verbindung zur Basisstation aufrecht, auch wenn von den angeschlossenen Geräten keine Datenpakete gesendet werden. Ist diese Option ausgeschaltet, wird die Clientstation automatisch aus dem Funknetzwerk abgemeldet, wenn für eine bestimmte Zeit keine Pakete über die WLAN-Verbindung fließen.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Client-Einstellungen

**Mögliche Werte:**

- Ein
- Aus

**Default:** Ein

#### 2.23.20.6.4 Netzwerk-Typen

Mit der Auswahl der 'Netzwerktypen' wird festgelegt, ob sich die Station nur an Infrastruktur- oder auch in Adhoc-Netzwerken anmelden darf.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Client-Einstellungen

**Mögliche Werte:**

- Infrastruktur
- Adhoc

**Default:** Infrastruktur

#### 2.23.20.6.5 Scanne-Baender

Legen Sie hier fest, ob die Clientstation nur das 2,4 GHz-, nur das 5 GHz-Band oder alle verfügbaren Bänder absuchen soll, um eine Basisstation zu finden.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Client-Einstellungen

**Mögliche Werte:**

- 2,4/5 GHz
- 2,4 GHz
- 5 GHz

**Default:** 2,4/5 GHz

#### 2.23.20.6.6 Bevorzugtes-BSS

Wenn sich die Clientstation nur bei einem bestimmten Access Point einbuchen soll, können Sie hier die MAC-Adresse der WLAN-Karte aus diesem Access Point eintragen.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Client-Einstellungen

**Mögliche Werte:**

- Gültige MAC-Adresse

**Default:** Leer

#### 2.23.20.6.7 Adress-Anpassung

Im Client-Modus ersetzt die Clientstation üblicherweise die MAC-Adressen in den Datenpaketen der an ihr angeschlossenen Geräte durch die eigene MAC-Adresse. Der Access-Point auf der anderen Seite der Verbindung „sieht" also immer nur die MAC-Adresse der Clientstation, nicht jedoch die MAC-Adresse der oder des angeschlossenen Rechners.

In manchen Installationen ist es jedoch gewünscht, dass die MAC-Adresse eines Rechners und nicht die der Clientstation an den Access Point übertragen wird. Mit der Option 'Adress-Anpassung' wird das Ersetzen der MAC-Adresse durch die Clientstation unterbunden, die Datenpakete werden mit der originalen MAC-Adresse übertragen.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Client-Einstellungen

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

Die Adress-Anpassung funktioniert nur, wenn an die Clientstation nur ein einzelner Rechner angeschlossen ist!

#### 2.23.20.6.8 Cl.-Brg.-Support

Während mit der Adress-Anpassung nur die MAC-Adresse eines einzigen angeschlossenen Gerätes für den Access Point sichtbar gemacht werden kann, werden über die Client-Bridge-Unterstützung alle MAC-Adressen der Stationen im LAN hinter der Clientstationen transparent an den Access Point übertragen.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Client-Einstellungen

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

#### 2.23.20.6.9 Tx-Limit

Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients.

Ein Client übermittelt seine eigene Einstellung bei der Anmeldung an die Basisstation. Diese bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Client-Einstellungen

**Mögliche Werte:**

- 0 bis 4294967296 (2^32)

**Default:** 0

**Besondere Werte:** 0: keine Begrenzung

Die Bedeutung der Werte Rx und Tx ist abhängig von der Betriebsart des Gerätes. In diesem Fall als Access Point steht Rx für „Daten senden" und Tx für „Daten empfangen".

### 2.23.20.7 Betriebs-Einstellungen

In den Betriebseinstellungen können Sie grundsätzliche Parameter für den Betrieb ihrer WLAN-Schnittstelle vornehmen.

**SNMP-ID:** 2.23.20.7

**Pfad Telnet:** /Setup/Schnittstellen/WLAN

#### 2.23.20.7.1 Ifc

Öffnet die Einstellungen für die physikalische WLAN-Schnittstelle.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Betriebs-Einstellungen

**Mögliche Werte:**

- WLAN-1
- WLAN-2

#### 2.23.20.7.2 Aktiv

Schaltet die physikalische WLAN-Schnittstelle separat ein- oder aus.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Betriebs-Einstellungen

**Mögliche Werte:**

- Ein
- Aus

**Default:** Ein

#### 2.23.20.7.3 Betriebsart

LANCOM Wireless-Geräte können grundsätzlich in verschiedenen Betriebsarten arbeiten.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Betriebs-Einstellungen

**Mögliche Werte:**

- Basisstation: Als Basisstation (Access Point) stellt es für die WLAN-Clients die Verbindung zu einem kabelgebundenen LAN her.
- Client: Als Client sucht das Gerät selbst die Verbindung zu einem anderen Access Point und versucht sich in einem Funknetzwerk anzumelden. In diesem Fall dient das Gerät also dazu, ein kabelgebundenes Gerät über eine Funkstrecke an eine Basisstation anzubinden.
- Managed: Als Managed-Access Point sucht das Gerät einen zentralen WLAN Controller, von dem es eine Konfiguration beziehen kann.

**Default:** LANCOM Wireless Router: Basisstation; LANCOM Access Points: Managed

#### 2.23.20.7.4 Link-LED-Funktion

Bei der Einrichtung von Point-to-Point-Verbindungen oder in der Betriebsart als WLAN-Client ist es für eine möglichst gute Positionierung der Antennen wichtig, die Empfangsstärke in verschiedenen Positionen zu erkennen. Die WLAN-Link-LED kann z. B. für die Phase der Einrichtung zur Anzeige der Empfangsqualität genutzt werden. In der entsprechenden Betriebsart blinkt die WLAN-Link-LED umso schneller, je besser die Empfangsqualität in der jeweiligen Antennenposition ist.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Betriebs-Einstellungen

**Mögliche Werte:**

- Verbindungsanzahl: In dieser Betriebsart zeigt die LED mit einem „inversen Blitzen" die Anzahl der WLAN-Clients an, die bei dem Access Point als Client eingebucht sind. Nach der Anzahl der Blitzer für jeden Client erfolgt eine kurze Pause. Wählen Sie diese Betriebsart dann, wenn Sie den LANCOM Wireless Router im Access-Point-Modus betreiben.
- Client-Signalstärke: In dieser Betriebsart zeigt die LED die Signalstärke des Access Points an, bei dem ein LANCOM Wireless Router selbst als Client eingebucht ist. Je schneller die LED blinkt, umso besser ist das Signal. Wählen Sie diese Betriebsart nur, wenn Sie den LANCOM Wireless Router im Client-Modus betreiben.

- P2P1- bis P2P6-Signalstärke: In dieser Betriebsart zeigt die LED die Signalstärke des jeweiligen P2P-Partners, mit dem ein LANCOM Wireless Router eine P2P-Strecke bildet. Je schneller die LED blinkt, umso besser ist das Signal.

**Default:** Verbindungsanzahl

#### 2.23.20.7.5 Link-Fehler-Erkennung

Wenn ein Access Point keine Verbindung zum kabelgebundenen LAN hat, kann er in den meisten Fällen seine wesentliche Aufgabe – den eingebuchten WLAN-Clients einen Zugang zum LAN zu ermöglichen – nicht mehr erfüllen. Mit der Funktion der Broken-Link-Detection (Link-Fehler-Erkennung) können die WLAN-Module eines Geräts deaktiviert werden, wenn die LAN-Verbindung verloren geht. So können die beim Access Point eingebuchten Clients einen anderen Access Point (mit ggf. schwächerem Signal) suchen und sich mit diesem verbinden.

Bis zur LCOS-Version 7.80 bezog sich die Aktivierung der Link-Fehler-Erkennung immer auf LAN-1, auch wenn das Gerät über mehrere LAN-Interfaces verfügte. Außerdem wirkte sich die Deaktivierung auf alle verfügbaren WLAN-Module des Gerätes aus. Ab LCOS-Version 8.00 kann die Link-Fehler-Erkennung gezielt an ein bestimmtes LAN-Interface gebunden werden.

Mit dieser Funktion werden die WLAN-Module des Geräts deaktiviert, wenn das zugeordnete LAN-Interface nicht über einen Link zum LAN verfügt.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Betriebs-Einstellungen/Link-Fehler-Erkennung

**Mögliche Werte:**

- Nein: Link-Fehler-Erkennung wird nicht genutzt.
- LAN-1 bis LAN-n (je nach verfügbaren LAN-Interfaces im Gerät): Alle WLAN-Module des Geräts werden deaktiviert, wenn das hier angegebene LAN-Interface keine Verbindung zum kabelgebundenen LAN hat.

**Default:**

- Nein

Die Interface-Bezeichnungen LAN-1 bis LAN-n repräsentieren die logischen LAN-Schnittstellen. Die verfügbaren physikalischen Ethernet-Ports des Geräts müssen zur Nutzung dieser Funktion ggf. auf die entsprechenden Werte LAN-1 bis LAN-n eingestellt werden.

Die Link-Fehler-Erkennung kann auch für WLAN-Geräte in der Betriebsart als WLAN-Client genutzt werden. Bei eingeschalteter Link-Fehler-Erkennung werden die WLAN-Module eines WLAN-Clients nur dann aktiviert, wenn die entsprechenden LAN-Schnittstellen eine Verbindung zum kabelgebunden LAN haben.

### 2.23.20.8 Radio-Einstellungen

Hier können Sie Einstellungen am physikalischen Sende- und Empfangsverhalten ihrer WLAN-Schnittstelle vornehmen.

**SNMP-ID:** 2.23.20.8

**Pfad Telnet:** /Setup/Schnittstellen/WLAN

#### 2.23.20.8.1 Ifc

Öffnet die Einstellungen für die physikalische WLAN-Schnittstelle.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Radio-Einstellungen

**Mögliche Werte:**

- Auswahl aus den verfügbaren physikalischen WLAN-Schnittstellen.

#### 2.23.20.8.10 AP-Dichte

Mit zunehmender Dichte von Access Points überlagern sich die Empfangsbereich der Antennen. Mit der Einstellung der 'Basisstations-Dichte' kann die Empfangs-Empfindlichkeit der Antennen reduziert werden.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Radio-Einstellungen

**Mögliche Werte:**

- Niedrig
- Mittel
- Hoch
- Mini-Zelle
- Mikro-Zelle

**Default:** Niedrig

#### 2.23.20.8.12 Antennengewinn

Mit diesem Eintrag können Sie den Antennen-Verstärkungsfaktor (Gewinn in dBi) abzüglich der Dämpfungen für Kabel und (evtl.) Blitzschutz angeben. Hieraus errechnet Ihre Basisstation die in Ihrem Land und für das jeweilige Frequenzband maximal zulässige Sendeleistung.

Die Sendeleistung kann minimal auf 0,5 dBm im 2,4-GHz-Band bzw. 6,5 dBm im 5-GHz-Band reduziert werden. Das begrenzt den maximal einzutragenden Wert im 2,4-GHz-Band auf 17,5 dBi, im 5-GHz-Band auf 11,5 dBi. Bitte achten Sie darauf, dass Ihr Antennen/Kabel/Blitzschutz-Setup unter diesen Bedingungen den Regulierungsanforderungen des Landes entspricht, in dem Sie das System einsetzen.

Die Empfindlichkeit des Empfängers bleibt hiervon unbeeinflusst.

**Beispiel:** AirLancer O-18a: Antennengewinn: 18dBi, Kabeldämfung: 4dB --> Einzutragender Wert = 18dBi - 4dB = 14dBi.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Radio-Einstellungen

**Mögliche Werte:** max. 4 Zeichen

**Default:** 3

Das Minimum von 6,5 dBm gilt nur bei alten abg-Funkmodulen mit WLAN im G-Modus.

Die aktuelle Sendeleistung können Sie mit Hilfe des Web-Interfaces des Gerätes oder per Telnet unter 'Status->WLAN-Statistik->WLAN-Parameter->Sendeleistung' oder per LANmonitor unter 'System-Informationen->WLAN-Karte->Sendeleistung' einsehen.

#### 2.23.20.8.13 Kanalliste

Bei automatischer Kanalwahl oder im Client-Modus legt dieses Feld die Untermenge der zu benutzenden Kanäle fest.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Radio-Einstellungen

**Mögliche Werte:**

- Kommaseparierte Liste von einzelnen Zahlen oder Bereichen.

**Default:** leer

#### 2.23.20.8.14 Hintergrund-Scan

Zur Erkennung anderer Access Points in der eigenen Funkreichweite können LANCOM Wireless Router die empfangenen Beacons (Management-Frames) aufzeichnen und in der Scan-Tabelle speichern. Da diese Aufzeichnung im Hintergrund neben der „normalen" Funktätigkeit der Access Points abläuft, wird diese Funktion auch als „Background Scan" bezeichnet.

Wird hier ein Wert angegeben, so sucht der LANCOM Wireless Router innerhalb dieses Intervalls zyklisch die aktuell ungenutzten Frequenzen des aktiven Bandes nach erreichbaren Access Points ab.

Für LANCOM Wireless Router im Access-Point-Modus wird die Background-Scan-Funktion üblicherweise zur Rogue AP Detection eingesetzt. Das Scan-Intervall sollte hier der Zeitspanne angepasst werden, innerhalb derer unbefugte Access Points erkannt werden sollen, z. B. 1 Stunde.

Für LANCOM Wireless Router im Client-Modus wird die Background-Scan-Funktion hingegen meist für ein besseres Roaming von mobilen WLAN-Clients genutzt. Um ein schnelles Roaming zu erzielen, wird die Scan-Zeit hierbei auf z. B. 260 Sekunden beschränkt.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Radio-Einstellungen

**Mögliche Werte:**

- 0 bis 4294967295

**Default:** 0

**Besondere Werte:** 0: Mit einer Hintergrund-Scan-Zeit von '0' wird die Funktion des Background-Scanning ausgeschaltet.

#### 2.23.20.8.15 DFS-Rescan-Stunden

In einigen Ländern ist das DFS-Verfahren zur automatischen Kanalsuche vorgeschrieben.

Beim DFS-Verfahren (Dynamic Frequency Selection) wird automatisch eine freie Frequenz gewählt, z. B. um das Stören von Radaranlagen zu verhindern und um die WLAN-Geräte möglichst gleichmäßig über das ganze Frequenzband zu verteilen. Nach dem Einschalten oder Booten wählt das Gerät aus den (z. B. aufgrund der Ländereinstellungen) verfügbaren Kanälen einen zufälligen Kanal aus und prüft, ob auf diesem Kanal ein Radarsignal gefunden wird und ob auf diesem Kanal schon ein anderes Wireless LAN arbeitet. Dieser Scan-Vorgang wird solange wiederholt, bis ein radarfreier Kanal mit möglichst wenig anderen Netzwerken gefunden wurde. Anschließend wird der gewählte Kanal erneut für 60 Sekunden beobachtet, um evtl. auftretende Radarsignale sicher auszuschließen. Die Datenübertragung kann daher durch diesen Scan-Vorgang und die erneute Suche eines freien Kanals für 60 Sekunden unterbrochen werden.

Damit der 60-Sekunden-Scanvorgang nicht zur unpassenden Zeit ausgelöst wird, können Sie die gewünschten Zeitpunkte für den Scanvorgang einstellen, zu denen das Löschen der DFS-Datenbank erzwungen wird. Für die Definition der Stunde können die Möglichkeiten der cron-Befehle genutzt werden, z. B. '1,6,13' für einen DFS-Scan immer um 1 Uhr, um 6 und um 13 Uhr oder '0-23/4' für einen DFS-Scan in der Zeit von 0 bis 23 Uhr alle vier Stunden.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Radio-Einstellungen

**Mögliche Werte:**

- Kommaseparierte Liste von Stunden

**Default:** Leer



Voraussetzung für das Erzwingen des DFS-Scans ist eine korrekte Systemzeit im Gerät.

#### 2.23.20.8.16 Erlaube-40MHz

In der Standardeinstellung wird die Bandbreite automatisch optimal eingestellt. Wenn die momentanen Betriebsbedingungen es zulassen wird eine Bandbreite von 40MHz zugelassen, ansonsten wird sie auf 20MHz begrenzt.

Weiterhin haben Sie die Möglichkeit diese Automatik abzuschalten, um die Bandbreite bewusst schmal auf 20MHz begrenzt zu halten.

Beim 802.11n Standard ist eine Bandbreitenverdopplung (Channel Bonding) von 20MHz auf 40MHz vorgesehen.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Radio-Einstellungen/Erlaube-40MHz

#### 2.23.20.8.17 Antennen-Maske

Um den Gewinn durch Spatial-Multiplexing zu optimieren ist es notwendig die Antennengruppierung optimal zu konfigurieren. In der Standardeinstellung wird die Gruppierung automatisch anhand der gegenwärtigen Bedingungen optimal gewählt. Weiterhin haben Sie die Möglichkeit eine Antennengruppe mit beliebiger Antennenkombination manuell einzustellen. Die Einstellung hat sowohl Einfluss auf das Abstrahl-, als auch auf das Empfangsverhalten des Funksystems.

**SNMP-ID:** 2.23.20.8.17

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Radio-Einstellungen/Antennen-Maske

**Mögliche Werte:**

- Auto
- Antenne-1
- Antenne-1+2
- Antenne-1+3
- Antenne-1+2+3

**Default:** Auto

#### 2.23.20.8.18 Hintergrund-Scan-Einheit

Einheit für die Angabe des Background-Scan-Intervalls

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Radio-Einstellungen

**Mögliche Werte:**

- Millisekunden
- Sekunden
- Minuten
- Stunden
- Tage

**Default:** Sekunden

#### 2.23.20.8.19 Kanal-Paarung

Dieser Wert bestimmt bei 11n-Geräten im 40-MHz-Modus, welche Kanalpaare das Gerät verwendet.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Radio-Einstellungen/Kanal-Paarung

**Mögliche Werte:**

- 11n-konform: das Gerät die Kanäle nach Vorschrift der 802.11n. Dabei verschieben sich die 40-MHz-Kanäle gegenüber den alten, proprietären Kanälen im Turbo-Modus um 20 MHz.
- legacy-turbo-freundlich: nur sinnvoll im Outdoor-Bereich, um Überlappungen mit anderen 11a-Strecken im Turbo-Modus zu vermeiden.

**Default:** 11n-konform

#### 2.23.20.8.2 Sende-Leistungs-Reduktion

Im Gegensatz zum Antennen-Gewinn reduziert der Eintrag im Feld 'Sendeleistungs-Reduktion' die Leistung immer statisch um den dort eingetragenen Wert, ohne Berücksichtigung der anderen Parameter.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Radio-Einstellungen

**Mögliche Werte:**

- 0 bis 999 dB

**Default:** 0

Durch die Sendeleistungsreduktion wird nur die abgestrahlte Leistung reduziert. Die Empfangsempfindlichkeit (der Empfangs-Antennengewinn) der Antennen bleibt davon unberührt. Mit dieser Variante können z. B. bei Funkbrücken große Entfernungen durch den Einsatz von kürzeren Kabeln überbrückt werden. Der Empfangs-Antennengewinn wird erhöht, ohne die gesetzlichen Grenzen der Sendeleistung zu übersteigen. Dadurch wird die maximal mögliche Distanz und insbesondere die erreichbare Datenübertragungsgeschwindigkeit verbessert.

#### 2.23.20.8.20 Bevorzugtes-DFS-Schema

Alle WLAN-Systeme, die nach Inkrafttreten der EN 301 893-V1.5 in Betrieb genommen werden, müssen im 5 GHz-Band DFS3 verwenden.

Hier haben Sie die Möglichkeit zwischen DFS2 (EN 301 893-V1.3) und DFS3 (EN 301 893-V1.5) zu wählen.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Radio-Einstellungen/Bevorzugtes-DFS-Schema

**Mögliche Werte:**

- EN 301 893-V1.5
- EN 301 893-V1.3

**Default:** EN 301 893-V1.5

Bei einem Upgrade von einer Firmware vor LCOS-Version 8.00 auf eine LCOS-Version 8.00 oder höher wird die vorherige Einstellung DFS2 (EN 301 893-V1.3) beibehalten.

Die Auswahl ist nicht möglich für WLAN-Geräte, die fest auf DFS3-Betrieb eingestellt sind, deren Prozessor die DFS3-Technologie nicht unterstützt oder die nur auf dem 2,4 GHz-Band senden.

#### 2.23.20.8.3 5GHz-Modus

Wenn Sie gleichzeitig zwei benachbarte, freie Kanäle für die Funkübertragung nutzen, können Sie die Übertragungsgeschwindigkeit mit dem Turbo-Modus auf bis zu 108 MBit/s steigern.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Radio-Einstellungen

**Mögliche Werte:**

- Normal (54 Mbit/s-Modus)
- 108 Mbit/s (Turbo-Modus)

**Default:** Normal (802.11a) oder 802.11a/n gemischt (bei 11n-Geräten)

Diese Einstellung ist nur verfügbar für Geräte, die DFS2 bzw. DFS3 beherrschen.

#### 2.23.20.8.4 Maximalentfernung

Bei sehr großen Entfernungen zwischen Sender und Empfänger im Funknetz steigt die Laufzeit der Datenpakete. Ab einer bestimmten Grenze erreichen die Antworten auf die ausgesandten Pakete den Sender nicht mehr innerhalb der erlaubten Zeit. Mit der Angabe des maximalen Abstands kann die Wartezeit auf die Antworten erhöht werden. Diese Distanz wird umgerechnet in eine Laufzeit, die den Datenpakete bei der drahtlosen Kommunikation zugestanden werden soll.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Radio-Einstellungen

**Mögliche Werte:**

- 0 bis 65535 km

**Default:** 0

#### 2.23.20.8.5 Diversity

Die Diversity-Einstellungen legen fest, welche Antennen zum Senden bzw. zum Empfangen verwendet werden:

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Radio-Einstellungen

**Mögliche Werte:**

- nur-RX: In dieser Standardeinstellung wird über die am Main-Anschluss des Access Points angeschlossene Antenne gesendet. Zum Empfangen (RX) wird die Antennen ausgewählt, die den bestem Empfang hat (an Main oder AUX).

- TX/RX: Wird die Diversity-Funktion auch auf das Senden angewendet (TX), wird auch zum Senden die Antennen mit dem stärksten Signal ausgewählt.
- keine: Hierbei wird nur die Main-Antenne zum Senden verwendet, zum Empfangen bevorzugt die Antenne am AUX-Anschluss. Mit dieser Variante können Antennen mit sehr hohen Leistungen zum Empfangen eingesetzt werden, die aus rechtlichen Gründen nicht zum Senden verwendet werden dürfen.

**Default:** nur-RX

#### 2.23.20.8.6 Band

Mit der Auswahl des Frequenzbandes legen Sie fest, ob die WLAN-Karte im 2,4 GHz- oder im 5 GHz-Band arbeitet, und damit gleichzeitig die möglichen Funkkanäle.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Radio-Einstellungen

**Mögliche Werte:**

- 2,4 GHz
- 5 GHz

**Default:** 2.4 Ghz

#### 2.23.20.8.7 Unterbaender

Im 5 GHz-Band kann neben dem Frequenzband ein Unterband gewählt werden, an das wiederum bestimmte Funkkanäle und maximale Sendeleistungen geknüpft sind.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Radio-Einstellungen

**Mögliche Werte:**

- Je nach gewähltem Frequenzband

**Default:** Band-1

#### 2.23.20.8.8 Funk-Kanal

Mit dem Funkkanal wird ein Teil des theoretisch denkbaren Frequenzbandes für die Datenübertragung im Funknetz ausgewählt.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Radio-Einstellungen

**Mögliche Werte:**

- Je nach gewähltem Frequenzband und nach gewähltem Land.

**Default:** 11

Im 2,4 GHz-Band müssen zwei getrennte Funknetze mindestens drei Kanäle auseinander liegen, um Störungen zu vermeiden.

#### 2.23.20.8.9 2.4GHz-Modus

Im 2,4 GHz-Band gibt es zwei verschiedene Funk-Standards: den IEEE 802.11b-Standard mit einer Übertragungsgeschwindigkeit von bis zu 11 MBit/s und den IEEE 802.11g-Standard mit bis zu 54 MBit/s. Wenn als Frequenzband das 2,4 GHz-Band ausgewählt ist, kann zusätzlich die Übertagungsgeschwindigkeit eingestellt werden.

Um eine möglichst hohe Übertragungsgeschwindigkeit zu erreichen, gleichzeitig aber auch langsamere Clients nicht auszuschließen, bietet sich der 802.11g/b-Kompatibilitätsmodus an. In diesem Modus arbeitet die WLAN-Karte im Access Point grundsätzlich nach dem schnelleren Standard, fällt aber auf den langsameren Modus zurück, wenn sich entsprechende Clients im WLAN anmelden. Im '2-MBit-Kompatibilitätsmodus' unterstützt der Access Point auch die älteren 802.11b-Karten mit einer maximalen Übertragungsgeschwindigkeit von 2 MBit/s.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Radio-Einstellungen

**Mögliche Werte:**

- 802.11g/b gemischt
- 802.11g/b 2 Mbit-kompatibel
- 802.11b (11 Mbit)
- 802.11g (54 Mbit)
- 802.11g (108 Mbit)

**Default:** 802.11b/g gemischt oder 802.11b/g/n gemischt (bei 11n-Geräten)

Bitte beachten Sie, dass sich Clients, die nur einen langsameren Standard unterstützen, sich ggf. nicht mehr in Ihrem WLAN anmelden können, wenn Sie die Übertragungsgeschwindigkeit auf einen hohen Wert einstellen.

## 2.23.20.9 Leistung

Hier können Sie Parameter definieren, die Einfluss auf die Leistung ihrer WLAN-Schnittstelle haben.

**SNMP-ID:** 2.23.20.9

**Pfad Telnet:** /Setup/Schnittstellen/WLAN

### 2.23.20.9.1 Ifc

Öffnet die Einstellungen für die physikalische WLAN-Schnittstelle.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Leistung

**Mögliche Werte:**

- Auswahl aus den verfügbaren physikalischen WLAN-Schnittstellen.

### 2.23.20.9.2 Tx-Bursting

Erlaubt/Verbietet das Paket-Bursting, was den Durchsatz erhöht, jedoch die Fairness auf dem Medium verschlechtert.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Leistung

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

### 2.23.20.9.3 Kompression

Erlaubt oder verbietet eine Hardwarekompression von Paketen.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Leistung

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

### 2.23.20.9.5 QoS

Mit der Erweiterung der 802.11-Standards um 802.11e können auch für WLAN-Übertragungen definierte Dienst-güten angeboten werden (Quality of Service). 802.11e unterstützt u. a. eine Priorisierung von bestimmten Datenpaketen. Die Erweiterung stellt damit eine wichtige Basis für die Nutzung von Voice-Anwendungen im WLAN dar (Voiceoder WLAN – VoWLAN).Die Wi-Fi-Alliance zertifiziert Produkte, die Quality of Service nach 802.11e unterstützen, unter dem Namen WMM(Wi-Fi Multimedia, früher WME für Wireless Multimedia Extension). WMM definiert vier Kategorien (Sprache,

Video,Best Effort und Hintergrund) die in Form separater Warteschlangen zur Prioritätensteuerung genutzt werden. Der 802.11e-Standard nutzt Steuerung der Prioritäten die VLAN-Tags bzw. die DiffServ-Felder von IP-Paketen, wenn keine VLAN-Tags vorhanden sind. Die Verzögerungszeiten (Jitter) bleiben mit weniger als zwei Millisekunden in einem Bereich, der vom menschlichen Gehör nicht wahrgenommen wird. Zur Steuerung des Zugriffs auf das Übertragungsmedium nutzt der 802.11e-Standard die Enhanced Distributed Coordination Function (EDCF).

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Leistung

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

Die Steuerung der Prioritäten ist nur möglich, wenn sowohl der WLAN-Client als auch der Access Point den802.11e-Standard bzw. WMM unterstützen und die Anwendungen die Datenpakete mit den entsprechen-den Prioritäten kennzeichnen.

## 2.23.20.10 Beaconing

Die Beaconing-Einstellungen sind nur in der Basisstations-Betriebsart von Bedeutung. Die Wireless-LAN-Basisstation (WLAN-AP) sendet regelmäßig ein Funksignal (Beacon), damit die Clients ihn bzw. die durch ihn aufgespannten logischen WLAN-Netze (SSIDs) finden können.

**SNMP-ID:** 2.23.20.10

**Pfad Telnet:** /Setup/Schnittstellen/WLAN

### 2.23.20.10.1 Ifc

Öffnet die Experten-Einstellungen für die physikalische WLAN-Schnittstelle.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Beaconing

**Mögliche Werte:**

- Auswahl aus den verfügbaren physikalischen WLAN-Schnittstellen.

### 2.23.20.10.2 Beacon-Periode

Dieser Wert gibt den zeitlichen Abstand in Kµs an, in dem Beacons verschickt werden (1 Kµs entspricht 1024 Mikrosekunden und stellt eine Recheneinheit des 802.11-Standard dar – 1 Kµs wird auch als Timer Unit TU bezeichnet). Niedrigere Werte ergebenen kleinere Beacon-Timeout-Zeiten auf dem Client und erlauben damit ein schnelleres Roaming beim Access Point-Ausfall, erhöhen aber den Overhead auf dem WLAN.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Beaconing

**Mögliche Werte:**

- 20 bis 65535 TU

**Default:** 100

### 2.23.20.10.3 DTIM-Periode

Dieser Wert gibt an, nach welcher Anzahl von Beacons die gesammelten Multicasts ausgesendet werden. Höhere Werte erlauben längere Sleep-Intervalle der Clients, verschlechtern aber die Latenzzeiten.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Beaconing

**Mögliche Werte:**

- 1 bis 255

**Default:** 1

#### 2.23.20.10.4 Beacon-Abfolge

Die Beacon-Abfolge bezeichnet die Reihenfolge, in der die Beacon zu den verschiedenen WLAN-Netzen versendet werden. Wenn z. B. drei logische WLAN-Netze aktiv sind und die Beacon-Periode 100 Kµs beträgt, so werden alle 100 Kµs die Beacons für die drei WLANs verschickt. Je nach Beacon-Abfolge werden die Beacons zu folgenden Zeitpunkten versendet

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Beaconing

**Mögliche Werte:**

- Zyklisch: In diesem Modus beginnt der Access Point beim ersten Beacon-Versand (0 Kµs) mit WLAN-1, gefolgt von WLAN-2 und WLAN-3. Beim zweiten Beacon-Versand (100 Kµs) wird zuerst WLAN-2 versendet, das WLAN-3 und erst dann kommt wieder WLAN-1 an die Reihe. Beim dritten Beacon-Versand (200 Kµs) entsprechend WLAN-3, WLAN-1, WLAN-2 – dann beginnt die Reihe wieder von vorne.
- Gestaffelt: In diesem Modus werden die Beacons nicht gemeinsam zu einem Zeitpunkt verschickt, sondern auf die verfügbare Beacon-Periode aufgeteilt. Zum Start bei 0 Kµs wird nur WLAN-1 verschickt, nach 33,3 Kµs kommt WLAN-2, nach 66,6 Kµs WLAN-3 – mit Beginn einer neuen Beacon-Periode startet der Versand wieder mit WLAN-1.
- Einfach-Burst: In diesem Modus verschickt der Access Point die Beacons für die definierten WLAN-Netze immer in der gleichen Abfolge. Beim ersten Beacon-Versand (0 Kµs) mit WLAN-1, WLAN-2 und WLAN-3, beim zweiten Versand nach dem gleichen Muster und so weiter.

**Default:** zyklisch

Ältere WLAN-Clients sind manchmal nicht in der Lage, die schnell aufeinander folgenden Beacons richtig zu verarbeiten, wie sie bei einem einfachen Burst auftreten. In der Folge erkennen diese Clients oft nur die ersten Beacons und können sich daher auch nur bei diesem einem Netz einbuchen. Die gestaffelte Aussendung der Beacons führt zum besten Ergebnis, erhöht aber die Prozessorlast für den Access Point. Die zyklische Aussendung stellt sich als guter Kompromiss dar, weil hier jedes Netz einmal als erstes ausgesendet wird.

### 2.23.20.11 Roaming

Die Roaming-Einstellungen sind nur in der Client-Betriebsart von Bedeutung. Sie regeln ob und wann der Client seine Basis-Station wechselt, wenn er mehr als eine Basisstation erreichen kann.

**SNMP-ID:** 2.23.20.11

**Pfad Telnet:** /Setup/Schnittstellen/WLAN

#### 2.23.20.11.1 Ifc

Öffnet die Experten-Einstellungen für die physikalische WLAN-Schnittstelle.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Roaming

**Mögliche Werte:**

- Auswahl aus den verfügbaren physikalischen WLAN-Schnittstellen.

#### 2.23.20.11.10 Min.-Verbindung-Halten-Signalpegel

Analog zum Verbindung-Halten-Schwellwert, Angabe jedoch als absolute Signalstärke

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Roaming

**Mögliche Werte:**

- 0 bis -128 dBm

**Default:** 0

#### 2.23.20.11.11 Sperrzeit

In der Betriebsart als WLAN-Client und bei mehreren gleichen WLAN-Zugangspunkte (gleiche SSID auf mehreren Access Points) können Sie hier einen Zeitraum zu definieren, in dem sich der WLAN-Client nicht mehr mit einem Access Point verbindet, nachdem die Anmeldung an diesem Access Point abgelehnt wurde (Association-Reject).

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Roaming

**Mögliche Werte:**

- 0 bis 4294967295 in Sekunden
- maximal 10 Zeichen

**Default:**

- 0

#### 2.23.20.11.2 Beacon-Verlust-Schwellwert

Der Beacon-Verlust-Schwellwert gibt an, wie viele Beacons der Access Points empfangsgestört sein dürfen, bevor ein eingebuchter Client eine erneute Suche beginnt.

Je höher der eingestellte Wert ist, desto eher kann es unbemerkt zu einer Unterbrechung der Verbindung kommen, gefolgt von einem zeitverzögerten Wiederaufbau der Verbindung.

Je kleiner der eingestellte Wert ist, desto eher kann eine möglicherweise folgende Unterbrechung erkannt werden, der Client kann frühzeitig mit dem Suchen nach einem alternativen Access Point beginnen.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Roaming

**Mögliche Werte:**

- 0 bis 99%

**Default:** 4

Zu kleine Werte können dazu führen, dass der Client unnötig oft einen Verbindungsverlust erkennt.

#### 2.23.20.11.3 Roaming-Schwellwert

Dieser Schwellwert gibt an, um wieviel Prozent die Signalstärke eines anderen Access Points besser sein muss, damit der Client auf den anderen Access Point wechselt.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Roaming

**Mögliche Werte:**

- 0 bis 99%

**Default:** 15

In anderem Zusammenhang wird die Signalstärke teilweise in dB angegeben. In diesen Fällen gilt für die Umrechnung:

64dB - 100%

32dB - 50%

0dB - 0%

#### 2.23.20.11.4 Kein-Roaming-Schwellwert

Dieser Schwellwert gibt die Feldstärke in Prozent an, ab welcher der aktuelle Access Point als so gut betrachtet wird, dass auf keinen Fall auf einen anderen Access Point gewechselt wird.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Roaming

**Mögliche Werte:**

- 0 bis 99%

**Default:** 45

#### 2.23.20.11.5 Zwangs-Roaming-Schwellwert

Dieser Schwellwert gibt die Feldstärke in Prozent an, ab welcher der aktuelle Access Point als so schlecht betrachtet wird, dass auf jeden Fall auf einen anderen, besseren Access Point gewechselt wird.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Roaming

**Mögliche Werte:**

- 0 bis 99%

**Default:** 12

#### 2.23.20.11.6 Soft-Roaming

Diese Option ermöglicht dem Client, anhand verfügbarer Scan-Informationen ein Roaming zu einem stärkeren Access Point durchzuführen (Soft-Roaming). Roaming aufgrund eines Verbindungsverlustes (Hard-Roaming) bleibt davon natürlich unbeeinflusst. Die eingestellten Roaming-Schwellwerte haben nur eine Funktion, wenn Soft-Roaming aktiviert ist.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Roaming

**Mögliche Werte:**

- Ein
- Aus

**Default:** Ein

#### 2.23.20.11.7 Verbindungs-Schwellwert

Dieser Schwellwert gibt die Feldstärke in Prozent an, die ein Access Point mindestens aufweisen muss, damit ein Client einen Versuch zum Einbuchen bei diesem Access Point startet.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Roaming

**Mögliche Werte:**

- 0 bis 99%

**Default:** 0

#### 2.23.20.11.8 Verbindung-Halten-Schwellwert

Dieser Schwellwert gibt die Feldstärke in Prozent an, die der aktuelle Access Point mindestens aufweisen muss, damit die Verbindung nicht als abgerissen betrachtet wird.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Roaming

**Mögliche Werte:**

- 0 bis 99%

**Default:** 0

#### 2.23.20.11.9 Min.-Verbindungs-Signalpegel

Analog zum Verbindungs-Schwellwert, Angabe jedoch als absolute Signalstärke

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Roaming

**Mögliche Werte:**

- 0 bis -128 dBm

**Default:** 0

## 2.23.20.12 Interpoint-Gegenstellen

Tragen Sie hier die WLAN-Basisstation ein, die über Punkt-zu-Punkt-Verbindung vernetzt werden sollen.

**SNMP-ID:** 2.23.20.12

**Pfad Telnet:** /Setup/Schnittstellen/WLAN

### 2.23.20.12.1 Ifc

Öffnet die Einstellungen für die Punkt-zu-Punkt-Partner.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Interpoint-Einstellungen

**Mögliche Werte:**

- Auswahl aus den verfügbaren Punkt-zu-Punkt-Verbindungen.

### 2.23.20.12.2 Erkenne-An

Wählen Sie hier aus, anhand welchen Merkmals die P2P-Gegenstelle identifiziert werden soll.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Interpoint-Einstellungen

**Mögliche Werte:**

- MAC-Adresse: Wählen Sie diese Einstellung, wenn die Geräte den P2P-Partner anhand der MAC-Adresse erkennen können. Tragen Sie in diesem Fall als 'MAC-Adresse' die WLAN-MAC-Adresse der physikalischen WLAN-Schnittstelle des P2P-Partners ein.
- Stations-Name: Wählen Sie diese Einstellung, wenn die Geräte den P2P-Partner anhand des Stations-Namens erkennen können. Tragen Sie in diesem Fall als 'Gegenstellen-Name' den Geräte-Names des P2P-Partners ein oder alternativ den als 'Stations-Name' in den physikalischen Einstellungen definierten Namen.
- Serial-Autoconfig: Wählen Sie diese Einstellung, wenn die P2P-Partner beim Start der Geräte die MAC-Adresse über eine serielle Verbindung austauschen.

**Default:** MAC-Adresse

### 2.23.20.12.3 MAC-Adresse

MAC-Adresse der P2P-Gegenstelle

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Interpoint-Einstellungen

**Mögliche Werte:**

- Gültige MAC-Adresse

**Default:** Leer

Wenn Sie die Erkennung durch MAC-Addresse verwenden, dann tragen Sie hier die MAC-Addresse des WLAN-Adapters und nicht die des Gerätes selbst ein.

### 2.23.20.12.4 Gegenstellen-Name

Stations-Name der P2P-gegenstelle

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Interpoint-Einstellungen

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen

**Default:** Leer

#### 2.23.20.12.5 Aktiv

Aktiviert bzw. deaktiviert diesen Punkt-zu-Punkt-Kanal.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Interpoint-Einstellungen

**Mögliche Werte:**

- Ein
- Aus

**Default:** Aus

### 2.23.20.13 Netzwerk-Alarm-Grenzen

In dieser Tabelle finden Sie die Einstellungen der Netzwerk-Alarm-Grenzen für die logischen WLAN-Netzwerke des Gerätes (SSIDs).

**SNMP-ID:** 2.23.20.13

**Pfad Telnet:** /Setup/Schnittstellen/WLAN

#### 2.23.20.13.1 Ifc

Wählen Sie hier das logische WLAN_Netzwerk (SSID), für welches Sie die Netzwerk-Alarm-Grenzen bearbeiten möchten.

**SNMP-ID:** 2.23.20.13.1

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Netzwerk-Alarm-Grenzen

**Mögliche Werte:**

- Auswahl aus den im Gerät verfügbaren SSIDs, z. B. WLAN-1, WLAN-1-2 etc.

#### 2.23.20.13.2 Phy-Signal

Der negative Grenzwert für den Signalpegel der entsprechenden SSID. Wird dieser Grenzwert unterschritten, wird ein Alarm abgesetzt. Der Wert 0 entspricht einer Deaktivierung der Prüfung.

**SNMP-ID:** 2.23.20.13.2

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Netzwerk-Alarm-Grenzen

**Mögliche Werte:**

- 3 numerische Zeichen

**Default:** 0

#### 2.23.20.13.3 Total-Wiederholungen

Der Grenzwert für die Gesamtanzahl an Sendewiederholungen für die entsprechende SSID. Sobald der Wert erreicht ist, wird ein Alarm abgesetzt. Der Wert 0 entspricht einer Deaktivierung der Prüfung.

**SNMP-ID:** 2.23.20.13.3

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Netzwerk-Alarm-Grenzen

**Mögliche Werte:**

- 4 numerische Zeichen zur Angabe der Wiederholungen in Promille

**Default:** 0 Promille

#### 2.23.20.13.4 Tx-Fehler

Die Gesamtanzahl der verlorenen Pakete für die entsprechende SSID. Sobald der Wert erreicht ist, wird ein Alarm abgesetzt. Der Wert 0 entspricht einer Deaktivierung der Prüfung.

**SNMP-ID:** 2.23.20.13.4

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Netzwerk-Alarm-Grenzen

**Mögliche Werte:**

- 4 numerische Zeichen zur Angabe der Wiederholungen in Promille

**Default:** 0 Promille

### 2.23.20.14 Interpoint-Alarm-Grenzen

In dieser Tabelle finden Sie die Einstellungen der Interpoint-Alarm-Grenzen für P2P-Verbindungen des Gerätes (SSIDs).

**SNMP-ID:** 2.23.20.14

**Pfad Telnet:** /Setup/Schnittstellen/WLAN

#### 2.23.20.14.1 Ifc

Wählen Sie hier die P2P-Verbindung, für welche Sie die Interpoint-Alarm-Grenzen bearbeiten möchten.

**SNMP-ID:** 2.23.20.14.1

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Interpoint-Alarm-Grenzen

**Mögliche Werte:**

- Auswahl aus den im Gerät verfügbaren P2P-Verbindungen, z. B. P2P-1-1, P2P-1-2 etc.

#### 2.23.20.14.2 Phy-Signal

Der negative Grenzwert für den Signalpegel der entsprechenden P2P-Verbindung. Wird dieser Grenzwert unterschritten, wird ein Alarm abgesetzt. Der Wert 0 entspricht einer Deaktivierung der Prüfung.

**SNMP-ID:** 2.23.20.14.2

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Interpoint-Alarm-Grenzen

**Mögliche Werte:**

- 3 numerische Zeichen

**Default:** 0

#### 2.23.20.14.3 Total-Wiederholungen

Der Grenzwert für die Gesamtanzahl an Sendewiederholungen für die entsprechende P2P-Verbindung. Sobald der Wert erreicht ist, wird ein Alarm abgesetzt. Der Wert 0 entspricht einer Deaktivierung der Prüfung.

**SNMP-ID:** 2.23.20.14.3

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Interpoint-Alarm-Grenzen

**Mögliche Werte:**

- 4 numerische Zeichen zur Angabe der Wiederholungen in Promille

**Default:** 0 Promille

#### 2.23.20.14.4 Tx-Fehler

Die Gesamtanzahl der verlorenen Pakete für die entsprechende P2P-Verbindung. Sobald der Wert erreicht ist, wird ein Alarm abgesetzt. Der Wert 0 entspricht einer Deaktivierung der Prüfung.

**SNMP-ID:** 2.23.20.14.4

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Interpoint-Alarm-Grenzen

**Mögliche Werte:**

- 4 numerische Zeichen zur Angabe der Wiederholungen in Promille

**Default:** 0 Promille

## 2.23.21 LAN-Schnittstellen

Dieses Menü enthält die Einstellungen für die LAN-Schnittstellen.

**SNMP-ID:** 2.23.21

**Pfad Telnet:** /Setup/Schnittstellen/LAN-Schnittstellen

### 2.23.21.1 Ifc

Wählen Sie hier die LAN-Schnittstelle, für welche die folgenden Einstellungen gelten.

**SNMP-ID:** 2.23.21.1

**Pfad Telnet:** /Setup/Schnittstellen/LAN-Schnittstellen/Ifc

**Mögliche Werte:**

- Auswahl aus den verfügbaren LAN-Schnittstellen.

### 2.23.21.2 Anschluss

Wählen Sie hier aus, welchen Netzwerkanschluss Sie für die Verbindung zu Ihrem lokalen Netz verwenden. Wenn Sie die Einstellung **Auto** wählen, wird der benutzte Anschluss vom Gerät automatisch erkannt.

**SNMP-ID:** 2.23.21.2

**Pfad Telnet:** /Setup/Schnittstellen/LAN-Schnittstellen/Anschluss

**Mögliche Werte:**

- Auto
- Auto-10
- Auto-100
- 10B-T
- FD10B-TX
- 100B-TX
- FD100B-TX
- FD1000B-TX
- Power-Down

**Default:** Auto

Die LAN-Schnittstellen des Geräts sind je nach Modell mit unterschiedlicher Hardware ausgestattet. Die erste LAN-Schnittstelle unterstützt bis zu 1000 MBit im Full-Duplex-Modus. Die zweite LAN-Schnittstelle unterstützt maximal 100 MBit im Full-Duplex-Modus.

### 2.23.21.3 MDI-Modus

Dieser Schalter aktiviert oder deaktiviert das automatische Kreuzen der Sende- und Empfangsleitungspaare (Auto-MIDIX), was den Einsatz von Node/Hub-Schaltern bzw. Crossover-Kabeln überflüssig macht. In Einzelfällen (z. B. bestimmte Glasfaser- Medienkonverter) kann es erforderlich sein, diese Automatik auszuschalten und die Leitungen fix zu kreuzen (MDIX) oder nicht zu kreuzen (MDI).

**SNMP-ID:** 2.23.21.3

**Pfad Telnet:** /Setup/Schnittstellen/LAN-Schnittstellen/MDI-Modus

**Mögliche Werte:**

- Auto
- MDI
- MDIX

**Default:** Auto

### 2.23.21.5 Takt-Rolle

Ein Ethernet-Port, der im 1000BASE-Tx-Modus arbeitet, erfordert einen kontinuierlichen Datenstrom zwischen beiden verbundenen Partnern, um synchronisiert zu bleiben. Naturgemäß brauchen beide Seiten eine synchronisierte Uhr (Takt), um Daten zu übertragen. IEEE 802.3 führte das Konzept eines Masters und eines Slaves für solche Verbindungen ein. Der Master gibt den Takt zur Datenübertragung in beide Richtungen vor, und der Slave synchronisiert sich auf diesen Takt. Die Rollen als Takt-Master und -Slave werden in der automatischen Aushandlungs-Phase der Verbindung verteilt. Normalerweise braucht diesem Detail keine Beachtung geschenkt zu werden, da die automatische Aushandlung durchaus gut funktioniert. In bestimmten Fällen kann es erforderlich werden, die Master-/Slave-Aushandlung zu beeinflussen. Hierzu dient die Einstellung des Takt-Gebers mit folgenden möglichen Werten:

**SNMP-ID:** 2.23.21.5

**Pfad Telnet:** /Setup/Schnittstellen/LAN-Schnittstellen/Takt-Rolle

**Mögliche Werte:**

- Bevorzugt Slave: Dies ist die empfohlene Standard-Einstellung für Geräte, die nicht als Switch eingesetzt werden. Während der Aushandlungs-Phase versucht der Port die Rolle des Slave auszuhandeln. Falls erforderlich, akzeptiert er auch die Rolle des Masters.
- Bevorzugt Master: Während der Aushandlungs-Phase versucht der Port die Rolle des Masters auszuhandeln. Falls erforderlich, akzeptiert er auch die Rolle des Slave.
- Slave: Der Port ist ausschließlich auf die Rolle des Slaves eingestellt. Eine Verbindung wird abgelehnt, wenn beide Verbindungs-Partner die Rolle des Slaves verwenden.
- Master: Der Port ist ausschließlich auf die Rolle des Masters eingestellt. Eine Verbindung wird abgelehnt , wenn beide Verbindungs-Partner die Rolle des Masters verwenden.

**Default:** Bevorzugt Slave

Die LAN-Schnittstellen des Geräts sind je nach Modell mit unterschiedlicher Hardware ausgestattet. Die Einstellung für den Takt-Geber hat für die zweite LAN-Schnittstelle keine Auswirkung.

### 2.23.21.7 Aktiv

Aktivieren oder deaktivieren Sie hier die ausgewählte LAN-Schnittstelle.

**SNMP-ID:** 2.23.21.7

**Pfad Telnet:** /Setup/Schnittstellen/LAN-Schnittstellen

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

### 2.23.21.8 Tx-Limit

Geben Sie hier das Bandbreitenlimit (kbit/s) in Senderichtung an. Der Wert 0 entspricht keinem Limit.

**SNMP-ID:** 2.23.21.8

**Pfad Telnet:** /Setup/Schnittstellen/LAN-Schnittstellen

**Mögliche Werte:**

- Maximal 10 numerische Zeichen

**Default:** 0

Diese Einstellung ist nur bei Geräten verfügbar, die über ein WLAN-Modul verfügen.

### 2.23.21.9 Rx-Limit

Geben Sie hier das Bandbreitenlimit (kbit/s) in Empfangsrichtung an. Der Wert 0 entspricht keinem Limit.

**SNMP-ID:** 2.23.21.9

**Pfad Telnet:** /Setup/Schnittstellen/LAN-Schnittstellen

**Mögliche Werte:**

- Maximal 10 numerische Zeichen

**Default:** 0

Diese Einstellung ist nur bei Geräten verfügbar, die über ein WLAN-Modul verfügen.

## 2.23.30 Ethernet-Ports

Die Ethernet-Schnittstellen von öffentlich zugänglichen LANCOM-Geräten können ggf. von unbefugten Anwendern genutzt werden, um physikalischen Zugang zu einem Netzwerk zu erhalten. Um diesen Versuch zu verhindern, können die Ethernet-Schnittstellen der Geräte ausgeschaltet werden.

**SNMP-ID:** 2.23.30

**Pfad Telnet:** /Setup/Schnittstellen

### 2.23.30.1 Port

Der Name des gewählten Ports.

**Pfad Telnet:** /Setup/Schnittstellen/Ethernet-Ports

### 2.23.30.2 Anschluss

Wählen Sie hier aus, welchen Netzwerkanschluss Sie für die Verbindung zu Ihrem lokalen Netz verwenden. Wenn Sie die Einstellung Auto wählen, wird der benutzte Anschluss vom Gerät automatisch erkannt.

**Pfad Telnet:** /Setup/Schnittstellen/Ethernet-Ports

**Mögliche Werte:**

- Auto
- 10B-T
- FD10B-TX
- 100B-TX
- FD100B-TX

**Default:** Auto

### 2.23.30.3 Privat-Modus

Wird der Privat-Modus aktiviert, kann dieser Switch-Port keine Daten unmittelbar mit den anderen Switch- Ports austauschen.

**Pfad Telnet:** /Setup/Schnittstellen/Ethernet-Ports

**Mögliche Werte:**

- ja
- nein

**Default:** nein

### 2.23.30.4 Zuordnung

Wählen Sie hier aus, wie diese Schnittstelle verwendet werden soll.

**Pfad Telnet:** /Setup/Schnittstellen/Ethernet-Ports

**Mögliche Werte:**

- LAN-1 bis LAN-n: Die Schnittstelle ist einem logischen LAN zugeordnet.
- DSL-1 bis DSL-n: Die Schnittstelle ist einem DSL-Interface zugeordnet.
- Idle: Die Schnittstelle ist keiner Verwendung zugeordnet, sie ist allerdings physikalisch aktiv.
- Monitor: Der Port ist ein Monitor-Port, d.h. es wird alles, was auf den anderen Ports empfangen wird, auf diesem Port wieder ausgegeben. Damit kann an diesem Port z. B. ein Paket-Sniffer (wie Ethereal) angeschlossen werden.
- Power down: Die Schnittstelle ist deaktiviert.

**Default:** Abhängig von der jeweiligen Schnittstelle bzw. dem spezifischen Hardware-Modell.

### 2.23.30.5 MDI-Modus

Hier kann die Verbindungsart des Switch-Ports eingestellt werden. Die Verbindungsart wird entweder automatisch gewählt oder sie kann fest eingestellt werden, auf gekreuzte (MDIX) oder nicht gekreuzte (MDI) Verbindung.

**Pfad Telnet:** /Setup/Schnittstellen/Ethernet-Ports

**Mögliche Werte:** Auto, MDI, MDIX

**Default:** Auto

### 2.23.30.6 Takt-Rolle

Ein Ethernet-Port, der im 1000BASE-Tx-Modus arbeitet, erfordert einen kontinuierlichen Datenstrom zwischen beiden verbundenen Partnern, um synchronisiert zu bleiben. Naturgemäß brauchen beide Seiten eine synchronisierte Uhr (Takt), um Daten zu übertragen. IEEE 802.3 führte das Konzept eines Masters und eines Slaves für solche Verbindungen ein. Der Master gibt den Takt zur Datenübertragung in beide Richtungen vor, und der Slave synchronisiert sich auf diesen Takt. Die Rollen als Takt-Master und -Slave werden in der automatischen Aushandlungsphase der Verbindung verteilt. Normalerweise braucht diesem Detail keine Beachtung geschenkt zu werden, da die automatische Aushandlung durchaus gut funktioniert. In bestimmten Fällen kann es erforderlich werden, die Master-/Slave-Aushandlung zu beeinflussen.

**Pfad Telnet:** /Setup/Schnittstellen/WLAN/Ethernet-Ports/Takt-Rolle

**Mögliche Werte:**

- Bevorzugt Slave: Dies ist die empfohlene Standard-Einstellung für Nicht-Switch-Geräte. Während der Aushandlungphase versucht der Port die Rolle des Slave auszuhandeln. Falls erforderlich, akzeptiert er allerdings auch die Rolle des Masters.
- Bevorzugt Master: Während der Aushandlungsphase versucht der Port die Rolle des Masters auszuhandeln. Falls erforderlich, akzeptiert er allerdings auch die Rolle des Slave.
- Slave: Der Port wird gezwungen, die Rolle des Slave auszuhandeln. Eine Verbindung wird **nicht** zustande kommen, wenn beide Verbindungs-Partner dazu gezwungen werden, die Rolle des Slave auszuhandeln.
- Master: Der Port wird gezwungen, die Rolle des Masters auszuhandeln. Eine Verbindung wird **nicht** zustande kommen, wenn beide Verbindungs-Partner dazu gezwungen werden, die Rolle des Masters auszuhandeln.

**Default:** Bevorzugt Slave

## 2.23.40 Modem

Fortsetzung der Befehle und Optionen für ein optional am seriellen Interface angeschlossenes externes Modem.

**SNMP-ID:** 2.23.40

**Pfad Telnet:** /Setup/Schnittstellen

### 2.23.40.5 Anwahl

Das Gerät verwendet diesen Befehl zum Wählen über das extern angeschlossene Modem. Dabei hängt das Gerät die Rufnummer aus der Gegenstellentabelle an die hier eingetragene Zeichenkette an.

**Pfad Telnet:** /Setup/Schnittstellen/Modem/Anwahl

**Mögliche Werte:**

- maximal 31 alphanumerische Zeichen

**Default:** DT

### 2.23.40.14 AT-Poll_Anzahl

Wenn das extern angeschlossene Modem auf die AT-Polls des Gerätes für die hier eingestellte Anzahl nacheinander nicht antwortet, führt das Gerät einen Hardware-Reset für das extern angeschlossene Modem aus.

**Pfad Telnet:** /Setup/Schnittstellen/Modem/AT-Poll_Anzahl

**Mögliche Werte**

- Numerische Zeichen von 0 bis 9

**Default:** 5

### 2.23.40.2 Echo-Deaktivieren

Wenn das Modem-Echo aktiviert ist, sendet das extern angeschlossene Modem jedes empfangene Zeichen zurück. Für die korrekte Funktion des externen Modems am hier beschriebenden Gerät ist es erforderlich, das Modem-Echo zu deaktivieren. Das Gerät verwendet diesen Befehl zum Deaktivieren des "Modem-Echo".

**Pfad Telnet:** /Setup/Schnittstellen/Modem/Echo-Deaktivieren

**Mögliche Werte:**

- maximal 9 alphanumerische Zeichen

**Default:** E0

### 2.23.40.9 Escapsesquenz-(Data-CMD)

Das Gerät verwendet diese Befehlssequenz, um in der Datenphase einzelne Kommandos an das Modem zu übertragen.

**Pfad Telnet:** /Setup/Schnittstellen/Modem/Escapsesquenz-(Data-CMD)

**Mögliche Werte**:

- Max. 9 Alphanumerische Zeichen

**Default**: +++

### 2.23.40.11 Init.-Anwahl

Das Gerät sendet die Initialisierungssequenz zur Anwahl vor der Ausgabe des Wählbefehls an das extern angeschlossene Modem.

**Pfad Telnet:** /Setup/Schnittstellen/Modem/Init.-Anwahl

**Mögliche Werte:**

- maximal 63 alphanumerische Zeichen

**Default:** leer

### 2.23.40.12 Init.-Rufannahme

Das Gerät sendet die Initialisierungssequenz zur Rufannahme vor der Ausgabe des Rufannahmebefehls an das extern angeschlossene Modem.

**Pfad Telnet:** /Setup/Schnittstellen/Modem/Init.-Rufannahme

**Mögliche Werte:**

- maximal 63 alphanumerische Zeichen

**Default:** leer

### 2.23.40.4 Initialisierung

Das Gerät verwendet diesen Befehl zur Initialisierung des extern angeschlossenen Modems.

Das Gerät sendet diese Sequenz nach einem Hardware-Reset des extern angeschlossenen Modems an eben dieses extern angeschlossene Modem.

**Pfad Telnet:** /Setup/Schnittstellen/Modem/Initialisierung

**Mögliche Werte:**

- maximal 63 alphanumerische Zeichen

**Default:** L0X1M1S0=0

### 2.23.40.6 Modemkennung_abfragen

Das Gerät verwendet diesen Befehl zur Abfrage der Modemkennung. Das Ergebnis wird im Modem-Status ausgegeben.

**Pfad Telnet:** /Setup/Schnittstellen/Modem/Modemkennung_abfragen

**Mögliche Werte:**

- maximal 9 alphanumerische Werte

**Default:** I6

### 2.23.40.3 Reset

Das Gerät verwendet diesen Befehl, um einen Hardware-Reset auf dem extern angeschlossenen Modem auszuführen.

**SNMP-ID:** 2.23.40.3

**Pfad Telnet:** /Setup/Schnittstellen/Modem/Reset

**Mögliche Werte:**

- maximal 9 alphanumerische Zeichen

**Default:** &F

### 2.23.40.1 Ring-Count

Anzahl Klingeltöne bis zur Rufannahme.

**Pfad Telnet:** /Setup/Schnittstellen/Modem/Ring-Count

**Mögliche Werte:**

- Numerische Zeichen von 0 bis 99

**Default:** 1

### 2.23.40.7 Rufannahme

Das Gerät verwendet diesen Befehl zur Annahme eines Rufes am extern angeschlossenen Modem.

**Pfad Telnet:** /Setup/Schnittstellen/Modem/Rufannahme

**Mögliche Werte**:

- Max. 9 Alphanumerische Zeichen

**Default**: A

### 2.23.40.8 Verbindung_trennen

Das Gerät verwendet diesen Befehl zum Trennen eines Rufes am extern angeschlossenen Modem (Auflegen).

**Pfad Telnet:** /Setup/Schnittstellen/Modem/Verbindung_trennen

**Mögliche Werte**:

- Max. 9 Alphanumerische Zeichen

**Default**: H

### 2.23.40.10 Wartezeit-nach-Escapesequenz-(ms)

Nach der Escapesequenz wartet das Gerät für die hier eingestellte Zeit, bevor das Kommando zum Auflegen ausgegeben wird.

**Pfad Telnet:** /Setup/Schnittstellen/Modem/Wartezeit-nach-Escapesequenz-(ms)

**Mögliche Werte:**

- Numerische Werte von 0 bis 9999 Millisekunden

**Default:** 1000

### 2.23.40.13 Zykluszeit-AT-Poll-(s)

Wenn keine Verbindung besteht, prüft das Gerät die Existenz und korrekte Funktion des extern angeschlossenen Modems durch Ausgabe der Zeichenfolge "AT" an das Modem. Wenn das Modem korrekt angeschlossen ist und funktioniert, antwortet es mit "OK". Die Zykluszeit für den "AT-Poll" definiert den Abstand zwischen zwei Prüfungen.

**Pfad Telnet:** /Setup/Schnittstellen/Modem/Zykluszeit-AT-Poll-(s)

**Mögliche Werte:**

- Numerische Zeichen von 0 bis 9 Sekunden

**Default:** 1 Sekunde

## 2.23.41 Mobilfunk

Hier finden Sie die Einstellungen für den Mobilfunk.

**SNMP-ID:** 2.23.41

**Pfad Telnet:** /Setup/Schnittstellen/Mobilfunk

### SNMPID.2.23.41.4 Aufbau-Ueberwachung

Kontrolliert den Aufbau der WAN-Verbindung. War dieser für die unter "2.23.41.5. Versuche" eingestellte Anzahl der Aufbauversuche nacheinander nicht erfolgreich, führt das Gerät einen Hardware-Reset des Mobilfunk-Moduls aus.

**Pfad Telnet:** /Setup/Schnittstellen/Mobilfunk/Aufbau-Ueberwachung

**Mögliche Werte:**

- keine: Das Gerät führt keine Aufbauüberwachung durch.
- PPP: Das Gerät führt eine Aufbauüberwachung für PPP-Verbindungen durch.
- PPP+IP: Das Gerät führt eine Aufbauüberwachung für PPP- und IP-Verbindungen durch.

**Default:** keine

Geräte mit einer Firmware-Version 8.00 oder höher ignorieren die unter "2.23.41.5. Versuche" eingestellte Anzahl der Aufbauversuche und verwenden fest den Wert "10". Dieser Parameter entfällt für Firmware-Versionen 8.20 oder höher, das Gerät führt die Aufbauüberwachung dann immer durch.

### 2.23.41.8 HSUPA-erlauben

Aktivieren oder deaktivieren Sie hier die Nutzung von HSUPA.

**Pfad Telnet:** /Setup/Schnittstellen/Mobilfunk/HSUPA-erlauben

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

### 2.23.41.2 Netzsuche

Dieser Befehl startet eine Suche nach den verfügbaren Netzen. Die Liste der gefundenen Netze finden Sie im Modem-Status als Netzwerkliste.

**Pfad Telnet:** /Setup/Schnittstellen/Mobilfunk/Netzsuche

### 2.23.41.6 Protokollierungsintervall(Sec)

Protokollierungsintervall in Sekunden für die Werte, die der Modem-Status unter History anzeigt.

**PfadTelnet:** /Setup/Schnittstellen/Mobilfunk/Protokollierungsintervall(Sec)

**Mögliche Werte:**

- 0 bis 999999 Sekunden

**Default:** 0

**Besondere Werte:** '0' deaktivierte die Protokollierung der History-Werte.

### 2.23.41.3 PUK-Eingeben

Wenn die PIN der im Gerät verwendeten SIM-Karte nach mehrfacher Fehleingabe gesperrt ist (z. B. aufgrund fehlerhafter Profile), ist die Freischaltung der SIM-Karte durch die Eingabe der PUK erforderlich. Dieser Befehl startet die Abfrage der PUK.

**Pfad Telnet:** /Setup/Schnittstellen/Mobilfunk/PUK-Eingeben

### 2.23.41.11 Rueckfallpruefung-wenn-verbunden

Aktivieren Sie diese Option, wenn das Gerät auch bei bestehenden WAN-Verbindungen auf 2G-Verbindungen zurückfallen darf.

**Pfad Telnet:** /Setup/Schnittstellen/Mobilfunk/Rueckfallpruefung-wenn-verbunden

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

Diese Einstellung wirkt sich nur aus, wenn der Rückfall von 3G- auf 2G-Verbindungen generell konfiguriert ist.

### 2.23.41.10 Schwellwert-3G-nach-2G(dB)

Dieser Wert gibt den Schwellwert für den Rückfall von 3G- nach 2G-Verbindungen an. Wird im 3G-Betrieb dieser Schwellwert unterschritten, wechselt das Gerät auf eine 2G-Verbindung (sofern verfügbar). Positive Werte werden automatisch in negative Werte umgewandelt.

**Pfad Telnet:** /Setup/Schnittstellen/Mobilfunk/Schwellwert-3G-nach-2G(dB)

**Mögliche Werte:**

- -51 bis -111 bzw. von 51 bis 111 dB

**Default:** -89 dB

**Besondere Werte:** '0' deaktiviert den Rückfall von 3G- auf 2G-Verbindungen.

### 2.23.41.9 Signal-Pruefintervall(Min)

Dieser Wert gibt die Zeit in Minuten an, nach der das Gerät wieder eine 3G-Verbindung (sofern verfügbar) wechseln darf.

**Pfad Telnet:** /Setup/Schnittstellen/Mobilfunk/Signal-Pruefintervall(Min)

**Mögliche Werte:**

- 0 bis 9999 Minuten

**Default:** 0 Minuten

**Besondere Werte:** '0' deaktiviert den Rückfall von 3G- auf 2G-Verbindungen.

## 2.23.41.7 Syslog-senden

Aktivieren Sie diese Option, damit das Gerät die Werte aus der History im Modem-Status (siehe auch '2.23.41.6 Protokollierungsintervall(Sec)') auch per SYSLOG protokolliert.

**Pfad Telnet:** /Setup/Schnittstellen/Mobilfunk/Syslog-senden

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

## 2.23.41.5 Versuche

Anzahl der Aufbauversuche, nach denen das Gerät einen Hardware-Reset für das Mobilfunk-Modul durchführt.

**Pfad Telnet:** /Setup/Schnittstellen/Mobilfunk/Versuche

**Mögliche Werte:**

- 3 numerische Zeichen

**Default:** leer

Das Gerät verwendet die Anzahl der Aufbauversuche nur dann, wenn die Option "2.23.41.4 Aufbau-Ueberwachung" eingeschaltet ist. Geräte mit einer Firmware-Version 8.00 oder höher ignorieren diesen Wert und verwenden als Anzahl der Aufbauversuche fest den Wert "10". Dieser Parameter entfällt für Firmware-Versionen 8.20 oder höher, das Gerät führt die Aufbauüberwachung dann immer durch.

## 2.23.41.1 Profile

In dieser Tabelle finden Sie die Einstellungen für die GPRS/UMTS-Profile.

**Pfad Telnet:** /Setup/Schnittstellen/Mobilfunk/Profile

### 2.23.41.1.1 Profil

Geben Sie hier einen eindeutigen Namen für dieses UMTS/GPRS-Profil ein. Dieses Profil kann dann in den UMTS/GPRS-WAN-Einstellungen ausgewählt werden.

**Pfad Telnet:** /Setup/Schnittstellen/Mobilfunk/Profile/Profil

**Mögliche Werte:**

- maximal 16 alphanumerische Zeichen

**Default:** leer

### 2.23.41.1.2 PIN

Geben Sie hier die 4-stellige PIN der im UMTS/GPRS-Interface verwendeten Mobilfunk-SIM-Karte ein. Der Router benötigt diese Information, um das UMTS/GPRS-Interface in Betrieb zu nehmen.

**Pfad Telnet:** /Setup/Schnittstellen/Mobilfunk/Profile/PIN

**Mögliche Werte:**

- maximal 6 numerische Zeichen

**Default:** leer

Die SIM-Karte protokolliert jeden Fehlversuch mit einer ungeeigneten PIN. Die Anzahl dieser Fehlversuche bleibt auch dann erhalten, wenn das Gerät zwischenzeitlich vom Stromnetz getrennt ist. Nach 3 Fehlversuchen sperrt sich die SIM-Karte gegen weitere Zugangsversuche. In diesem Zustand benötigen Sie die in der Regel 8-stelligen PUK oder SuperPIN, um die Sperre aufzuheben.

#### 2.23.41.1.3 APN

Geben Sie hier den Namen des Zugangs-Servers für Mobilfunk-Datendienste ein, kurz APN (Access Point Name). Er ist spezifisch für Ihren Mobilfunk-Dienstanbieter und Sie finden diese Information in den Unterlagen Ihres Mobilfunk-Vertrages.

**Pfad Telnet:** /Setup/Schnittstellen/Mobilfunk/Profile/APN

**Mögliche Werte:**

- maximal 48 alphanumerische Zeichen

**Default:** leer

#### 2.23.41.1.4 Netz

Wenn Sie die manuelle Mobilfunk-Netzwahl selektiert haben, dann bucht sich das UMTS/GPRS-Interface ausschließlich in dem hier unter seinem vollen Namen angegebenen Mobilfunk-Netz ein.

**Pfad Telnet:** /Setup/Schnittstellen/Mobilfunk/Profile/Netz

**Mögliche Werte:**

- maximal 16 alphanumerische Zeichen

**Default:** leer

#### 2.23.41.1.5 Auswahl

Wenn Sie die automatische Mobilfunk-Netzwahl selektieren, dann bucht sich das UMTS/GPRS-Interface selbstständig in einem der verfügbaren und erlaubten Mobilfunk-Netze ein. Selektieren Sie hingegen die manuelle Mobilfunk- Netzwahl, dann bucht sich das UMTS/GPRS-Interface ausschließlich in dem darunter angegebenen Mobilfunk-Netz ein.

**Pfad Telnet:** /Setup/Schnittstellen/Mobilfunk/Profile/Auswahl

**Mögliche Werte:**

- Auto.
- Manuell

**Default:** Auto.

Die manuelle Mobilfunk-Netzwahl eignet sich insbesondere dann, wenn der Router stationär betrieben wird und es häufiger vorkommen kann, dass sich das UMTS/GPRS-Interface in ein benachbartes oder funktechnisch starkeres, mitunter aber unerwünschtes oder teureres Mobilfunk-Netz einbucht.

#### 2.23.41.1.6 Modus

Wählen Sie hier den vom UMTS/GPRS-Interface bevorzugten Mobilfunk-Datenübertragungs-Standard.

**Pfad Telnet:** /Setup/Schnittstellen/Mobilfunk/Profile/Modus

**Mögliche Werte:**

- Auto.
- GPRS
- UMTS

**Default:** Auto.

#### 2.23.41.1.7 QoS-Downstream-Datenrate

Damit die Quality-of-Service (QoS)-Funktionen der Firewall einwandfrei funktionieren, geben Sie hier die Übertragungsraten des verwendeten UMTS-Anschlusses an.

**Pfad Telnet:** /Setup/Schnittstellen/Mobilfunk/Profile/QoS-Downstream-Datenrate

**Mögliche Werte:**

- maximal 5 numerische Zeichen

**Default:** 0

**Besondere Werte:** 0: das Interface ist unbeschränkt und QoS-Mechanismen können nicht greifen.

#### 2.23.41.1.8 QoS-Upstream-Datenrate

Damit die Quality-of-Service (QoS)-Funktionen der Firewall einwandfrei funktionieren, geben Sie hier die Übertragungsraten des verwendeten UMTS-Anschlusses an.

**Pfad Telnet:** /Setup/Schnittstellen/Mobilfunk/Profile/QoS-Upstream-Datenrate

**Mögliche Werte:**

- maximal 5 numerische Zeichen

**Default:** 0

**Besondere Werte:** 0: das Interface ist unbeschränkt und QoS-Mechanismen können nicht greifen

## 2.23.50 Analog

Hier finden Sie die Einstellungen für die analoge Schnittstelle.

**SNMP-ID:** 2.23.50

**Pfad Telnet:** /Setup/Schnittstellen/Analog

### 2.23.50.8 Lifeline

Hier können Sie das inaktive Interface Analog-1 dauerhaft mit dem Leitungsinterface verbinden.

**Pfad Telnet:** /Setup/Schnittstellen/Analog/Lifeline

**Mögliche Werte:**

- nein
- ja

**Default:** nein

### 2.23.50.1 Operating

Aktivieren oder deaktivieren Sie hier die analogen Schnittstellen Ihres Gerätes.

**Pfad Telnet:** /Setup/Schnittstellen/Analog/Operating

#### 2.23.50.1.1 Ifc

Wählen Sie hier die analoge Schnittstelle, die Sie aktivieren oder deaktivieren wollen.

**Pfad Telnet:** /Setup/Schnittstellen/Analog/Operating/Ifc

**Mögliche Werte:**

- Line-1
- Analog-1
- Analog-2

**Default:** Line-1

#### 2.23.50.1.2 Active

Aktivieren oder deaktivieren Sie hier die entsprechende Schnittstelle.

**Pfad Telnet:** /Setup/Schnittstellen/Analog/Operating/Active

**Mögliche Werte:**

- ja
- nein

**Default:** ja

# 2.24 Public-Spot-Modul

In diesem Menü finden sie die Einstellungen für den Public-Spot.

**SNMP-ID:** 2.24

**Pfad Telnet:** /Setup

## 2.24.19 Neuer-Benutzer-Assistent

Mit Hilfe des Assistenten in WEBconfig können Sie Public-Spot-Benutzerkonten auf einfache Weise angelegen. Der Assistent generiert automatisch Benutzername und Passwort und präsentiert eine Seite zum Ausdrucken aller notwendigen Zugangsdaten. In diesem Menü finden Sie die Einstellungen für diesen Assistenten.

**SNMP-ID:** 2.24.19

**Pfad Telnet:** /Setup/Public-Spot-Modul

### 2.24.19.5 Default-Laufzeit

In dieser Tabelle definieren Sie die möglichen Standard-Laufzeiten für den Public-Spot-Benutzer-Assistenten. Der Assistent bietet diese Laufzeiten beim Erstellen eines Benutzerkontos an.

**SNMP-ID:** 2.24.19.5

**Pfad Telnet:** /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent

#### 2.24.19.5.1 Laufzeit

Wählen Sie hier die Laufzeit eines Benutzerkontos für den Public Spot.

**SNMP-ID:** 2.24.19.5.1

**Pfad Telnet:** /Setup/Public-Spot-Modul/Default-Laufzeit

**Mögliche Werte:** max. 5 Zeichen

**Default:** leer

#### 2.24.19.5.2 Einheit

Wählen Sie hier die Einheit für die Laufzeit eines Benutzerkontos für den Public Spot.

**SNMP-ID:** 2.24.19.5.2

**Pfad Telnet:** /Setup/Public-Spot-Modul/Default-Laufzeit

**Mögliche Werte:**

- Minuten(n)
- Stunde(n)
- Tage(e)

**Default:** Stunden(n)

## 2.24.19.6 Kommentarfelder

In dieser Tabelle definieren Sie die Kommentarfelder für den Public-Spot-Benutzer-Assistenten.

**SNMP-ID:** 2.24.19.6

**Pfad Telnet:** /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent/Kommentarfelder

### 2.24.19.6.1 Feldname

Der Public-Spot-Benutzer-Assistent kann auf dem Ausdruck bis zu 5 Kommentare ausgeben. Wählen Sie hier die Namen dieser Kommentarfelder, die der Assistent im Formular beim Erstellen der Benutzerkonten anzeigt.

**Pfad Telnet:** /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent/Kommentarfelder/Feldname

**Mögliche Werte:**

- max. 31 Zeichen

**Default:** leer

Aktivieren Sie den Ausdruck der Kommentare mit der Option *2.24.19.8 Drucke-Kommentare-auf-Voucher*.

## 2.24.19.11 SSID-Tabelle

Diese Tabelle enthält die Liste der für Public-Spot-Benutzer freigegebene Netzwerknamen.

**SNMP-ID:**

2.24.19.11

**Pfad Telnet:**

**Setup** > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **SSID-Tabelle**

### 2.24.19.11.1 Netzwerkname

Geben Sie hier den Namen eines im Gerät gespeicherten logischen WLAN-Netzes an, wenn Sie für dessen Zugang Public-Spot-Benutzern abrechenbare Vouchers erstellen.

**SNMP-ID:**

2.24.19.11.1

**Pfad Telnet:**

**Setup** > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **SSID-Tabelle**

**Mögliche Werte:**

maximal 32 alphanumerische Zeichen

aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

**Default**

leer

#### 2.24.19.11.2 Default

Bestimmen Sie den Namen des WLAN-Netzes als Standardwert. Der Assistent zum Anlegen neuer Public-Spot-Benutzer schlägt in der Liste verfügbarer WLAN-Netze diesen Wert automatisch vor. Diesen Vorschlag ändern Sie bei Bedarf noch in der Eingabemaske des Assistenten.

**SNMP-ID:**

2.24.19.11.2

**Pfad Telnet:**

**Setup** > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **SSID-Tabelle**

**Mögliche Werte:**

nein

ja

**Default**

nein

### 2.24.19.2 Benutzer-Name-Muster

Geben Sie hier das Format für den Namen des neuen Benutzerkontos an.

**SNMP-ID:** 2.24.19.2

**Pfad Telnet:** /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent

**Mögliche Werte:**

- max. 19 Zeichen. Für die Zeichenfolge '%n' setzt der Public Spot eine automatisch generierte, eindeutige Nummer für das Konto ein.

**Default:** user%n

### 2.24.19.8 Drucke-Kommentare-auf-Voucher

Aktivieren oder deaktivieren Sie hier den Ausdruck der Kommentarfelder auf dem Voucher für den Public-Spot-Benutzer.

**SNMP-ID:** 2.24.19.8

**Pfad Telnet:** /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent/Drucke-Kommentare-auf-Voucher

**Mögliche Werte:**

- ja
- nein

**Default:** nein

### 2.24.19.9 Maximale-Voucher-Gueltigkeitsdauer

Mit diesem Wert definieren Sie die maximale Gültigkeitsdauer des Vouchers in Tagen.

**SNMP-ID:** 2.24.19.9

**Pfad Telnet:** /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent/Maximale-Voucher-Gueltigkeitsdauer

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 365 Tage

Wenn Sie den Startzeitpunkt für die Laufzeit eines Vouchers auf 'erster-Login' einstellen (*2.24.19.7 Standard-Startzeitpunkt*), beginnt die Laufzeit des Vouchers erst zu einem Zeitpunkt in der Zukunft. Die maximale Gültigkeit hat Vorrang vor der Laufzeit des einzelnen Vouchers. Wenn der Benutzer das Voucher aktiviert, kann die Laufzeit ggf. schon abgelaufen sein oder noch während der eigentlich vorgesehenen Laufzeit ablaufen.

### 2.24.19.3 Passwort-Länge

Definieren Sie hier die Länge des Passworts, welches der Public-Spot-Benutzer-Assistent für ein neues Konto generiert.

**SNMP-ID:** 2.24.19.3

**Pfad Telnet:** /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent

**Mögliche Werte:**

- 0 bis 255

**Default:** 6

### 2.24.19.4 SSID

Geben Sie hier die SSID an, die der Public-Spot-Benutzer-Assistent auf dem Formular für den Benutzer ausgibt.

**SNMP-ID:** 2.24.19.4

**Pfad Telnet:** /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent

**Englische Bezeichnung**: SSID

**Mögliche Werte:**

- max. 32 alphanumerische Zeichen

**Default:** leer

Wenn Sie dieses Feld frei lassen, gibt der Public-Spot-Benutzer-Assistent auf dem Formular die SSID des ersten logischen WLAN mit aktivem Public-Spot aus.

### 2.24.19.7 Standard-Startzeitpunkt

Wählen Sie hier aus, zu welchem Zeitpunkt die Laufzeit des Vouchers startet. Mit der Option, die Laufzeit erst ab dem ersten Login beginnen zu lassen, können Sie mehrere Voucher auf Vorrat drucken. Der Benutzer kann dennoch die komplette Laufzeit nutzen.

**SNMP-ID:** 2.24.19.7

**Pfad Telnet:** /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent/Standard-Startzeitpunkt

Wählen Sie den Standard-Startzeitpunkt.

**Mögliche Werte:**

- sofort
- erster-Login

**Default:** erster-Login

### 2.24.19.10 Verfuegbare-Ablauf-Methoden

Mit dieser Einstellung legen Sie fest, welche Ablauf-Methoden der Public-Spot-Benutzer-Assistent bei der Erstellung von neuen Benutzerkonten anbietet.

**SNMP-ID:** 2.24.19.10

**Pfad Telnet:** /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent/Verfuegbare-Ablauf-Methoden

**Mögliche Werte:**

- Alle-Methoden: Der Assistent bietet alle verfügbaren Ablauf-Methoden an.
- Aktuelle-Zeit-Methode: Der Assistent bietet nur die Ablauf-Methode der aktuellen Zeit an. Die Laufzeit der so erstellen Benutzerkonten beginnt sofort zu dem Zeitpunkt, an dem das Benutzerkonto erstellt wird.
- Login-Zeit-Methode: Der Assistent bietet nur die Ablauf-Methode der Login-Zeit an. Die Laufzeit der so erstellen Benutzerkonten beginnt erst zu dem Zeitpunkt, zu dem sich der Benutzer zum ersten Mal am Public Spot anmeldet.

**Default:** Alle-Methoden

Wenn Sie die Login-Zeit-Methode auswählen, kann die Laufzeit eines Benutzerkontos je nach Einstellung der maximalen Voucher-Gültigkeitsdauer (*2.24.19.9 Maximale-Voucher-Gueltigkeitsdauer*) schon vor dem ersten Login überschritten werden.

## 2.24.3 Anbieter-Tabelle

Bei der Konfiguration eines Public-Spot können die Benutzer-Anmeldedaten zur Authentifizierung und für das Accounting an einen oder mehrere RADIUS-Server weitergeleitet werden. Diese werden in der Anbieter-Liste konfiguriert.

**SNMP-ID:** 2.24.3

**Pfad Telnet:** /Setup/Public-Spot-Modul

Konfigurieren Sie neben den dedizierten Parametern für die RADIUS-Anbieter auch die allgemeinen RADIUS-Werte wie Wiederholung und Timeout in den entsprechenden Konfigurationsbereichen.

### 2.24.3.1 Name

Name des Anbieters, der den RADIUS-Server für die Authentifizierung und/oder das Accounting bereitstellt.

**Pfad Telnet:** /Setup/Public-Spot-Modul/Anbieter-Tabelle/Name

**Mögliche Werte:**

- max. 16 alphanumerische Zeichen

**Default:** leer

### 2.24.3.2 Auth.-Server-Adresse

Geben Sie hier die IP-Adresse des Servers an, den der Public-Spot für die Authentifizierung der Zugänge bei diesem Anbieter kontaktiert.

**Pfad Telnet:** /Setup/Public-Spot-Modul/Anbieter-Tabelle/Auth.-Server-Adresse

**Mögliche Werte:**

- gültige IP-Adresse

**Default:** 0.0.0.0

### 2.24.3.3 Auth.-Server-Port

Geben Sie hier den Port des Servers an, über den der Public-Spot die Authentifizierung der Zugänge bei diesem Anbieter anfragt.

**Pfad Telnet:** /Setup/Public-Spot-Modul/Anbieter-Tabelle/Auth.-Server-Port

**Mögliche Werte:**

- gültige Port-Bezeichnung

**Default:** l0

### 2.24.3.4 Auth.-Server-Schluessel

Geben Sie hier den Schlüssel (Shared Secret) für den Zugang zum RADIUS-Server des Anbieters an. Stellen Sie sicher, dass dieser Schlüssel im entsprechenden RADIUS-Server übereinstimmend konfiguriert ist.

**SNMP-ID:** 2.24.3.4

**Pfad Telnet:** /Setup/Public-Spot-Modul/Anbieter-Tabelle/Auth.-Server-Schluessel

**Mögliche Werte:**

- max. 32 alphanumerische Zeichen

**Default:** leer

### 2.24.3.9 Auth.-Server-Loopback-Adr.

Geben Sie hier die Loopback-Adresse des Servers an, den der Public-Spot für die Authentifizierung der Zugänge bei diesem Anbieter kontaktiert.

**Pfad Telnet:** /Setup/Public-Spot-Modul/Anbieter-Tabelle/Auth.-Server-Loopback-Adr.

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LBO ... LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

**Default:** leer

### 2.24.3.11 Auth.-Server-Protokoll

Wählen Sie hier das Protokoll, das der Public-Spot für die Authentifizierung der Zugänge bei diesem Anbieter verwendet.

**Pfad Telnet:** /Setup/Public-Spot-Modul/Anbieter-Tabelle/Auth.-Server-Protokoll

**Mögliche Werte:**

- RADIUS
- RADSEC

**Default:** RADIUS

### 2.24.3.5 Acc.-Server-Adresse

Geben Sie hier die IP-Adresse des Servers an, den der Public-Spot für das Accounting der Zugänge bei diesem Anbieter kontaktiert.

**Pfad Telnet:** /Setup/Public-Spot-Modul/Anbieter-Tabelle/Auth.-Server-Adresse

**Mögliche Werte:**

- gültige IP-Adresse

**Default:** 0.0.0.0

### 2.24.3.6 Acc.-Server-Port

Geben Sie hier den Port des Servers an, über den der Public-Spot das Accounting der Zugänge bei diesem Anbieter durchführt.

**SNMP-ID:** 2.24.3.6

**Pfad Telnet:** /Setup/Public-Spot-Modul/Anbieter-Tabelle/Acc.-Server-Port

**Mögliche Werte:**

- gültige Port-Bezeichnung

**Default:** l0

### 2.24.3.7 Acc.-Server-Schluessel

Geben Sie hier den Schlüssel (Shared Secret) für den Zugang zum Accounting-Server des Anbieters an. Stellen Sie sicher, dass dieser Schlüssel im entsprechenden Accounting-Server übereinstimmend konfiguriert ist.

**SNMP-ID:** 2.24.3.7

**Pfad Telnet:** /Setup/Public-Spot-Modul/Anbieter-Tabelle/Acc.-Server-Schluessel

**Mögliche Werte:**

- max. 32 alphanumerische Zeichen

**Default:** leer

### 2.24.3.10 Acc.-Server-Loopback-Adr.

Geben Sie hier die Loopback-Adresse des Servers an, den der Public-Spot für das Accounting der Zugänge bei diesem Anbieter kontaktiert.

**Pfad Telnet:** /Setup/Public-Spot-Modul/Anbieter-Tabelle/Acc.-Server-Loopback-Adr.

**Mögliche Werte:**

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LBO ... LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

**Default:** leer

### 2.24.3.12 Acc.-Server-Protokoll

Wählen Sie hier das Protokoll, das der Public-Spot für das Accounting der Zugänge bei diesem Anbieter verwendet.

**Pfad Telnet:** /Setup/Public-Spot-Modul/Anbieter-Tabelle/Acc.-Server-Protokoll

**Mögliche Werte:**

- RADIUS
- RADSEC

**Default:** RADIUS

#### 2.24.3.8 Backup

Wählen Sie einen anderen Eintrag der Anbieter-Tabelle als Backup aus. Der Public Spot kontaktiert den Backup-Anbieter zur Authentifizierung und/oder Accounting der Zugänge, wenn der Server des primären Anbieters nicht erreichbar ist.

**SNMP-ID:** 2.24.3.8

**Pfad Telnet:** /Setup/Public-Spot-Modul/Anbieter-Tabelle/Backup

**Mögliche Werte:**

- Auswahl aus der Liste der definierten RADIUS-Anbieter, max. 16 Zeichen

**Default:** leer

### 2.24.2 Benutzer-Tabelle

Die Benutzer, welche Zugang zu Ihrem Netz erhalten sollen, werden in der Benutzer-Tabelle angelegt.

**SNMP-ID:** 2.24.2

**Pfad Telnet:** /Setup/Public-Spot-Modul

#### 2.24.2.1 Name

Tragen Sie den Namen des Benutzers ein.

**Pfad Telnet:** /Setup/Public-Spot-Modul/Benutzer-Tabelle/Name

**Mögliche Werte:**

- max. 64 Zeichen

#### 2.24.2.2 Passwort

Geben Sie ein Passwort ein.

**Pfad Telnet:** /Setup/Public-Spot-Modul/Benutzer-Tabelle/Passwort

**Mögliche Werte:**

- max. 16 Zeichen

#### 2.24.2.3 MAC-Adresse

Geben sie die MAC-adresse an.

**Pfad Telnet:** /Setup/Public-Spot-Modul/Benutzer-Tabelle/MAC-Adresse

**Mögliche Werte:**

- max. 12 Zeichen

#### 2.24.2.4 Kommentar

Hier können Sie einen Kommentar eingeben.

**Pfad Telnet:** /Setup/Public-Spot-Modul/Benutzer-Tabelle/Kommentar

**Mögliche Werte:**

- max. 80 Zeichen

### 2.24.2.5 Anbieter

Geben Sie den Namen des Anbieters ein.

**Pfad Telnet:** /Setup/Public-Spot-Modul/Benutzer-Tabelle/Anbieter

**Mögliche Werte:**

- max. 16 Zeichen

### 2.24.2.6 Ende

Geben Sie den Gültigkeitsbereich für die Einstellung an (Datum).

**Pfad Telnet:** /Setup/Public-Spot-Modul/Benutzer-Tabelle/Ende

**Mögliche Werte:**

- max. 20 Zeichen

## 2.24.31 Freie Netze

Zusätzlich zum frei erreichbaren Web-Server können Sie weitere Netze definieren, die Ihre Kunden ohne Anmeldung nutzen dürfen.

**SNMP-ID:** 2.24.31

**Pfad Telnet:** /Setup/Public-Spot-Modul

### 2.24.31.1 Host-Name

Geben Sie hier eine IP-Adresse oder einen Host-Namen für einen Server oder ein Netz ein, das Ihre Kunden ohne Anmeldung nutzen dürfen.

**SNMP-ID:** 2.24.31.1

**Pfad Telnet:** /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent/Freie-Netze/Host-Name

**Mögliche Werte:**

- max. 64 Zeichen

**Default:** leer

### 2.24.31.2 Maske

Geben Sie hier die zugehörige Netzmaske ein. Wenn Sie nur eine einzelne Station mit der zuvor angegebenen Adresse freischalten wollen, geben Sie 255.255.255.255 ein. Wenn Sie ein ganzes IP-Netz freigeben wollen, geben Sie die zugehörige Netzmaske ein.

**SNMP-ID:** 2.24.31.2

**Pfad Telnet:** /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent/Freie-Netze/Maske

**Mögliche Werte:**

- max. 15 Zeichen

**Default:** 0.0.0.0

## 2.24.15 Port-Tabelle

In dieser Tabelle aktivieren oder deaktivieren Sie die Authentifizierung über den Public Spot für die im Gerät vorhandenen Ports.

**SNMP-ID:** 2.24.15

**Pfad Telnet:** /Setup/Public-Spot-Modul/Port-Tabelle

### 2.24.15.2 Port

Wählen Sie hier den Port, für den Sie die Authentifizierung über den Public Spot aktivieren oder deaktivieren möchten.

**SNMP-ID:** 2.24.15.2

**Pfad Telnet:** /Setup/Public-Spot-Modul/Port-Tabelle/Port

**Mögliche Werte:**

- Auswahl aus den im Gerät verfügbaren Ports, z. B. LAN-1

### 2.24.15.3 Authentifizierung-erforderlich

Aktivieren oder deaktivieren Sie die Authentifizierung über den Public Spot für den gewählten Port.

**SNMP-ID:** 2.24.15.3

**Pfad Telnet:** /Setup/Public-Spot-Modul/Port-Tabelle/Authentifizierung-erforderlich

**Mögliche Werte:**

- ja
- nein

**Default:** nein

## 2.24.8 Seitentabelle

Zusätzlich zum frei erreichbaren Web-Server können Sie Spezial-Seiten definieren, die Ihre Kunden ohne Anmeldung nutzen dürfen.

In der Seitentabelle können Sie bestimmten vordefinierten Ereignissen bestimmte Seiten auf Ihren Servern zuordnen, um die für diese Ereignisse im Gerät vorhandenen Standard-Seiten zu ersetzen.

**SNMP-ID:** 2.24.8

**Pfad Telnet:** /Setup/Public-Spot-Modul

### 2.24.8.1 Seite

Name der Seite, die Ihre Kunden ohne Anmeldung nutzen dürfen.

**SNMP-ID:** 2.24.8.1

**Pfad Telnet:** /Setup/Public-Spot-Modul/Seitentabelle/Seite

### 2.24.8.2 URL

URL der Seite, die Ihre Kunden ohne Anmeldung nutzen dürfen.

**SNMP-ID:** 2.24.8.2

**Pfad Telnet:** /Setup/Public-Spot-Modul/Seitentabelle/URL

**Mögliche Werte:**

- max. 100 Zeichen

**Default:** Standardmäßig sind je nach gewählter Seite verschiedene HTML-Seiten aus dem Dateisystem des Geräts voreingestellt.

### 2.24.8.3 Rueckfall

Aktivieren oder deaktivieren Sie den Rückfall auf die eingebaute Seite für den Fall, dass der Public Spot die benutzerdefinierte URL nicht anzeigen kann.

**SNMP-ID:** 2.24.8.3

**Pfad Telnet:** /Setup/Public-Spot-Modul/Seitentabelle/Rueckfall

**Mögliche Werte:**

- ja
- nein

**Default:** nein

### 2.24.8.4 Typ

Wählen Sie den Typ der Seite.

**SNMP-ID:** 2.24.8.4

**Pfad Telnet:** /Setup/Public-Spot-Modul/Seitentabelle/Typ

**Mögliche Werte:**

- Template
- Redirect

**Default:** Template

### 2.24.8.5 Loopback-Addr.

Geben Sie eine Loopback-Adresse ein.

**SNMP-ID:** 2.24.8.5

**Pfad Telnet:** /Setup/Public-Spot-Modul/Seitentabelle/Loopback-Addr.

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

**Default:** Leer

## 2.24.20 VLAN-Tabelle

Standardmäßig werden alle Daten über das relevante Interface geroutet. Bei Angabe von VLAN-ID-Tags werden jedoch nur Daten über die relevanten Interfaces geroutet, die mit der angegebenen VLAN-ID getaggt sind. Wählen Sie hier nur VLAN-IDs aus, wenn nicht alle Datenpakete über das entsprechende Interface geroutet werden sollen.

**SNMP-ID:** 2.24.20

**Pfad Telnet:** /Setup/Public-Spot-Modul

### 2.24.20.1 VLAN-ID

Geben Sie die VLAN-ID ein.

**Pfad Telnet:** /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent/VLAN-Tabelle/VLAN-ID

**Mögliche Werte:**

- 0 bis 4096

**Default:** leer

## 2.24.7 Accounting-Meldezyklus

Geben Sie hier die Zeit in Sekunden für den Accounting-Meldezyklus ein.

**SNMP-ID:** 2.24.7

**Pfad Telnet:** /Setup/Public-Spot-Modul

## 2.24.1 Authentifizierungs-Modus

Ihr Gerät unterstützt die Benutzeranmeldung via Public-Spot. Die Anmeldung erfolgt dabei mit Benutzername und Passwort. Zusätzlich können Sie auch die Überprüfung der MAC-Adresse fordern.

Die Benutzer, welche Zugang zu Ihrem Netz erhalten sollen, werden in der Benutzer-Tabelle angelegt.

**SNMP-ID:** 2.24.1

**Pfad Telnet:** /Setup/Public-Spot-Modul

**Mögliche Werte:**

- Keine
- Benutzer+Passwort
- MAC+Benutzer+Passwort

## 2.24.16 Auto-Löschen-Benutzer-Tabelle

Bestimmen Sie, ob die automatische Bereinigung der Benutzer-Liste aktiviert ist. Da die Größe der Benutzer-Tabelle beschränkt ist, sollten verwaiste Konten so bald wie möglich gelöscht werden.

**SNMP-ID:** 2.24.16

**Pfad Telnet:** /Setup/Public-Spot-Modul

**Mögliche Werte:**

- ja
- nein

**Default:** nein

## 2.24.30 Freier-Server

Geben Sie hier die IP-Adresse der öffentlichen Seite Ihres Public-Spot Dienstes an. Auf dieser Seite sollten Sie Informationen anbieten, die den neuen Benutzer in die Lage versetzen, Sie zu kontaktieren, um sich bei Ihnen anzumelden.

**SNMP-ID:** 2.24.30

**Pfad Telnet:** /Setup/Public-Spot-Modul/Freier-Server

**Mögliche Werte**:

- max. 64 Zeichen

**Default:** leer

## 2.24.22 Geräte-Hostname

Zertifikate werden üblicherweise auf DNS-Namen ausgestellt, deswegen muss der PublicSpot hier anstelle einer internen IPAdresse den DNS-Namen des Zertifikats als Ziel angeben. Dieser Name muss im DNS-Server auf die entsprechende IP-Adresse des PublicSpots aufgelöst werden.

**SNMP-ID:** 2.24.22

**Pfad Telnet:** /Setup/Public-Spot-Modul

**Mögliche Werte:**

- max. 31 Zeichen

**Default:** leer

## 2.24.14 Idle-Timeout

Wenn eine Leerlaufzeitüberschreitung definiert wird (entweder hier oder über RADIUS), beendet der Public-Spot die Verbindung, wenn innerhalb des angegebenen Intervalls keine Daten vom Client empfangen wurden.

**SNMP-ID:** 2.24.14

**Pfad Telnet:** /Setup/Public-Spot-Modul

**Mögliche Werte**:

- max. 10 Zeichen

**Default:** 0

## 2.24.12 Kommunikations-Port

Stellen Sie hier den Port ein, über den der Public Spot mit den angemeldeten Clients kommuniziert.

**SNMP-ID:** 2.24.12

**Pfad Telnet:** /Setup/Public-Spot-Modul/Kommunikations-Port

**Mögliche Werte:**

- Gültige Port-Bezeichnung, max. 5 Zeichen

**Default:** leer

## 2.24.21 Login-Seiten-Typ

Wählen Sie aus, über welches Protokoll der Public Spot die Login-Seiten anzeigt.

**SNMP-ID:** 2.24.21

**Pfad Telnet:** /Setup/Public-Spot-Modul/Login-Seiten-Typ

**Mögliche Werte**:

- HTTP
- HTTPS

**Default:** HTTPS

## 2.24.9 Roaming-Schluessel

Beim Wechsel in den Funkbereich einer anderen Basis-Station (Roaming) wird die erneute Anmeldung erforderlich. Wenn Sie sich im Überschneidungsbereich zweier Basis-Stationen befinden, kann es sogar zu einem regelmäßigen Verbindungswechsel zwischen beiden Basis-Stationen kommen. Die Angabe des Roaming Secret ermöglicht die Übergabe einer Public-Spot-Sitzung an anderen Access Point ohne Neuanmeldung.

**SNMP-ID:** 2.24.9

**Pfad Telnet:** /Setup/Public-Spot-Modul/Roaming-Schluessel

**Mögliche Werte**:

- max. 32 Zeichen

**Default:** leer

## 2.24.17 Server-Datenbank-liefern

Wählen Sie hier aus, ob der Public Spot die MAC-Adressliste über RADIUS zur Verfügung stellt.

**SNMP-ID:** 2.24.17

**Pfad Telnet:** /Setup/Public-Spot-Modul/Server-Datenbank-liefern

**Mögliche Werte**:

- ja
- nein

**Default:** nein

## 2.24.6 Server-Verzeichnis

Geben Sie hier das Verzeichnis der öffentlichen Seite Ihres Public-Spot Dienstes an. Auf dieser Seite sollten Sie Informationen anbieten, die den neuen Benutzer in die Lage versetzen, Sie zu kontaktieren, um sich bei Ihnen anzumelden.

**SNMP-ID:** 2.24.6

**Pfad Telnet:** /Setup/Public-Spot-Modul/Server-Verzeichnis

**Mögliche Werte**:

- max. 127 Zeichen

**Default:** leer

## 2.24.5 Traffic-Limit-Bytes

Bereits vor der Anmeldung sind unabhängig von den oben angegebenen Servern, Netzen und Seiten einige DHCP-, DNS- und ARP-Anfragen notwendig. Diese sind daher grundsätzlich erlaubt. Sie können allerdings dazu missbraucht werden, unberechtigterweise andere Daten zu tunneln.

Hier können Sie daher ein maximales Transfervolumen definieren. Es umfasst ausschließlich Daten, welche vor der Anmeldung und nicht vom bzw. zum oben angegebenen freien Web-Server übertragen werden. Dieser bleibt zu jeder Zeit unlimitiert.

**SNMP-ID:** 2.24.5

**Pfad Telnet:** /Setup/Public-Spot-Modul

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

### 2.24.18 Verbiete-Mehrfach-Logins

Erlaubt die mehrfache Anmeldung mit einem Benutzer-Account zur gleichen Zeit.

**SNMP-ID:** 2.24.18

**Pfad Telnet:** /Setup/Public-Spot-Modul

**Mögliche Werte:**

- nein
- ja

**Default:** nein

Die Option für die Mehrfach-Logins muss deaktiviert werden, wenn der RADIUS-Benutzer ein Zeit-Budget erhalten soll. Die Einhaltung des Zeit-Budgets kann nur überwacht werden, wenn für den Benutzer zu jeder Zeit nur eine Sitzung aktiv ist.

### 2.24.26 Stations-Tabellen-Limit

Sie können die maximale Anzahl der Clients auf bis zu 65536 Teilnehmer vergrößern.

**SNMP-ID:**

2.24.26

**Pfad Telnet:**

**Setup** > **Public-Spot-Modul** > **Stations-Tabellen-Limit**

**Mögliche Werte:**

16 bis 65536

**Default:**

8192

Während des Betriebs wird ausschließlich eine Erweiterung der Stationstabelle sofort übernommen. Starten Sie den Access-Point neu, damit eine Reduzierung der Stationstabelle wirksam wird.

## 2.25 RADIUS

Dieses Menü enthält die Einstellungen für den RADIUS-Server.

**SNMP-ID:** 2.25

**Pfad Telnet:** /Setup

### 2.25.4 Auth.-Timeout

Dieser Wert gibt an, nach wie vielen Millisekunden eine erneute RADIUS-Authentifizierung versucht werden soll.

**SNMP-ID:** 2.25.4

**Pfad Telnet:** /Setup/RADIUS

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 5000

## 2.25.5 Auth.-Wiederholung

Dieser Wert gibt an, wie viele Authentifizierungs-Versuche insgesamt durchgeführt werden, bevor eine Ablehnung erfolgt.

**SNMP-ID:** 2.25.5

**Pfad Telnet:** /Setup/RADIUS

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 3

## 2.25.9 Backup-Abfrage-Strategie

Dieser Wert gibt an, wie das Gerät mit unbeantworteten Anfragen mehrerer RADIUS-Server umgehen soll.

**SNMP-ID:** 2.25.9

**Pfad Telnet:** /Setup/RADIUS/Backup-Abfrage-Strategie

**Mögliche Werte**:

- Block: das Gerät schickt zunächst die maximale Anzahl an Wiederholungsanfragen an den ersten Server zurück, bevor es diese an den Backup-Server weiterleitet.
- Zyklisch: das Gerät schickt unbeantwortete Anfragen abwechselnd an die konfigurierten Server.

**Default**: Block

## 2.25.10 Server

Dieses Menü enthält die Einstellungen für den RADIUS-Server.

**SNMP-ID:** 2.25.10

**Pfad Telnet:** /Setup/RADIUS

### 2.25.10.12 Accounting-Interim-Intervall

Geben Sie hier an, welchen Wert der RADIUS-Server bei erfolgreicher Authentifizierung als "Accounting-Interim-Interval" ausgeben soll. Sofern das anfragende Gerät dieses Attribut unterstützt, wird damit gesteuert, in welchem Intervall (in Sekunden) ein Update der Accounting-Daten an den Accounting-RADIUS-Server geschickt wird.

**SNMP-ID:** 2.25.10.12

**Pfad Telnet:** /Setup/RADIUS/Server

**Mögliche Werte:**

- max. 4 Ziffern

**Default:** 0

**Besondere Werte:** 0: schaltet die Verwendung dieser Funktion aus.

### 2.25.10.11 Accounting-Port

Geben Sie hier den Port an, über den der RADIUS-Server Accounting-Informationen entgegennimmt. Üblicherweise wird der Port 1813 verwendet.

**SNMP-ID:** 2.25.10.11

**Pfad Telnet:** /Setup/RADIUS/Server

**Mögliche Werte:**

- max. 4 Ziffern

**Default:** 0

**Besondere Werte:** 0: schaltet die Verwendung dieser Funktion aus.

### 2.25.10.1 Authentifizierungs-Port

Geben Sie hier den Port an, über den die Authenticator mit dem RADIUS-Server im Access Point kommunizieren.

**SNMP-ID:** 2.25.10.1

**Pfad Telnet:** /Setup/RADIUS/Server

**Mögliche Werte:**

- max. 5 Ziffern

**Default:** 0

**Besondere Werte:** 0: schaltet den RADIUS-Server aus.

### 2.25.10.14 Auto-Loeschen-Benutzer-Tabelle

Wenn diese Funktion aktiviert ist, dann löscht der RADIUS-Server automatisch Accounts aus der Benutzertabelle, deren Ablaufdatum überschritten ist.

**Pfad Telnet:** /Setup/RADIUS/Server/Auto-Loeschen-Benutzer-Tabelle

**Mögliche Werte:**

- ja
- nein

**Default:** nein

### 2.25.10.5 Default-Realm

Dieser Realm wird verwendet, wenn der übermittelte Benutzername einen unbekannten Realm verwendet, der nicht in der Liste der Weiterleitungs-Server enthalten ist.

**SNMP-ID:** 2.25.10.5

**Pfad Telnet:** /Setup/RADIUS/Server

**Mögliche Werte:**

- max. 24 Zeichen

**Default:** Leer

### 2.25.10.6 Empty-Realm

Dieser Realm wird verwendet, wenn der übermittelte Benutzername keinen Realm enthält.

**SNMP-ID:** 2.25.10.6

**Pfad Telnet:** /Setup/RADIUS/Server

**Mögliche Werte:**

- max. 24 Zeichen

**Default:** Leer

## 2.25.10.13 RADSEC-Port

Geben Sie hier an, über welchen (TCP-)Port der Server über RADSEC verschlüsselte Accounting- oder Authentifizierungs-Anfragen annimmt. Üblicherweise wird Port 2083 verwendet.

**SNMP-ID:** 2.25.10.13

**Pfad Telnet:** /Setup/RADIUS/Server

**Mögliche Werte:**

- max. 5 Ziffern

**Default:** 0

**Besondere Werte:** 0: deaktiviert RADSEC im RADIUS-Server.

## 2.25.10.2 Clients

In der Clients-Tabelle werden die Clients eingetragen, die mit dem RADIUS-Server kommunizieren können.

**SNMP-ID:** 2.25.10.2

**Pfad Telnet:** /Setup/RADIUS/Server

### 2.25.10.2.1 IP-Netz

IP-Netz (Bereich von IP-Adressen) der RADIUS-Clients, für die das in diesem Eintrag definierte Kennwort gilt.

**SNMP-ID:** 2.25.10.2.1

**Pfad Telnet:** /Setup/RADIUS/Server/Clients

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** Leer

### 2.25.10.2.2 Secret

Kennwort, das der Client für den Zugang zum RADIUS-Server im LANCOM Access Point benötigt.

**SNMP-ID:** 2.25.10.2.2

**Pfad Telnet:** /Setup/RADIUS/Server/Clients

**Mögliche Werte:**

- max. 32 Zeichen

**Default:** Leer

### 2.25.10.2.3 IP-Netzmaske

IP-Netzmaske des RADIUS-Clients.

**SNMP-ID:** 2.25.10.2.3

**Pfad Telnet:** /Setup/RADIUS/Server/Clients

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** Leer

#### 2.25.10.2.4 Protokoll

Protokoll für die Kommunikation zwischen dem internen RADIUS-Server und den Clients.

**SNMP-ID:** 2.25.10.2.4

**Pfad Telnet:** /Setup/RADIUS/Server/Clients

**Mögliche Werte:**

- RADSEC
- RADIUS
- alle

**Default:** RADIUS

### 2.25.10.3 Weiterleit-Server

Wenn Sie RADIUS-Weiterleitung nutzen möchten, müssen Sie hier weitere Angaben machen.

**SNMP-ID:** 2.25.10.3

**Pfad Telnet:** /Setup/RADIUS/Server

#### 2.25.10.3.1 Realm

Zeichenkette, mit der das Weiterleitungs-Ziel identifiziert wird.

**SNMP-ID:** 2.25.10.3.1

**Pfad Telnet:** /Setup/RADIUS/Server/Weiterleit-Server

**Mögliche Werte:**

- max. 24 Zeichen

**Default:** Leer

#### 2.25.10.3.2 IP-Adresse

IP-Adresse des RADIUS-Servers, an den die Anfrage weitergeleitet werden soll.

**SNMP-ID:** 2.25.10.3.2

**Pfad Telnet:** /Setup/RADIUS/Server/Weiterleit-Server

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

#### 2.25.10.3.3 Port

Offener Port, über den mit dem Weiterleitungs-Server kommuniziert werden kann.

**SNMP-ID:** 2.25.10.3.3

**Pfad Telnet:** /Setup/RADIUS/Server/Weiterleit-Server

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

#### 2.25.10.3.4 Secret

Kennwort, das für den Zugang zum Weiterleitungs-Server benötigt wird.

**SNMP-ID:** 2.25.10.3.4

**Pfad Telnet:** /Setup/RADIUS/Server/Weiterleit-Server

**Mögliche Werte:**

- max. 32 Zeichen

**Default:** Leer

#### 2.25.10.3.5 Backup

Alternativer Weiterleitungs-Server, an den Anfragen weitergeleitet werden, wenn der erste Weiterleitungs-Server nicht erreichbar ist.

**SNMP-ID:** 2.25.10.3.5

**Pfad Telnet:** /Setup/RADIUS/Server/Weiterleit-Server

**Mögliche Werte:**

- max. 24 Zeichen

**Default:** Leer

#### 2.25.10.3.6 Loopback-Addr.

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

**SNMP-ID:** 2.25.10.3.6

**Pfad Telnet:** /Setup/RADIUS/Server/Weiterleit-Server

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

**Default:** Leer

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, wird die zugehörige IP-Adresse verwendet.

#### 2.25.10.3.7 Protokoll

Protokoll für die Kommunikation zwischen dem internen RADIUS-Server und dem Weiterleitungs-Server.

**SNMP-ID:** 2.25.10.3.7

**Pfad Telnet:** /Setup/RADIUS/Server/Weiterleit-Server

**Mögliche Werte:**

- RADSEC
- RADIUS

**Default:** RADIUS

### 2.25.10.7 Benutzer

Tragen Sie in die folgende Tabelle die Daten der Benutzer ein, die von diesem Server authentifiziert werden.

**SNMP-ID:** 2.25.10.7

**Pfad Telnet:** /Setup/RADIUS/Server/Benutzer

**Mehrfach-Logins**

Erlaubt die mehrfache Anmeldung mit einem Benutzer-Account zur gleichen Zeit.

Mögliche Werte: Ja, Nein

Default: Ja

Die Option für die Mehrfach-Logins muss deaktiviert werden, wenn der RADIUS-Benutzer ein Zeit-Budget erhalten soll. Die Einhaltung des Zeit-Budgets kann nur überwacht werden, wenn für den Benutzer zu jeder Zeit nur eine Sitzung aktiv ist.

**Ablauf-Art**

Diese Option legt fest, wie die Gültigkeitsdauer des Benutzer-Accounts bestimmt wird.

Mögliche Werte:

- Absolut: Die Gültigkeit des Benutzer-Accounts endet zu einem festen Zeitpunkt.
- Relativ: Die Gültigkeit des Benutzer-Accounts endet eine bestimmte Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.

Default: Leer: Die Gültigkeit des Benutzer-Accounts endet nie, es sei denn, ein definiertes Zeit- oder Volumen-Budget wird erreicht.

Die beiden Optionen können kombiniert werden. In diesem Fall endet die Gültigkeit des Benutzer-Accounts dann, wenn einer der beiden Grenzwerte erreicht wird.

Für die Nutzung der Zeit-Budgets bei Benutzer-Accounts muss das Gerät über eine gültige Zeit verfügen, da ansonsten der Ablauf der Gültigkeit nicht geprüft werden kann.

**Abs.-Ablauf**

Wenn der Ablauf-Typ "Absolut" aktiviert ist, endet die Gültigkeit des Benutzer-Accounts zu dem in diesem Wert angegebenen Zeitpunkt.

Mögliche Werte: Gültige Zeitinformation aus Datum und Uhrzeit. Maximal 20 Zeichen aus 0123456789/:.Pp

Default: Leer

Besondere Werte: 0 schaltet die Überwachung der absoluten Ablaufzeit aus.

**Rel.-Ablauf**

Wenn der Ablauf-Typ "Relativ" aktiviert ist, endet die Gültigkeit des Benutzer-Accounts nach der in diesem Wert angegebenen Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.

Mögliche Werte: Zeitspanne in Sekunden. Maximal 10 Zeichen aus 0123456789

Default: 0

Besondere Werte: 0 schaltet die Überwachung der relativen Ablaufzeit aus.

**Zeit-Budget**

Maximale Nutzungsdauer für diesen Benutzer-Account. Diese Nutzungsdauer kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.

Mögliche Werte: Zeitspanne in Sekunden. Maximal 10 Zeichen aus 0123456789

Default: 0

Besondere Werte: 0 schaltet die Überwachung der Nutzungsdauer aus.

**Volumen-Budget**

Maximales Datenvolumen für diesen Benutzer-Account. Dieses Datenvolumen kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.

Mögliche Werte: Volumen-Budget in Bytes. Maximal 10 Zeichen aus 0123456789

Default: 0

Besondere Werte: 0 schaltet die Überwachung des Datenvolumens aus.

**Kommentar**

Kommentar zu diesem Eintrag.

**Service-Typ**

Der Service-Typ ist ein spezielles Attribut des RADIUS-Protokoll, welches der NAS (Network Access Server) mit dem Authentication Request übermittelt. Der Request wird nur dann positiv beantwortet, wenn der angefragte Service-Typ mit dem Service-Typ des Benutzer-Accounts übereinstimmt.

Mögliche Werte:

- Umrahmt: Für Prüfung von WLAN-MAC-Adressen über RADIUS bzw. bei IEEE 802.1x.
- Login: Für Public-Spot-Anmeldungen.
- Nur-Auth.: Für Einwahl-Gegenstellen über PPP, die mit RADIUS authentifiziert werden.
- Beliebig

Default: Beliebig

Die Anzahl der Einträge mit dem Service-Typ "Beliebig" oder "Login" ist je nach Modell auf 64 oder 256 begrenzt. So wird die Tabelle nicht vollständig mit Einträgen von Public-Spot-Zugängen belegt (die den Service-Typ "Beliebig" verwenden) und ermöglicht eine parallele Nutzung für Anmeldungen über 802.1x.

#### 2.25.10.7.1 Benutzername

Name des Benutzers.

**SNMP-ID:** 2.25.10.7.1

**Pfad Telnet:** /Setup/RADIUS/Server/Benutzer

**Mögliche Werte:**

- max. 48 Zeichen

**Default:** Leer

#### 2.25.10.7.10 Abs.-Ablauf

Wenn der Ablauf-Typ "Absolut" aktiviert ist, endet die Gültigkeit des Benutzer-Accounts zu dem in diesem Wert angegebenen Zeitpunkt.

**SNMP-ID:** 2.25.10.7.10

**Pfad Telnet:** /Setup/RADIUS/Server/Abs.-Ablauf

**Mögliche Werte:**

- Gültige Zeitinformation aus Datum und Uhrzeit. Maximal 20 Zeichen aus 0123456789/:.

**Default:** 0

**Besondere Werte:** 0 schaltet die Überwachung der absoluten Ablaufzeit aus.

#### 2.25.10.7.11 Zeit-Budget

Maximale Nutzungsdauer für diesen Benutzer-Account. Diese Nutzungsdauer kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.

**SNMP-ID:** 2.25.10.7.11

**Pfad Telnet:** /Setup/RADIUS/Server/Zeit-Budget

**Mögliche Werte:**

- Zeitspanne in Sekunden. Maximal 10 Zeichen aus 0123456789

**Default:** 0

**Besondere Werte:** 0 schaltet die Überwachung der Nutzungsdauer aus.

#### 2.25.10.7.12 Volumen-Budget

Maximales Datenvolumen für diesen Benutzer-Account. Dieses Datenvolumen kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.

**Pfad Telnet:** /Setup/RADIUS/Server/Volumen-Budget

**Mögliche Werte:**

- Volumen-Budget in Bytes. Maximal 10 Zeichen aus 0123456789

**Default:** 0

**Besondere Werte:** 0 schaltet die Überwachung des Datenvolumens aus.

#### 2.25.10.7.13 Ablauf-Typ

Diese Option legt fest, wie die Gültigkeitsdauer des Benutzer-Accounts bestimmt wird.

**Pfad Telnet:** /Setup/RADIUS/Server/Weiterleit-Server/Ablauf-Typ

**Mögliche Werte:**

- absolut: Die Gültigkeit des Benutzer-Accounts endet zu einem festen Zeitpunkt.
- relativ: Die Gültigkeit des Benutzer-Accounts endet eine bestimmte Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.
- keiner: Die Gültigkeit des Benutzer-Accounts endet nie, es sei denn, ein definiertes Zeit- oder Volumen-Budget wird erreicht.

**Default:** absolut

Die beiden Optionen können kombiniert werden. In diesem Fall endet die Gültigkeit des Benutzer-Accounts dann, wenn einer der beiden Grenzwerte erreicht wird.

Für die Nutzung der Zeit-Budgets bei Benutzer-Accounts muss das Gerät über eine gültige Zeit verfügen, da ansonsten der Ablauf der Gültigkeit nicht geprüft werden kann.

#### 2.25.10.7.14 Rel.-Ablauf

Wenn der Ablauf-Typ “Relativ” aktiviert ist, endet die Gültigkeit des Benutzer-Accounts nach der in diesem Wert angegebenen Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.

**SNMP-ID:** 2.25.10.7.14

**Pfad Telnet:** /Setup/RADIUS/Server/Rel.-Ablauf

**Mögliche Werte:**

- Zeitspanne in Sekunden. Maximal 10 Zeichen aus 0123456789

**Default:** 0

**Besondere Werte:** 0 schaltet die Überwachung der relativen Ablaufzeit aus.

#### 2.25.10.7.15 Kommentar

Kommentar zu diesem Eintrag.

**SNMP-ID:** 2.25.10.7.15

**Pfad Telnet:** /Setup/RADIUS/Server/Kommentar

**Mögliche Werte:**

- Max. 64 Zeichen

**Default:** leer

#### 2.25.10.7.16 Service-Typ

Der Service-Typ ist ein spezielles Attribut des RADIUS-Protokoll, welches der NAS (Network Access Server) mit dem Authentication Request übermittelt. Der Request wird nur dann positiv beantwortet, wenn der angefragte Service-Typ mit dem Service-Typ des Benutzer-Accounts übereinstimmt. Der Service-Typ für Public-Spot ist z. B. 'Login', für 802.1x 'Umrahmt'.

**SNMP-ID:** 2.25.10.7.16

**Pfad Telnet:** /Setup/RADIUS/Server/Service-Typ

**Mögliche Werte:**

- Beliebig
- Umrahmt: Für Prüfung von WLAN-MAC-Adressen über RADIUS bzw. bei IEEE 802.1x.
- Login: Für Public-Spot-Anmeldungen.
- Nur-Auth.: Für Einwahl-Gegenstellen über PPP, die mit RADIUS authentifiziert werden.

**Default:** Beliebig

Die Anzahl der Einträge mit dem Service-Typ “Beliebig” oder “Login” ist je nach Modell auf 64 oder 256 begrenzt. So wird die Tabelle nicht vollständig mit Einträgen von Public-Spot-Zugängen belegt (die den Service- Typ “Beliebig” verwenden) und ermöglicht eine parallele Nutzung für Anmeldungen über 802.1x.

#### 2.25.10.7.2 Passwort

Passwort des Benutzers.

**SNMP-ID:** 2.25.10.7.2

**Pfad Telnet:** /Setup/RADIUS/Server/Benutzer

**Mögliche Werte:**

- max. 32 Zeichen

**Default:** Leer

#### 2.25.10.7.3 Limitiere-Auth-Methoden

Mit dieser Option können die für den Benutzer erlaubten Authentifizierungsverfahren eingeschränkt werden.

**SNMP-ID:** 2.25.10.7.3

**Pfad Telnet:** /Setup/RADIUS/Server/Benutzer

**Mögliche Werte:**

- Beliebige Kombination aus folgenden Werten:
- PAP
- CHAP
- MSCHAP
- MSCHAPv2
- EAP
- Alle

**Default:** Alle

#### 2.25.10.7.4 VLAN-Id

Mit dieser Option kann dem Benutzer bei erfolgreicher Authentifizierung eine bestimmte VLAN-ID zugewiesen werden.

**SNMP-ID:** 2.25.10.7.4

**Pfad Telnet:** /Setup/RADIUS/Server/Benutzer

**Mögliche Werte:**

- 0 bis 4094

**Default:** 0

**Besondere Werte:** 0: Es wird keine VLAN-ID zugewiesen.

#### 2.25.10.7.5 Rufende-Station-Id-Maske

Mit dieser Maske wird die Gültigkeit des Eintrags auf bestimmte IDs eingeschränkt, die von der rufenden Station (WLAN-Client) übermittelt wird. Bei der Authentifizierung über 802.1x wird die MAC-Adresse der rufenden Station im ASCII-Format (nur Großbuchstaben) übertragen, dabei werden Zeichenpaare durch einen Bindestrich getrennt (z. B. "00-10-A4-23-19-C0")

**SNMP-ID:** 2.25.10.7.5

**Pfad Telnet:** /Setup/RADIUS/Server/Benutzer

**Mögliche Werte:**

- max. 48 Zeichen

**Default:** Leer

**Besondere Werte:** Mit dem * als Platzhalter können ganze Gruppen von IDs erfasst und als Maske definiert werden.

#### 2.25.10.7.6 Gerufene-Station-Id-Maske

Mit dieser Maske wird die Gültigkeit des Eintrags auf bestimmte IDs eingeschränkt, die von der gerufenen Station (BSSID und SSID des Access Point) übermittelt wird. Bei der Authentifizierung über 802.11x werden MAC-Adresse (BSSID) der gerufenen Station im ASCII-Format (nur Großbuchstaben) übertragen, dabei werden Zeichenpaare durch einen Bindestrich getrennt. Die SSID wird nach einem Doppelpunkt als Trennzeichen angehängt (z. B. "00-10-A4-23-19-C0:AP1")

**SNMP-ID:** 2.25.10.7.6

**Pfad Telnet:** /Setup/RADIUS/Server/Benutzer

**Mögliche Werte:**

- max. 48 Zeichen

**Default:** Leer

**Besondere Werte:** Mit dem * als Platzhalter können ganze Gruppen von IDs erfasst und als Maske definiert werden. Mit der Maske "*:AP1" wird z. B. ein Eintrag definiert, der für einen Client in der Funkzelle mit dem Namen "AP1" gilt, egal über welchen Access Point der Client sich eingebucht hat. Auf diese Weise kann der Client von einem Access Point zum nächsten wechseln (Roaming) und jeweils mit den gleichen Authentifizierungsdaten arbeiten.

#### 2.25.10.7.7 Tx-Limit

Begrenzung der Bandbreite für RADIUS-Clients.

**Pfad Telnet:** /Setup/RADIUS/Server/Benutzer/Tx-Limit

**Mögliche Werte:**

- 0 bis 4294967295 (2^32-1)

**Default:** 0

#### 2.25.10.7.8 Rx-Limit

Begrenzung der Bandbreite für RADIUS-Clients.

**Pfad Telnet:** /Setup/RADIUS/Server/Benutzer/Rx-Limit

**Mögliche Werte:**

- 0 bis 4294967295 (2^32-1)

**Default:** 0

#### 2.25.10.7.9 Mehrfach-Logins

Erlaubt oder verbietet mehr als eine parallele Session mit der gleichen Benutzer-ID. Wenn parallele Sessions verboten sind, wird das Gerät Authentifizierungs-Anfragen für die aktuelle Benutzer-ID zurückweisen, wenn bereits eine Session für diesen Benutzer in der aktiven Session-Abrechnungs-Tabelle läuft. Dies ist eine Voraussetzung für eine sinnvolle Durchsetzung von Zeit- oder Volumen-Budgets.

**Pfad Telnet:** /Setup/RADIUS/Server/Mehrfach-Logins

**Mögliche Werte:**

- ja
- nein

**Default:** ja

Die Option für die Mehrfach-Logins muss deaktiviert werden, wenn der RADIUS-Benutzer ein Zeit-Budget erhalten soll. Die Einhaltung des Zeit-Budgets kann nur überwacht werden, wenn für den Benutzer zu jeder Zeit nur eine Sitzung aktiv ist.

### 2.25.10.10 EAP

Dieses Menü enthält die Einstellungen für EAP.

**SNMP-ID:** 2.25.10.10

**Pfad Telnet:** /Setup/RADIUS/Server

#### 2.25.10.10.6 PEAP-Vorgabe-Tunnel-Methode

Bei der Verwendung von PEAP werden zwei Authentifizierungmethoden ausgehandelt. Zunächst wird über EAP ein sicherer (TLS-Tunnel) ausgehandelt. In diesem Tunnel wird dann wiederum ein zweites Authentifizierungverfahren ausgehandelt. Bei diesen Verhandlungen bietet der Server jeweils ein Verfahren an, welches der Client annehmen (ACK) oder anlehnen (NAK) kann. Lehnt der Client ab, schickt er dem Server einen Vorschlag mit einem verfahren, welches er

gerne nutzen würde. Ist das vom Client vorgeschlagene Verfahren im Server erlaubt, so wird es verwendet, ansonsten bricht der Server die Verhandlung ab.

Mit diesem Parameter wird das Verfahren festgelegt, das der Server den Clients als Authentifizierungverfahren im TLS-Tunnel anbieten soll. Durch diese Vorgabe können abgelehnte Vorschläge bei der Verhandlung vermieden und so die Verhandlung beschleunigt werden.

**SNMP-ID:** 2.25.10.10.6

**Pfad Telnet:** /Setup/RADIUS/Server/EAP

**Mögliche Werte:**

- Keine
- MD5
- GTC
- MSCHAPv2

**Default:** MSCHAPv2

#### 2.25.10.10.3 Reauth-Periode

Wenn der interne RADIUS-Server auf die Anfrage eines Clients mit einem CHALLENGE antwortet (Verhandlung des Authentifizierungsverfahrens ist noch nicht abgeschlossen), kann der RADIUS-Server dem Authenticator mitteilen, wie lange (in Sekunden) er auf eine Antwort des Clients warten soll, bevor der CHALLENGE erneut zugestellt wird.

**SNMP-ID:** 2.25.10.10.3

**Pfad Telnet:** /Setup/RADIUS/Server/EAP

**Mögliche Werte:**

- max. 10 Ziffern

**Default:** 0

**Besondere Werte:** 0: Es wird kein Timeout an den Authenticator übermittelt.

Diese Funktion wird nicht von jedem Authenticator unterstützt.

#### 2.25.10.10.4 Retransmit-Timeout

Wenn der interne RADIUS-Server auf die Anfrage eines Clients mit einem ACCEPT antwortet (Verhandlung des Authentifizierungsverfahrens ist erfolgreich abgeschlossen), kann der RADIUS-Server dem Authenticator mitteilen, nach welcher Zeit (in Sekunden) er eine erneute Authentifizierung des Clients auslösen soll.

**SNMP-ID:** 2.25.10.10.4

**Pfad Telnet:** /Setup/RADIUS/Server/EAP

**Mögliche Werte:**

- max. 10 Ziffern

**Default:** 0

**Besondere Werte:** 0: Es wird kein Timeout an den Authenticator übermittelt.

Diese Funktion wird nicht von jedem Authenticator unterstützt.

#### 2.25.10.10.2 TLS-Pruefe-Benutzernamen

Bei TLS authentifiziert sich der Client alleine über sein Zertifikat. Ist diese Option aktiviert, so prüft der RADIUSServer zusätzlich, ob der im Zertifikat hinterlegte Benutzername in der RADIUS-Benutzertabelle enthalten ist.

**SNMP-ID:** 2.25.10.10.2

**Pfad Telnet:** /Setup/RADIUS/Server/EAP

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

#### 2.25.10.10.5 TTLS-Vorgabe-Tunnel-Methode

Bei der Verwendung von TTLS werden zwei Authentifizierungmethoden ausgehandelt. Zunächst wird über EAP ein sicherer (TLS-Tunnel) ausgehandelt. In diesem Tunnel wird dann wiederum ein zweites Authentifizierungverfahren ausgehandelt. Bei diesen Verhandlungen bietet der Server jeweils ein Verfahren an, welches der Client annehmen (ACK) oder anlehnen (NAK) kann. Lehnt der Client ab, schickt er dem Server einen Vorschlag mit einem verfahren, welches er gerne nutzen würde. Ist das vom Client vorgeschlagene Verfahren im Server erlaubt, so wird es verwendet, ansonsten bricht der Server die Verhandlung ab.

Mit diesem Parameter wird das Verfahren festgelegt, das der Server den Clients als Authentifizierungverfahren im TLS-Tunnel anbieten soll. Durch diese Vorgabe können abgelehnte Vorschläge bei der Verhandlung vermieden und so die Verhandlung beschleunigt werden.

**SNMP-ID:** 2.25.10.10.5

**Pfad Telnet:** /Setup/RADIUS/Server/EAP

**Mögliche Werte:**

- Keine
- MD5
- GTC
- MSCHAPv2

**Default:** MD5

#### 2.25.10.10.1 Tunnel-Server

Realm als Verweis auf den Eintrag in der Tabelle der Weiterleitungs-Server, der für getunnelte TTLS bzw. PEAP-Anfragen verwendet werden soll.

**SNMP-ID:** 2.25.10.10.1

**Pfad Telnet:** /Setup/RADIUS/Server/EAP

**Mögliche Werte:**

- max. 24 Zeichen

**Default:** Leer

#### 2.25.10.10.7 Default-Methode

Gibt, welche Methode der RADIUS-Server dem Client außerhalb eines eventuellen TTLS/PEAP-Tunnels anbieten soll.

**SNMP-ID:** 2.25.10.10.7

**Pfad Telnet:** /Setup/RADIUS/Server/EAP

**Mögliche Werte:**

- Keine
- MD5
- GTC

- MSCHAPv2
- TLS
- TTLS
- PEAP

**Default:** MD5

#### 2.25.10.10.8 Vorgabe-MTU

Definieren Sie hier die Maximum Transmission Unit, die das Gerät als Default für EAP-Verbindungen benutzt.

**SNMP-ID:** 2.25.10.10.8

**Pfad Telnet:** /Setup/RADIUS/Server/EAP/Vorgabe-MTU

**Mögliche Werte:**

- 100 bis 1496 Bytes

**Default:** 1036 Bytes

## 2.26 NTP

Dieses Menü enthält die Einstellungen für NTP.

**SNMP-ID:** 2.26

**Pfad Telnet:** /Setup

### 2.26.2 Aktiv

Schalten Sie hier den Zeit-Server Ihres Gerätes für das lokale Netz ein. Andere Geräte im gleichen Netz können sich dann mit diesem Server über das Netzwerk-Zeit-Protokoll (NTP) synchronisieren.

**SNMP-ID:** 2.26.2

**Pfad Telnet:** /Setup/NTP

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

### 2.26.4 BC-Intervall

Stellen Sie hier den zeitlichen Abstand ein, in welchem der Zeit-Server Ihres Gerätes jeweils die aktuelle Zeit an alle erreichbaren Geräte oder Stationen des lokalen Netzes senden soll.

**SNMP-ID:** 2.26.4

**Pfad Telnet:** /Setup/NTP

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 64

## 2.26.3 BC-Modus

Schalten Sie hier den Zeit-Server Ihres Gerätes in den Sende-Modus. In diesem Modus sendet er in regelmäßigen Abständen die jeweils aktuelle Zeit an alle erreichbaren Geräte oder Stationen des lokalen Netzes.

**SNMP-ID:** 2.26.3

**Pfad Telnet:** /Setup/NTP

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

## 2.26.7 RQ-Intervall

Geben Sie hier das Zeitintervall in Sekunden an, nach dem eine Überprüfung und gegebenenfalls Neusynchronisierung der internen Uhr des Gerätes mit einem der angegebenen Zeit-Server (NTP) erfolgen soll.

**SNMP-ID:** 2.26.7

**Pfad Telnet:** /Setup/NTP

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 86400

Zum Erreichen der Zeit-Server wird bei Bedarf eine Verbindung aufgebaut. Bitte bedenken Sie, dass hierdurch zusätzliche Kosten entstehen können.

## 2.26.12 RQ-Versuche

Geben Sie hier an, wie oft eine Synchronisation mit dem Zeit-Server versucht werden soll. Bei Angabe einer Null wird so lange versucht, bis eine gültige Synchronisation durchgeführt wurde.

**SNMP-ID:** 2.26.12

**Pfad Telnet:** /Setup/NTP

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 4

## 2.26.11 RQ-Addresse

Tragen Sie hier Zeit-Server ein, von denen sich das Gerät mit der aktuellen Uhrzeit versorgen kann.

**SNMP-ID:** 2.26.11

**Pfad Telnet:** /Setup/NTP

### 2.26.11.1 RQ-Addresse

Geben Sie hier die Zeit-Server (NTP) in der Reihenfolge an, in der Sie diese abfragen möchten. Die Server sollten über eines der vorhandenen Interfaces erreichbar sein. Vorsicht: Zum Erreichen der Zeit-Server wird bei Bedarf eine Verbindung aufgebaut. Bitte bedenken Sie, dass hierdurch zusätzliche Kosten entstehen können.

**SNMP-ID:** 2.26.11.1

**Pfad Telnet:** /Setup/NTP/RQ-Adresse

**Mögliche Werte:**

- max. 31 Zeichen

**Default:** leer

### 2.26.11.2 Loopback-Addr.

Hier können Sie optional eine Absenderadresse konfigurieren, die statt der ansonsten automatisch fiir die Zieladresse gewählten Absenderadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absenderadresse angeben.

Als Adresse werden verschiedene Eingabeformen akzeptiert:

• Name der IP-Netzwerke, deren Adresse eingesetzt werden soll.

• "INT" fiir die Adresse des ersten Intranets.

• "DMZ" fiir die Adresse der ersten DMZ (Achtung: wenn es eine Schnittstelle Namens "DMZ" gibt, dann wird deren Adresse genommen).

• LBO... LBF für die 16 Loopback-Adressen.

• Desweiteren kann eine beliebige IP-Adresse in der Form x.x.x.x angegeben werden.

**SNMP-ID:** 2.26.11.2

**Pfad Telnet:** /Setup/NTP/RQ-Adresse

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

**Default:** leer

Wenn es eine Schnittstelle namens "DMZ" gibt, dann wir diese Adresse genommen.

## 2.27 Mail

Dieses Menü enthält die Einstellungen für E-Mail.

**SNMP-ID:** 2.27

**Pfad Telnet:** /Setup

### 2.27.5 Benutzername

Geben Sie hier den Benutzername an, welcher benutzt wird um E-Mail-Benachrichtigungen an den o.a. SMTP-Server zu verschicken.

**SNMP-ID:** 2.27.5

**Pfad Telnet:** /Setup/Mail

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** leer

## 2.27.7 E-Mail-Absender

Geben sie hier eine gültige Absender-E-Mail-Adresse an, welche Ihr Gerät als Absender-Adresse benutzt, um E-Mail-Benachrichtigungen zu verschicken. An diese Adresse werden von den beteiligten SMTP-Servern Zustellprobleme gemeldet, wenn die Empfänger- E-Mail- Adresse vorübergehend nicht erreichbar sein sollte. Außerdem wird die Absender-E-Mail-Adresse von einigen Servern auf Gültigkeit überprüft und eine Zustellung verweigert, falls sie fehlt, eine ungültige Domain enthält oder eine ungültige E-Mail-Adresse ist.

**SNMP-ID:** 2.27.7

**Pfad Telnet:** /Setup/Mail

**Mögliche Werte:**

- max. 63 Zeichen

**Default:** leer

## 2.27.11 Loopback-Addr.

Hier können Sie optional eine Absenderadresse konfigurieren, die statt der ansonsten automatisch fiir die Zieladresse gewählten Absenderadresse verwendet wird. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absenderadresse angeben.

**SNMP-ID:** 2.27.11

**Pfad Telnet:** /Setup/Mail

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

**Default:** leer

Wenn es eine Schnittstelle namens "DMZ" gibt, dann wird deren Name genommen.

## 2.27.6 Passwort

Geben Sie hier das Passwort an, welches benutzt wird, um E-Mail-Benachrichtigungen an den angegebenen SMTP-Server zu verschicken.

**SNMP-ID:** 2.27.6

**Pfad Telnet:** /Setup/Mail

**Mögliche Werte:**

- max. 31 Zeichen

**Default:** leer

## 2.27.4 POP3-Port

Geben sie hier die Nummer des POP3-Ports des o. a. Servers fiir unverschlüsselte Mail an. Standardmäßig hat dieser die Nummer 110.

**SNMP-ID:** 2.27.4

**Pfad Telnet:** /Setup/Mail

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 110

## 2.27.3 POP3-Server

Bei vielen P0P3-Servern, die eine SMTP-nach-POP-Anmeldung erfordern, unterscheidet sich der POP3-Servername lediglich im gleichnamigen Präfix vom SMTP-Servernamen. Sie brauchen dann hier nur den Namen Ihres SMTP-Servers anzugeben und das darin befindliche 'SMTP' durch 'POP' oder "POP3" zu ersetzen.

**SNMP-ID:** 2.27.3

**Pfad Telnet:** /Setup/Mail

**Mögliche Werte:**

- max. 31 Zeichen

**Default:** leer

## 2.27.10 Pufferanzahl

Bei Verbindungsproblemen zum SMTP-Server werden die Nachrichten gepuffert und es wird wiederholt versucht, diese zuzustellen. Das gilt auch für Nachrichten, die aufgrund von fehlenden Einstellungen (z. B. SMTP-Daten hier oder Empfänger-E-Mail in den Mail erzeugenden Modulen) nicht zustellbar sind. Stellen Sie die maximale Anzahl gepufferter Nachrichten ein. Ist der eingestellte Puffer voll und es trifft eine weitere Nachricht ein, so wird die jeweils älteste Nachricht verworfen.

**SNMP-ID:** 2.27.10

**Pfad Telnet:** /Setup/Mail

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 100

## 2.27.8 Sendewiederholung-(Min)

Bei Verbindungsproblemen zum SMTP-Server werden die Nachrichten gepuffert und es wird wiederholt versucht, diese zuzustellen. Das gilt auch für Nachrichten, die aufgrund von fehlenden Einstellungen (z. B. SMTP-Daten hier oder Empfänger-E-Mail in den Mail erzeugenden Modulen) nicht zustellbar sind. Stellen Sie die Zeit ein, nach der erneut versucht wird, alle gepufferten Nachrichten zuzustellen - Außerdem wird eine Zustellung aller gepufferten Nachrichten bei jedem Eintreffen einer neuen Nachricht versucht.

**SNMP-ID:** 2.27.8

**Pfad Telnet:** /Setup/Mail

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 30

## 2.27.2 Serverport

Geben sie hier die Nummer des SMTP-Ports des o. a. Servers fiir unverschlüsselte Mail an. Standardmäßig hat dieser die Nummer 25.

**SNMP-ID:** 2.27.2

**Pfad Telnet:** /Setup/Mail

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 25

## 2.27.1 SMTP-Server

Geben sie hier den Namen oder die IP-Adresse eines für Sie erreichbaren SMTP-Servers an. Diese Angabe ist erforderlich, wenn Ihr Gerät Sie über bestimmte auswählbare Ereignisse per E-Mail benachrichtigen soll.

**SNMP-ID:** 2.27.1

**Pfad Telnet:** /Setup/Mail

**Mögliche Werte:**

- max. 31 Zeichen

**Default:** leer

Zum Versenden von E-Mail-Benachrichtigungen wird bei Bedarf eine Verbindung aufgebaut. Bitte bedenken Sie, dass hierdurch zusätzliche Kosten entstehen können.

## 2.27.9 Vorhaltezeit-(Std)

Bei Verbindungsproblemen zum SMTP-Server werden die Nachrichten gepuffert und es wird wiederholt versucht, diese zuzustellen. Das gilt auch für Nachrichten, die aufgrund von fehlenden Einstellungen (z. B. SMTP-Daten hier oder Empfänger-E-Mail in den Mail erzeugenden Modulen) nicht zustellbar sind. Stellen Sie die maximale Haltezeit einer Nachricht ein. Nach Ablauf der angegebenen Zeit wird nicht mehr versucht eine bestimmte Nachricht zuzustellen.

**SNMP-ID:** 2.27.9

**Pfad Telnet:** /Setup/Mail

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 72

# 2.30 IEEE802.1x

Dieses Menü enthält die Einstellungen des IEEE802.1x-Protokolls.

**SNMP-ID:** 2.30

**Pfad Telnet:** /Setup

## 2.30.3 Radius-Server

Sie können die Authentifizierung aller Wireless-LAN-Netze in einem zentralen RADIUS-Server verwalten (Name ist DEFAULT). Sie können darüber hinaus für bestimmte Wireless-LAN-Netze eigene RADIUS-Server definieren (anstelle der Passphrase für das logische Wireless-LAN-Netz anzugeben). Für jeden RADIUS-Server kann hier außerdem ein Backup-Server spezifiziert werden.

**SNMP-ID:** 2.30.3

**Pfad Telnet:** /Setup/IEEE802.1x

### 2.30.3.1 Name

Name des Servers.

**SNMP-ID:** 2.30.3.1

**Pfad Telnet:** /Setup/IEEE802.1x /RADIUS-Server

**Mögliche Werte:**

- max. 16 Zeichen

**Default:** leer

### 2.30.3.2 IP-Addresse

IP-Adresse des RADIUS-Servers. Der Name 'DEFAULT' ist reserviert für alle WLAN Netze die eine Authentifizierung über IEEE 802.1x nutzen und die keinen RADIUS-Server definiert haben. Jedes WLAN, das eine Authentifizierung über IEEE 802.1x verwendet, kann den eigenen RADIUS-Server durch die Anmgabe des entsprechenden Wertes in 'Schlüssel1/Passphrase' nutzen.

**SNMP-ID:** 2.30.3.2

**Pfad Telnet:** /Setup/IEEE802.1x /RADIUS-Server

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.30.3.3 Port

Port des RADIUS-Servers.

**SNMP-ID:** 2.30.3.3

**Pfad Telnet:** /Setup/IEEE802.1x /RADIUS-Server

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

### 2.30.3.4 Schlüssel

Schlüssel des RADIUS-Servers.

**SNMP-ID:** 2.30.3.4

**Pfad Telnet:** /Setup/IEEE802.1x /RADIUS-Server

**Mögliche Werte:**

- max. 32 Zeichen

**Default:** leer

### 2.30.3.5 Backup

Es besteht die Möglichkeit für jeden RADIUS-Server den Namen eines Backup-Servers anzugeben, welcher nur kontaktiert wird, wenn der hiesige Server nicht mehr erreicht werden kann. Den Namen des Backup-Servers können Sie aus derselben Tabelle wählen.

**SNMP-ID:** 2.30.3.5

**Pfad Telnet:** /Setup/IEEE802.1x /RADIUS-Server

**Mögliche Werte:**

- max. 24 Zeichen

**Default:** leer

### 2.30.3.6 Loopback-Addr.

Hier können Sie optional eine Absenderadresse konfigurieren, die statt der ansonsten automatisch fiir die Zieladresse gewählten Absenderadresse verwendet wird. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absenderadresse angeben.

**SNMP-ID:** 2.30.3.6

**Pfad Telnet:** /Setup/IEEE802.1x /RADIUS-Server

**Mögliche Werte:**

- Als Adresse werden verschiedene Eingabeformen akzeptiert:
- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll.
- "INT" für die Adresse des ersten Intranets.
- "DMZ" für die Adresse der ersten DMZ

Wenn es eine Schnittstelle Namens "DMZ" gibt, dann wird deren Adresse genommen.

- LBO... LBF für die 16 Loopback-Adressen.
- Desweiteren kann eine beliebige IP-Adresse in der Form x.x.x.x angegeben werden.

**Default:** leer

### 2.30.3.7 Protokoll

Protokoll für die Kommunikation zwischen dem internen RADIUS-Server und dem Weiterleitungs-Server.

**SNMP-ID:** 2.30.3.7

**Pfad Telnet:** /Setup/IEEE802.1x/RADIUS-Server/Protokoll

**Mögliche Werte:**

- RADSEC
- RADIUS

**Default:** RADIUS

## 2.30.4 Ports

Geben Sie für jedes lokale Netzwerk-Interface gesondert die Anmeldungseinstellungen an.

**SNMP-ID:** 2.30.4

**Pfad Telnet:** /Setup/IEEE802.1x

### 2.30.4.10 Re-Authentication

Hier aktivieren Sie die regelmäßige Neuanmeldung. Wird eine Neuanmeldung gestartet, so bleibt der Benutzer während der Verhandlung weiterhin angemeldet. Ein typischer Standardwert fiir das Neuanmelde-Intervall ist 3.600 Sekunden.

**SNMP-ID:** 2.30.4.10

**Pfad Telnet:** /Setup/IEEE802.1x /Ports

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

### 2.30.4.11 Re-Auth-Interval

Ein typischer Standardwert für das Neuanmelde-Intervall ist 3.600 Sekunden.

**SNMP-ID:** 2.30.4.11

**Pfad Telnet:** /Setup/IEEE802.1x /Ports

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 3600

### 2.30.4.12 Key-Transmission

Hier aktivieren Sie die regelmäßige Erzeugung dynamischer WEP-Schlüssel und deren Übertragung.

**SNMP-ID:** 2.30.4.12

**Pfad Telnet:** /Setup/IEEE802.1x /Ports

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

### 2.30.4.13 Key-Tx-Interval

Ein typischer Standardwert für das Schlüssel-Intervall ist 900 Sekunden.

**SNMP-ID:** 2.30.4.13

**Pfad Telnet:** /Setup/IEEE802.1x /Ports

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 900

### 2.30.4.2 Port

Schnittstelle des Gerätes, auf die sich dieser Eintrag bezieht.

**SNMP-ID:** 2.30.4.2

**Pfad Telnet:** /Setup/IEEE802.1x /Ports

**Mögliche Werte:**

- Alle im Gerät verfügbaren Schnittstellen.

**Default:** leer

### 2.30.4.4 Re-Auth-Max

Bei diesem Parameter handelt es sich um einen Timer der Authentication State Machine für IEEE 802.1x.

**SNMP-ID:** 2.30.4.4

**Pfad Telnet:** /Setup/IEEE802.1x /Ports

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 3

Die Änderungen dieser Parameter erfordert eine tiefgehende Kenntnis des Standards IEEE 802.1x. Nehmen Sie hier nur dann Änderungen vor, wenn die Systemkonfiguration das unbedingt erfordert.

### 2.30.4.5 Max-Req

Bei diesem Parameter handelt es sich um einen Timer der Authentication State Machine für IEEE 802.1x.

**SNMP-ID:** 2.30.4.5

**Pfad Telnet:** /Setup/IEEE802.1x /Ports

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 3

Die Änderungen dieser Parameter erfordert eine tiefgehende Kenntnis des Standards IEEE 802.1x. Nehmen Sie hier nur dann Änderungen vor, wenn die Systemkonfiguration das unbedingt erfordert.

### 2.30.4.6 Tx-Period

Bei diesem Parameter handelt es sich um einen Timer der Authentication State Machine für IEEE 802.1x.

**SNMP-ID:** 2.30.4.6

**Pfad Telnet:** /Setup/IEEE802.1x /Ports

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 30

Die Änderungen dieser Parameter erfordert eine tiefgehende Kenntnis des Standards IEEE 802.1x. Nehmen Sie hier nur dann Änderungen vor, wenn die Systemkonfiguration das unbedingt erfordert.

### 2.30.4.7 Supp-Timeout

Bei diesem Parameter handelt es sich um einen Timer der Authentication State Machine für IEEE 802.1x.

**SNMP-ID:** 2.30.4.7

**Pfad Telnet:** /Setup/IEEE802.1x /Ports

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 30

Die Änderungen dieser Parameter erfordert eine tiefgehende Kenntnis des Standards IEEE 802.1x. Nehmen Sie hier nur dann Änderungen vor, wenn die Systemkonfiguration das unbedingt erfordert.

### 2.30.4.8 Server-Timeout

Bei diesem Parameter handelt es sich um einen Timer der Authentication State Machine für IEEE 802.1x.

**SNMP-ID:** 2.30.4.8

**Pfad Telnet:** /Setup/IEEE802.1x /Ports

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 30

Die Änderungen dieser Parameter erfordert eine tiefgehende Kenntnis des Standards IEEE 802.1x. Nehmen Sie hier nur dann Änderungen vor, wenn die Systemkonfiguration das unbedingt erfordert.

### 2.30.4.9 Quiet-Period

Bei diesem Parameter handelt es sich um einen Timer der Authentication State Machine für IEEE 802.1x.

**SNMP-ID:** 2.30.4.9

**Pfad Telnet:** /Setup/IEEE802.1x /Ports

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 60

Die Änderungen dieser Parameter erfordert eine tiefgehende Kenntnis des Standards IEEE 802.1x. Nehmen Sie hier nur dann Änderungen vor, wenn die Systemkonfiguration das unbedingt erfordert.

## 2.31 PPPoE

Dieses Menü enthält die Einstellungen für PPPoE.

**SNMP-ID:** 2.31

**Pfad Telnet:** /Setup

## 2.31.1 Aktiv

Mit diesem Schalter wird der PPPoE-Server ein- bzw. ausgeschaltet.

**SNMP-ID:** 2.31.1

**Pfad Telnet:** /Setup/PPPoE-Server

**Mögliche Werte:**

- Ja
- Nein

## 2.31.3 Service

Unter 'Service' wird der Name des angebotenen Dienstes eingetragen. Das ermöglicht einem PPPoEClient die Auswahl eines bestimmten PPPoE-Servers, der dazu beim Client eingetragen wird.

**SNMP-ID:** 2.31.3

**Pfad Telnet:** /Setup/PPPoE-Server

**Mögliche Werte:**

- max. 32 Zeichen

**Default:** Leer

## 2.31.4 Session-Limit

Das 'Session-Limit' gibt an, wie oft ein Client mit der gleichen MAC-Adresse gleichzeitig angemeldet sein kann. Ist das Limit erreicht, dann antwortet der Server nicht mehr auf empfangene Anfragen des Clients. Defaultwert ist '1', max.wert '99'. Ein Session-Limit von '0' steht für eine unbegrenzte Session-Anzahl.

**SNMP-ID:** 2.31.4

**Pfad Telnet:** /Setup/PPPoE-Server

**Mögliche Werte:**

- 0 bis 99

**Default:** 1

**Besondere Werte:** 0: schaltet die Begrenzung der Sessions aus.

## 2.31.2 Namenliste

Definieren Sie in der Gegenstellen-Liste diejenigen Clients, welchen vom PPPoE-Server Zugang erlaubt und in der PPP-Liste oder der Firewall weitere Eigenschaften und Rechte zugeteilt werden sollen.

**SNMP-ID:** 2.31.2

**Pfad Telnet:** /Setup/PPPoE-Server

### 2.31.2.1 Gegenstelle

Definieren Sie hier einen Gegenstellen-Namen für jeden Client. Der Gegenstellen-Name muss beim Client als PPP-Benutzername verwendet werden.

**SNMP-ID:** 2.31.2.1

**Pfad Telnet:** /Setup/PPPoE-Server/Namenliste

**Mögliche Werte:**

- Auswahl aus der Liste der definierten Gegenstellen

**Default:** Leer

### 2.31.2.2 SH-Zeit

Definieren Sie hier die Haltezeit für die PPPoE-Verbindung an.

**SNMP-ID:** 2.31.2.2

**Pfad Telnet:** /Setup/PPPoE-Server/Namenliste

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

### 2.31.2.3 MAC-Adresse

Ist eine MAC-Adresse eingetragen, so wird die PPP-Verhandlung abgebrochen, wenn sich der Client von einer anderen MAC-Adresse anmeldet.

**SNMP-ID:** 2.31.2.3

**Pfad Telnet:** /Setup/PPPoE-Server/Namenliste

**Mögliche Werte:**

- max. 12 Zeichen

**Default:** 000000000000

## 2.31.5 Ports

Hier können Sie für einzelne Ports festlegen, ob der PPPoE Server Aktiviert ist.

**SNMP-ID:** 2.31.5

**Pfad Telnet:** /Setup/PPPoE-Server

### 2.31.5.2 Port

Port, für den der PPPoE-Server aktiviert oder deaktiviert werden soll.

**SNMP-ID:** 2.31.5.2

**Pfad Telnet:** /Setup/PPPoE-Server/Ports

**Mögliche Werte:**

- Auswahl aus der Liste der im Gerät verfügbaren Ports.

### 2.31.5.3 PPPoE-Aktiv

Aktiviert oder deaktiviert den PPPoE-Server für den gewählten Port.

**SNMP-ID:** 2.31.5.3

**Pfad Telnet:** /Setup/PPPoE-Server/Ports

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

# 2.32 VLAN

Die Konfiguration im VLAN-Bereich der Geräte hat zwei wichtige Aufgaben:

- Virtuelle LANs definieren und ihnen dabei einen Namen, eine VLAN-ID und die zugehörigen Interfaces zuordnen
- Für die Interfaces definieren, wie mit Datenpaketen mit bzw. ohne VLAN-Tags verfahren werden soll

**SNMP-ID:** 2.32

**Pfad Telnet:** /Setup

## 2.32.4 Aktiv

Schalten Sie das VLAN-Modul nur ein, wenn Sie mit den Auswirkungen der VLAN-Nutzung vertraut sind.

**SNMP-ID:** 2.32.4

**Pfad Telnet:** /Setup/VLAN

**Mögliche Werte:**

- ja
- nein

**Default:** nein

Mit fehlerhaften VLAN-Einstellungen können Sie den Konfigurationszugang zum Gerät verhindern.

## 2.32.5 Tag-Wert

Beim Übertragen von VLAN-getaggten Netzen über Netze der Provider, die ihrerseits VLAN verwenden, setzen die Provider teilweise spezielle VLAN-Tagging-IDs ein. Um die VLAN-Übertragung darauf einzustellen, kann der Ethernet2-Typ des VLAN-Tags als 'Tag-Value' als 16 Bit-Hexadezimalwert eingestellt werden. Default ist '8100' (VLAN-Tagging nach 802.1p/q), andere gängige Werte für VLAN-Tagging wären z. B. '9100' oder '9901'.

**SNMP-ID:** 2.32.5

**Pfad Telnet:** /Setup/VLAN

**Mögliche Werte:**

- max. 4 Zeichen

**Default:** 8100

## 2.32.1 Netzwerke

Die Netzwerkliste beinhaltet den Namen des VLANs, die VLAN-ID und die Ports. Zur Bearbeitung können Sie auf einen Eintrag klicken.

**SNMP-ID:** 2.32.1

**Pfad Telnet:** /Setup/VLAN

### 2.32.1.1 Name

Der Name des VLANs dient nur der Beschreibung bei der Konfiguration. Dieser Name wird an keiner anderen Stelle verwendet.

**SNMP-ID:** 2.32.1.1

**Pfad Telnet:** /Setup/VLAN/Netzwerke

### 2.32.1.2 VLAN-ID

Diese Nummer kennzeichnet das VLAN eindeutig.

**SNMP-ID:** 2.32.1.2

**Pfad Telnet:** /Setup/VLAN/Netzwerke

**Mögliche Werte:**

- 0 bis 4096

**Default:** 0

### 2.32.1.4 Ports

Tragen Sie hier Interfaces des Geräts ein, die zu dem VLAN gehören. Für ein Gerät mit einem LAN-Interface und einem WLAN-Port können z. B. die Ports "LAN-1" und "WLAN-1" eingetragen werden. Bei Portbereichen werden die einzelnen Ports durch eine Tilde getrennt: "P2P-1~P2P-4".

**SNMP-ID:** 2.32.1.4

**Pfad Telnet:** /Setup/VLAN/Netzwerke

**Mögliche Werte:**

- max. 251 Zeichen

**Default:** leer

Die erste SSID des ersten WLAN-Moduls heißt WLAN-1, die weiteren SSID WLAN-1-2 bis WLAN-1-8. Falls das Gerät über zwei WLAN-Module verfügt, heißen die SSIDs hier WLAN-2, WLAN-2-2 bis WLAN-2-8.

## 2.32.2 Port-Tabelle

In der Porttabelle werden die einzelnen Ports des Gerätes für die Verwendung im VLAN konfiguriert. Die Tabelle hat einen Eintrag für jeden Port des Gerätes.

**SNMP-ID:** 2.32.2

**Pfad Telnet:** /Setup/VLAN

### 2.32.2.1 Port

Der Name des Ports; nicht editierbar.

**SNMP-ID:** 2.32.2.1

**Pfad Telnet:** /Setup/VLAN/Port-Tabelle

### 2.32.2.4 Alle-VLANs-zulassen

Diese Option gibt an, ob getaggte Datenpakete mit beliebigen VLAN-IDs akzeptiert werden sollen, auch wenn der Port nicht Mitglied dieses VLANs ist.

**SNMP-ID:** 2.32.2.4

**Pfad Telnet:** /Setup/VLAN/Port-Tabelle

**Mögliche Werte:**

- ja
- nein

**Default:** ja

### 2.32.2.5 Port-VLAN-Id

Diese Port-ID hat zwei Funktionen:

- Ungetaggte Pakete, die auf diesem Port im Modus 'Gemischt' oder 'ankommend gemischt' empfangen werden, werden diesem VLAN zugeordnet, ebenso sämtliche ankommenden Pakete im Modus 'Niemals'.
- Im Modus 'Gemischt' entscheidet dieser Wert darüber , ob ausgehende Pakete ein VLAN-Tag erhalten oder nicht: Pakete, die dem für diesen Port definierten VLAN zugeordnet wurden, erhalten kein VLAN-Tag, alle anderen erhalten ein VLAN-Tag.

**SNMP-ID:** 2.32.2.5

**Pfad Telnet:** /Setup/VLAN/Port-Tabelle

**Mögliche Werte:**

- max. 4 Zeichen

**Default:** 1

### 2.32.2.6 Tagging-Modus

Steuert die Verarbeitung und Zuweisung von VLAN-Tags auf diesem Port.

**SNMP-ID:** 2.32.2.6

**Pfad Telnet:** /Setup/VLAN/Port-Tabelle

**Mögliche Werte:**

- **Nie**: Ausgehende Pakete erhalten auf diesem Port kein VLAN-Tag. Eingehende Pakete werde so behandelt, als hätten Sie kein VLAN-Tag. Haben die eingehenden Pakete ein VLAN-Tag, so wird es ignoriert und so behandelt, als ob es zur Payload des Paketes gehört. Eingehende Pakete werden immer dem für diesen Port definierten VLAN zugewiesen.
- **Immer:** Ausgehende Pakete erhalten auf diesem Port immer ein VLAN-Tag, egal ob sie dem für diesen Port definierten VLAN angehören oder nicht. Eingehende Pakete müssen über ein VLAN-Tag verfügen, anderenfalls werden sie verworfen.
- **Gemischt:** Erlaubt einen gemischten Betrieb von Paketen mit und ohne VLAN-Tags auf dem Port. Pakete ohne VLAN-Tag werden dem für diesen Port definierten VLAN zugeordnet. Ausgehende Pakete erhalten ein VLANTag, außer sie gehören dem für diesen Port definierten VLAN an.
- **Ingress-Gemischt:** Ankommende Pakete können ein VLAN-Tag haben oder nicht, ausgehende Pakete bekommen nie ein VLAN-Tag.

**Default:** Ingress-Gemischt

## 2.33 Voice-Call-Manager

Dieses Menü enthält die Einstellungen für den Voice-Call-Manager.

**SNMP-ID:** 2.33

**Pfad Telnet:** /Setup

## 2.33.1 Operating

Schaltet den Voice-Call-Manager ein/aus.

**Pfad Telnet:**/Setup/Voice-Call-Manager

**Mögliche Werte Telnet:**

- ja
- nein

**Default:** nein

## 2.33.2 General

Dieses Menü enthält die allgemeinen Einstellungen für den Voice-Call-Manager.

**SNMP-ID:** 2.33.2

**Pfad Telnet:** /Setup/Voice-Call-Manager

### 2.33.2.10 Analog-Gateway-Codecs

Mit dem Codec-Filter können Sie die erlaubten Codecs für Analog-Endgeräte einschränken und nur bestimmte Codecs zulassen.

**SNMP-ID:** 2.33.2.10

**Pfad Telnet:** /Setup/Voice-Call-Manager/General

**Mögliche Werte Telnet:**

- Hexadezimalwert zur Darstellung der erlaubten Codecs.

**Default:** Alle verfügbaren Codecs

### 2.33.2.11 ClnPartyNumType

Hiermit wird der Typ der abgehenden Rufnummer (CallingPartyNumber) auf einem ISDN-Interface für rausgehende Rufe eingestellt. Dies ist für TK-Anlagen und manche Vermittlungsstellen im Ausland nötig, da diese einem bestimmten Typ benötigen.

**SNMP-ID:** 2.33.2.11

**Pfad Telnet:** /Setup/Voice-Call-Manager/General

**Mögliche Werte Telnet:**

- subscriber
- unknown
- national

**Default:** subscriber(0)

### 2.33.2.13 Convert-Canonicals

Aktivieren Sie hier die Konvertierung der kanonischen VoIP-Namen.

**SNMP-ID:** 2.33.2.13

**Pfad Telnet:** /Setup/Voice-Call-Manager/General/Convert-Canonicals

**Mögliche Werte Telnet:**

- ja
- nein

**Default:** ja

### 2.33.2.9 Country

Das Land definiert die im LANCOM erzeugten Inband-Töne.

**SNMP-ID:** 2.33.2.9

**Pfad Telnet:** /Setup/Voice-Call-Manager/General

**Mögliche Werte Telnet:**

- Unbekannt
- Österreich
- Belgien
- Schweiz
- Deutschland
- Frankreich
- Italien
- Niederlande
- Spanien
- Groß-Britannien

**Default:** Unbekannt

### 2.33.2.1 Domain

Name der Domain, in der die angeschlossenen Telefone und der LANCOM VoIP Router betrieben werden.

Endgeräte, die mit der gleichen Domain arbeiten, melden sich als lokale Teilnehmer am LANCOM VoIP Router an und nutzen so den SIP-Proxy.

Endgeräte, die mit der anderen Domain einer aktiven SIP-PBX-Leitung arbeiten, melden sich als Teilnehmer an einer übergeordneten TK-Anlage an.

**SNMP-ID:** 2.33.2.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/General

**Mögliche Werte Telnet:**

- max. 63 Zeichen

**Default:** intern

### 2.33.2.4 Echo_Canceler

Aktiviert die Echounterdrückung des fernen Echos. Bei einem zu starkem Echo hört der Teilnehmer sich selber mit kurzer Verzögerung wieder. Mit der Aktivierung dieser Option wird das Echo am SIP-Gateway reduziert.

**SNMP-ID:** 2.33.2.4

**Pfad Telnet:** /Setup/Voice-Call-Manager/General

**Mögliche Werte Telnet:**

- Ein
- Aus

**Default:** Ein

### 2.33.2.6 Incoming-packet-reduction

Analog zu den abgehenden Datenpaketen wird hier die Behandlung der Nicht-VoIP-Datenpakete bei Bandbreitenreservierung für SIP-Daten eingestellt.

**SNMP-ID:** 2.33.2.6

**Pfad Telnet:** /Setup/Voice-Call-Manager/General

**Mögliche Werte Telnet:**

- Reduktion der PMTU: Die Teilnehmer der Datenverbindung werden informiert, dass sie nur Datenpakete bis zu einer bestimmen Länge versenden sollen (Path Maximum Transmission Unit, PMTU).
- Keine Veränderung: Die Länge der Datenpakete wird durch den VoIP-Betrieb nicht verändert.

**Default:** keine Veränderung

### 2.33.2.8 ISDN-Gateway-Codecs

Die beteiligten ISDN-Endgeräte handeln beim Verbindungsaufbau aus, welche Codecs für die Komprimierung der Sprachdaten verwendeten werden sollen. Mit dem Codec-Filter können Sie die erlaubten Codecs einschränken und nur bestimmte Codecs zulassen.

**SNMP-ID:** 2.33.2.8

**Pfad Telnet:** /Setup/Voice-Call-Manager/General

**Mögliche Werte Telnet:**

- Hexadezimalwert zur Darstellung der erlaubten Codecs.

**Default:** Alle verfügbaren Codecs.

### 2.33.2.3 Local-authentication

Normalerweise akzeptiert der SIP-Proxy Anmeldung von allen SIP-Benutzern, die sich mit einer gültigen Domain anmelden. Wird die lokale Authentifizierung erzwungen, können sich nur solche Teilnehmer beim SIP-Proxy anmelden, die in einer der Benutzertabellen mit den entsprechenden Zugangsdaten hinterlegt sind.

**SNMP-ID:** 2.33.2.3

**Pfad Telnet:** /Setup/Voice-Call-Manager/General

**Mögliche Werte Telnet:**

- nein
- ja

**Default:** nein/Aus

Die automatische Anmeldung ohne Eintrag eines Passworts ist auf die SIP-Benutzer im LAN beschränkt. SIP-Benutzer aus dem WAN und ISDN-Benutzer müssen immer über einen entsprechenden Benutzer-Eintrag mit Passwort authentifiziert werden.

### 2.33.2.18 Login-Fehler

Dieser Wert gibt an, nach welcher Anzahl von Fehlversuchen ein SIP-Benutzer für eine bestimmte Zeit gesperrt wird.

**SNMP-ID:**

2.33.2.18

**Pfad Telnet:**

**Setup** > **Voice-Call-Manager** > **Allgemein** > **Login-Fehler**

**Mögliche Werte:**

0 bis 255

**Besondere Werte:**

0: Die erste Falschanmeldung löst die Sperre aus.

**Default:**

5

### 2.33.2.5 Outgoing-packet-reduction

Für alle SIP-Gespräche wird abhängig vom verwendeten Audio-Codec eine ausreichende Bandbreite über die Firewall reserviert (soweit die verfügbare Bandbreite ausreicht). Stellen Sie hier zur Steuerung der Firewall die Behandlung der restlichen Datenpakete ein, die nicht zu den SIP-Datenströmen gehören.

**SNMP-ID:** 2.33.2.5

**Pfad Telnet:** /Setup/Voice-Call-Manager/General

**Mögliche Werte Telnet:**

- PMTU: Die Teilnehmer der Datenverbindung werden informiert, dass sie nur Datenpakete bis zu einer bestimmen Länge versenden sollen (Path Maximum Transmission Unit, PMTU).
- Fragmentation: Der LANCOM VoIP Router reduziert selbst die Datenpakete durch Fragmentierung auf die gewünschte Länge.
- NONE: Die Länge der Datenpakete wird durch den VoIP-Betrieb nicht verändert.
- PMTU + Fragmentation

**Default:** NONE/Reduktion der PMTU

### 2.33.2.2 Overlap-Timeout

Für diese Zeit in Sekunden wird bei der Wahl von einem ISDN-Telefon gewartet, bis die Rufnummer als vollständig angesehen wird und an den Call-Router übergeben wird.

**SNMP-ID:** 2.33.2.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/General

**Mögliche Werte Telnet:**

- 0 bis 99

**Default:** 6

**Besondere Werte:** 0: Bei einer Wählverzögerung von '0' muss die Eingabe der Rufnummer mit einem '#' abgeschlossen werden. Die Eingabe des Zeichens '#' nach der Rufnummer verkürzt die Wählverzögeung manuell.

### 2.33.2.7 Reduced-packet-size

Dieser Parameter gibt die Paketgröße in Byte an, die für die PMTU-Anpassung bzw. die Fragmentierung bei Bevorzugung der SIP-Daten verwendet werden soll.

**SNMP-ID:** 2.33.2.7

**Pfad Telnet:** /Setup/Voice-Call-Manager/General

**Mögliche Werte Telnet:**

- 0 bis 9999

**Default:** 576

### 2.33.2.12 Register-Time

Dieser Wert gibt die Re-Registrierungszeit in Sekunden an, die einem SIP-Benutzer auf der lokalen Seite signalisiert wird.

Mit dieser Funktion erreicht der Registrar eine Registrierung durch den VoIP-Client in kürzeren Zeitabständen, um so z. B. das Ausschalten des VoIP-Clients schneller zu erkennen.

**SNMP-ID:** 2.33.2.12

**Pfad Telnet:** /Setup/Voice-Call-Manager/General

**Mögliche Werte:**

- 60 bis 3600

**Default:** 120

### 2.33.2.16 RTP-DSCP

Legen Sie hier fest, mit welchen DiffServ-CodePoints (DSCP) die RTP-Pakete (Voice-Datenstrom) markiert werden.

**SNMP-ID:** 2.33.2.16

**Pfad Telnet:** /Setup/Voice-Call-Manager/General

**Mögliche Werte Telnet:**

BE, CS-0, CS-1, CS-2, CS-3, CS-4, CS-5, CS-6, CS-7, AF-11, AF-12, AF-13, AF-21, AF-22, AF-23, AF-31, AF-32, AF-33, AF-41, AF-42, AF-43, EF

BE/CS-0, CS-1, CS-2, CS-3, CS-4, CS-5, CS-6, CS-7, AF-11, AF-12, AF-13, AF-21, AF-22, AF-23, AF-31, AF-32, AF-33, AF-41, AF-42, AF-43, EF

**Default:** EF

Bei der Einstellung DSCP BE bzw. CS-0 werden die Pakete ohne Markierung versendet. Weitere Informationen zu den DiffServ-CodePoints finden Sie im Referenzhandbuch im Kapitel “QoS”.

### 2.33.2.15 SIP-DSCP

Legen Sie hier fest, mit welchen DiffServ-CodePoints (DSCP) die SIP-Pakete (Anruf-Signalisierung) markiert werden.

**SNMP-ID:** 2.33.2.15

**Pfad Telnet:** /Setup/Voice-Call-Manager/General

**Mögliche Werte Telnet:**

BE, CS-0, CS-1, CS-2, CS-3, CS-4, CS-5, CS-6, CS-7, AF-11, AF-12, AF-13, AF-21, AF-22, AF-23, AF-31, AF-32, AF-33, AF-41, AF-42, AF-43, EF

BE/CS-0, CS-1, CS-2, CS-3, CS-4, CS-5, CS-6, CS-7, AF-11, AF-12, AF-13, AF-21, AF-22, AF-23, AF-31, AF-32, AF-33, AF-41, AF-42, AF-43, EF

**Default:** CS-1

Die Verwendung von CS-1 ist heute überholt und zur Erhaltung der Abwärts-Kompatibilität als Default gesetzt. Typische Werte für aktuellen VoIP-Installationen sind CS-3, AF-31 oder AF-41. Wegen großer Verbreitung im Markt empfehlen wir den Einsatz von CS-3.

### 2.33.2.17 Sperr-Minuten

Bestimmen Sie, für wieviele Minuten ein SIP-Benutzer gesperrt wird, nachdem die Anmeldung aufgrund falscher Login-Daten fehlgeschlagen ist.

**SNMP-ID:**

2.33.2.17

**Pfad Telnet:**

**Setup** > **Voice-Call-Manager** > **Allgemein** > **Sperr-Minuten**

**Mögliche Werte:**

0 bis 255 Minuten

**Besondere Werte:**

0: Sperre deaktiviert

**Default:**

5 Minuten

### 2.33.2.14 Symmetrisch-RTP

Dieser Parameter schaltet die strenge Prüfung des RTP-Absenders ab. In der Regel findet eine bidirektionale RTP-Kommunikationen zwischen zwei Socket-Adressen (IP:Port) statt; d.h. die Media-Datenquellen (ausgehend) sind gleichzeitig auch Media-Datensenken (eingehend). Der Datenfluss ist symmetrisch.

Es gibt allerdings auch Media-Server, deren Implementierungen hiervon abweichen und die RTP-Quelle und das RTP-Ziel nicht die gleiche Socket-Adresse aufweisen. Deaktivieren Sie in solchen Fällen die Option "Symmetrisch-RTP".

**Pfad Telnet:** /Setup/Voice-Call-Manager/General/Symmetrisch-RTP

**Mögliche Werte:**

- ja
- nein

**Default:** ja

## 2.33.3 Users

Dieses Menü enthält die Benutzer-Einstellungen für den Voice-Call-Manager.

**SNMP-ID:** 2.33.3

**Pfad Telnet:** /Setup/Voice-Call-Manager

### 2.33.3.1 SIP-User

Dieses Menü enthält die SIP-Benutzer-Einstellungen für den Voice-Call-Manager.

**SNMP-ID:** 2.33.3.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/User

#### 2.33.3.1.3 Extern-Cln-Prefix

Dieses Präfix wird bei einem eingehenden, externen Anruf der vorhandenen Calling Party ID vorangestellt, wenn der Anruf an einen SIP-Benutzer gerichtet ist

**SNMP-ID:** 2.33.3.1.3

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/SIP-User

**Mögliche Werte Telnet:**

- max. 15 Ziffern oder *

**Default:** Leer

#### 2.33.3.1.2 Intern-Cln-Prefix

Dieses Präfix wird bei einem eingehenden, internen Anruf der vorhandenen Calling Party ID vorangestellt, wenn wenn der Anruf an einen SIP-Benutzer gerichtet ist.

**SNMP-ID:** 2.33.3.1.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/SIP-User

**Mögliche Werte Telnet:**

- max. 15 Ziffern oder *

**Default:** *

Ein Ruf gilt dann als extern, wenn er von einer „Leitung“ kommt. Wenn diese Leitung eine SIP-PBX Leitung ist, dann ist der Ruf nur dann extern, wenn die kommende Calling Party ID eine führende „0“ hat. Alle anderen Anruf gelten als intern.

#### 2.33.3.1.1 Users

Je nach Modell können unterschiedlich viele SIP-Benutzer angelegt werden. Mehr als die erlaubte Anzahl Benutzer können nicht angelegt werden, ebenso werden gleiche Namen oder gleiche Rufnummern nicht zugelassen.

**SNMP-ID:** 2.33.3.1.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/SIP-User

Die vom SIP-Teilnehmer verwendete Domäne wird üblicherweise im Endgerät selbst eingestellt.

##### 2.33.3.1.1.1 Number/Name

Telefonnummer des SIP-Telefons oder Name des Benutzers (SIP-URI).

**SNMP-ID:** 2.33.3.1.1.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/SIP-User/User

**Mögliche Werte Telnet:**

- max. 20 Zeichen

**Default:** Leer

##### 2.33.3.1.1.2 Auth-Name

Name zur Authentifizierung am SIP-Proxy, ggf. auch an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt. Der Name wird benötigt, wenn eine Anmeldung erforderlich ist (z. B. bei übergeordneter Anmeldung an einer SIP-TK-Anlage oder Setzen von "Lokale Authentifizierung erzwingen" für die SIP-Benutzer).

**SNMP-ID:** 2.33.3.1.1.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/SIP-User/Users

**Mögliche Werte Telnet:**

- max. 63 Zeichen

**Default:** Leer

**Besondere Werte:** Leer: Wenn hier nichts eingetragen ist, wird die Authentifizierung über den SIP-Namen (interne Rufnummer) versucht.

#### 2.33.3.1.1.3 Secret

Passwort zum Anmelden des SIP-Benutzers, ggf. auch an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt. Es ist möglich, dass sich Benutzer lokal am SIP-Proxy ohne Authentifizierung anmelden ("Lokale Authentifizierung erzwingen" für SIP-Benutzer ist deaktiviert) und ggf. an einer übergeordneten SIP-TK-Anlage mit einem gemeinsamen Passwort ("Standard-Passwort" an der SIP-PBX-Line) anmelden.

**SNMP-ID:** 2.33.3.1.1.3

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/SIP-User/Users

**Mögliche Werte Telnet:**

- max. 32 Zeichen

**Default:** Leer

#### 2.33.3.1.1.4 Active

Aktiviert oder deaktiviert den Eintrag.

**SNMP-ID:** 2.33.3.1.1.4

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/SIP-User/Users

**Mögliche Werte Telnet:**

- ja
- nein

**Default:** Ein

#### 2.33.3.1.1.5 Kommentar

Kommentar zu diesem Eintrag.

**SNMP-ID:** 2.33.3.1.1.5

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/SIP-User/Users

**Mögliche Werte Telnet:**

- max. 63 Zeichen

**Default:** Leer

#### 2.33.3.1.1.6 Device-Type

Typ des angeschlossenen Geräts.

Der Typ entscheidet, ob ggf. eine Umwandlung einer analogen Fax-Verbindung in SIP T.38 erfolgt. Bei Auswahl des Typs "Fax" oder "Telefon/Fax" wird eine Erkennung von Fax-Signalen aktiviert, die u.U. bei einem Telefon zu Beeinträchtigungen der Verbindungsqualität führen kann. Bitte wählen Sie daher den Typ entsprechend des angeschlossenen Gerätes, um die optimale Qualität zu erzielen.

**SNMP-ID:** 2.33.3.1.1.6

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/SIP-User/Users

**Mögliche Werte Telnet:**

- Phone
- Fax
- Auto

**Default:** Phone/Telefon

#### 2.33.3.1.1.7 CLIR

Schaltet die Übermittlung der Absenderinformationen ein oder aus.

**SNMP-ID:** 2.33.3.1.1.7

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/SIP-User/Users

**Mögliche Werte Telnet:**

- ja: Die Übermittlung der Absenderinformationen wird auf jeden Fall unterdrückt, unabhängig von den Einstellungen am Endgerät des Benutzers.
- nein: Die Übermittlung der Absenderinformationen wird nicht im Gerät unterdrückt, die Einstellungen am Endgerät des Benutzers entscheiden über Übermittlung der Absenderinformationen.

**Default:** nein/Aus

#### 2.33.3.1.1.8 Zugriff von WAN

Bestimmen Sie hier, ob und wie sich SIP-Clients über eine WAN-Verbindung mit dem entsprechenden Benutzerdaten anmelden können.

**SNMP-ID:**

2.33.3.1.1.8

**Pfad Telnet:**

**Setup** > **Voice-Call-Manager** > **User** > **SIP-User** > **User**

**Mögliche Werte:**

ja

nein

VPN

**Default:**

ja

### 2.33.3.2 ISDN-User

Dieses Menü enthält die ISDN-Benutzer-Einstellungen für den Voice-Call-Manager.

**SNMP-ID:** 2.33.3.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/User

#### 2.33.3.2.4 Extern-Cln-Prefix

Dieses Präfix wird bei einem eingehenden, externen Anruf der vorhandenen Calling Party ID vorangestellt, wenn der Anruf an einen ISDN-Benutzer gerichtet ist. Sofern ein Leitungspräfix definiert ist, wird dieses der gesamten Rufnummer vorangestellt.

**SNMP-ID:** 2.33.3.2.4

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/ISDN-User

**Mögliche Werte Telnet:**

- max. 15 Ziffern oder *.

**Default:** Leer

#### 2.33.3.2.1 Interfaces

Hier wählen Sie die Schnittstelle aus, an der ISDN-Benutzer angeschlossen werden.

**SNMP-ID:** 2.33.3.2.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/ISDN-User

#### 2.33.3.2.1.3 Active

Aktiviert oder deaktiviert den Eintrag.

**SNMP-ID:** 2.33.3.2.1.3

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/ISDN-User/Interfaces

**Mögliche Werte Telnet:**

- ja
- nein

**Default:** ja/Ein

#### 2.33.3.2.1.2 Ifc

Schnittstelle, an welche die ISDN-Teilnehmer angeschlossen sind.

**SNMP-ID:** 2.33.3.2.1.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/ISDN-User/Interfaces

**Mögliche Werte Telnet:**

- Auswahl aus verfügbaren ISDN-Schnittstellen, z. B. S0-1 und S0-2

**Default:** Je nach Modell verschieden.

#### 2.33.3.2.1.1 Name

Name der Schnittstelle

**SNMP-ID:** 2.33.3.2.1.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/ISDN-User/Interfaces

**Mögliche Werte Telnet:**

- ISDN

**Default:** ISDN

#### 2.33.3.2.1.4 Kommentar

Kommentar zu diesem Eintrag.

**SNMP-ID:** 2.33.3.2.1.4

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/ISDN-User/Interfaces

**Mögliche Werte Telnet:**

- max. 63 Zeichen

**Default:** Leer

#### 2.33.3.2.3 Intern-Cln-Prefix

Dieses Präfix wird bei einem eingehenden, internen Anruf der vorhandenen Calling Party ID vorangestellt, wenn der Anruf an einen ISDN-Benutzer gerichtet ist. Sofern ein Leitungspräfix definiert ist, wird dieses der gesamten Rufnummer vorangestellt.

**SNMP-ID:** 2.33.3.2.3

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/ISDN-User

**Mögliche Werte Telnet:**

- max. 15 Ziffern oder *.

**Default:** *

#### 2.33.3.2.5 Intern-Dial-Tone

Der Wählton bestimmt, welchen Ton ein Benutzer nach dem Abheben des Hörers hört. Der „interne Wählton" gleicht dem Ton, den ein Benutzer an einer TK-Anlage ohne spontane Amtsholung hört (drei kurze Töne gefolgt von einer Pause). Der „externe Wählton" gleicht folglich dem Ton, dass nach dem Abheben ein Amt anzeigt (anhaltender Ton ohne Unterbrechungen). Passen Sie den Wählton nach Bedarf an die Verwendung der spontanen Amtsholung an, um ein ähnliches Verhalten wie an einem externen Anschluss zu simulieren.

**SNMP-ID:** 2.33.3.2.5

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/ISDN-User

**Mögliche Werte Telnet:**

- Ja
- Nein

**Default:** Nein, es wird der externe Wählton verwendet

#### 2.33.3.2.2 Users

Hier können Sie alle lokalen ISDN-Benutzer (Endgeräte) definieren. Darüber hinaus können Sie Authentizifierungs-Daten zur SIP-Anmeldung angeben.

**SNMP-ID:** 2.33.3.2.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/ISDN-User

##### 2.33.3.2.2.1 Number/Name

Interne Rufnummer des ISDN-Telefons oder Name des Benutzers (SIP-URI).

**SNMP-ID:** 2.33.3.2.2.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/ISDN-User/User

**Mögliche Werte Telnet:**

- max. 20 Zeichen

**Default:** Leer

Mit dem #-Zeichen als Platzhalter können ganze Gruppen von Rufnummern z. B. bei der Verwendung von Durchwahlnummern an einem Anlagenanschluss in einem einzigen Eintrag erfaßt werden. Mit der Rufnummer '#' und der DDI '#' werden z. B. die Durchwahlnummern ohne Veränderung in interne Rufnummern umgesetzt. Mit der Rufnummer '3#' und der DDI '#' wird z. B. ein ankommender Ruf für die Durchwahl '55' an die interne Rufnummer '355' weitergeleitet, bei ausgehenden Rufen von der internen Rufnummer '377' wird die '77' als Durchwahl verwendet.

Benutzereinträge mit #-Zeichen zur Abbildung von Benutzergruppen können nicht für eine Anmeldung an einer übergeordneten TK-Anlage verwendet werden. Für diese Anmeldung ist immer ein spezifischer Eintrag für den einzelnen ISDN-Benutzer notwendig.

#### 2.33.3.2.2.10 Kommentar

Kommentar zu diesem Eintrag.

**SNMP-ID:** 2.33.3.2.2.10

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/ISDN-User/User

**Mögliche Werte Telnet:**

- max. 63 Zeichen

**Default:** Leer

#### 2.33.3.2.2.11 Device-Type

Typ des angeschlossenen Gerätes.

Der Typ entscheidet, ob ggf. eine Umwandlung einer analogen Fax-Verbindung in SIP T.38 erfolgt. Bei Auswahl des Typs "Fax" oder "Telefon/Fax" wird eine Erkennung von Fax-Signalen aktiviert, die u.U. bei einem Telefon zu Beeinträchtigungen der Verbindungsqualität führen kann. Bitte wählen Sie daher den Typ entsprechend des angeschlossenen Gerätes, um die optimale Qualität zu erzielen.

**SNMP-ID:** 2.33.3.2.2.11

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/ISDN-User/Users

**Mögliche Werte Telnet:**

- Phone
- Fax
- Auto

**Default:** Phone/Telefon

#### 2.33.3.2.2.12 CLIR

Schaltet die Übermittlung der Absenderinformationen ein oder aus.

**SNMP-ID:** 2.33.3.2.2.12

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/ISDN-User/Users

**Mögliche Werte Telnet:**

- ja: Die Übermittlung der Absenderinformationen wird auf jeden Fall unterdrückt, unabhängig von den Einstellungen am Endgerät des Benutzers.
- nein: Die Übermittlung der Absenderinformationen wird nicht im Gerät unterdrückt, die Einstellungen am Endgerät des Benutzers entscheiden über Übermittlung der Absenderinformationen.

**Default:** Nein/Aus

#### 2.33.3.2.2.2 Ifc

ISDN-Interface, das für den Verbindungsaufbau verwendet werden soll.

**SNMP-ID:** 2.33.3.2.2.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/ISDN-User/Users

**Mögliche Werte Telnet:**

- Kein, ein oder mehrere verfügbare S0-Busse.

**Default:** Abhängig vom Gerätetyp.

#### 2.33.3.2.2.3 MSN/DDI

Interne MSN, die für diesen Benutzer auf dem internen ISDN-Bus verwendet wird.

MSN: Nummer des Telefonanschlusses, wenn es sich um einen Mehrgeräteanschluss handelt.

DDI (Direct Dialing in): Durchwahlnummer des Telefons, wenn der Anschluss als Anlagenanschluss konfiguriert ist.

**SNMP-ID:** 2.33.3.2.2.3

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/ISDN-User/Users

**Mögliche Werte Telnet:**

- max. 19 Ziffern und #-Zeichen

**Default:** Leer

Mit dem #-Zeichen als Platzhalter können ganze Gruppen von Rufnummern z. B. bei der Verwendung von Durchwahlnummern in einem einzigen Eintrag erfasst werden.

Benutzereinträge mit #-Zeichen zur Abbildung von Benutzergruppen können nicht für eine Anmeldung an einer übergeordneten TK-Anlage verwendet werden. Für diese Anmeldung ist immer ein spezifischer Eintrag für den einzelnen ISDN-Benutzer notwendig.

#### 2.33.3.2.2.4 Display-Name

Name, der auf dem angerufenen Telefondisplay erscheinen soll.

**SNMP-ID:** 2.33.3.2.2.4

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/ISDN-User/Users

**Mögliche Werte Telnet:**

- max. 32 alphanumerische Zeichen

**Default:** Leer

#### 2.33.3.2.2.5 Auth-Name

Name zur Authentifizierung an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt.

**SNMP-ID:** 2.33.3.2.2.5

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/ISDN-User/Users

**Mögliche Werte Telnet:**

- max. 63 Zeichen

**Default:** Leer

Nur erforderlich bei Anmeldung des Benutzers an einer übergeordneten SIP-TK-Anlage.

#### 2.33.3.2.2.6 Secret

Passwort zum Anmelden als SIP-Benutzer an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des ISDN-Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt. Es ist möglich, dass sich ISDN-Benutzer an einer übergeordneten SIP-TK-Anlage mit einem gemeinsamen Passwort ("Standard-Passwort" an der SIP-PBX-Line) anmelden.

**SNMP-ID:** 2.33.3.2.2.6

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/ISDN-User/Users

**Mögliche Werte Telnet:**

- max. 32 Zeichen

**Default:** Leer

#### 2.33.3.2.2.7 Domain

Domäne einer übergeordneten SIP-TK-Anlage, wenn der ISDN-Benutzer als SIP-Benutzer angemeldet werden soll. Die Domäne muss bei einer SIP-PBX-Line konfiguriert sein, damit eine übergeordnete Anmeldung erfolgt.

**SNMP-ID:** 2.33.3.2.2.7

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/ISDN-User/Users

**Mögliche Werte Telnet:**

- max. 63 Zeichen

**Default:** Leer

Nur erforderlich bei Anmeldung des Benutzers an einer übergeordneten SIP-TK-Anlage.

#### 2.33.3.2.2.8 DialCompl

Mit der Blockwahlerkennung kann die gewählt Nummer automatisch als vollständig markiert werden (z. B. bei Zielwahl oder Wahlwiederholung), der Ruf wird damit schneller aufgebaut. Eine Nachwahl ist nicht möglich.

**SNMP-ID:** 2.33.3.2.2.8

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/ISDN-User/Users

**Mögliche Werte Telnet:**

- Auto: Blockwahl wird automatisch erkannt (z. B. bei Zielwahl oder Wahlwiederholung), und der Ruf damit schneller aufgebaut. Eine Nachwahl ist nicht möglich.
- Manual: Keine Blockwahl, mit Eingabe des "#" kann die Nummer als vollständig gekennzeichnet werden und somit der Rufaufbau initiiert werden.

**Default:** Auto/Automatisch

Mit Eingabe des "#" kann bei ausgeschalteter Blockwahlerkennung die Nummer manuell als vollständig gekennzeichnet und somit der Rufaufbau initiiert werden.

#### 2.33.3.2.2.9 Active

Aktiviert oder deaktiviert den Eintrag.

**SNMP-ID:** 2.33.3.2.2.9

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/ISDN-User/Users

**Mögliche Werte Telnet:**

- nein
- ja

**Default:** ja/Ein

### 2.33.3.3 Analog-User

Dieses Menü enthält die Analoge-Benutzer-Einstellungen für den Voice-Call-Manager.

**SNMP-ID:** 2.33.3.3

**Pfad Telnet:** /Setup/Voice-Call-Manager/User

#### 2.33.3.3.4 Extern-Cln-Prefix

Dieses Präfix wird bei einem eingehenden, externen Anruf der vorhandenen Calling Party ID vorangestellt, wenn der Anruf an einen Analog-Benutzer gerichtet ist. Sofern ein Leitungspräfix definiert ist, wird dieses der gesamten Rufnummer vorangestellt.

**SNMP-ID:** 2.33.3.3.4

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Analog-User

**Mögliche Werte Telnet:**

- max. 15 Ziffern oder *.

**Default:** Leer

#### 2.33.3.3.1 Interfaces

Hier wählen Sie die Schnittstelle aus, an der analoge Benutzer angeschlossen werden.

**SNMP-ID:** 2.33.3.3.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Analog-User

#### 2.33.3.3.1.1 Name

Name für die Schnittstelle

**SNMP-ID:** 2.33.3.3.1.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Analog-User/Interfaces

**Mögliche Werte Telnet:**

- ANALOG

**Default:** ANALOG

#### 2.33.3.3.1.2 Ifc

Ein internes Interface, an das Analog-Teilnehmer angeschlossen sind.

**SNMP-ID:** 2.33.3.3.1.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Analog-User/Interfaces

**Mögliche Werte Telnet:**

- Keine
- Analog-1
- Analog-2

**Default:** Analog-1

#### 2.33.3.3.1.3 Active

Aktiviert oder deaktiviert den Eintrag.

**SNMP-ID:** 2.33.3.3.1.3

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Analog-User/Interfaces

**Mögliche Werte Telnet:**

- Ja
- Nein

**Default:** Ja

#### 2.33.3.3.1.4 Kommentar

Kommentar zu diesem Eintrag

**SNMP-ID:** 2.33.3.3.1.4

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Analog-User/Interfaces

**Mögliche Werte Telnet:**

- max. 63 Zeichen

**Default:** leer

### 2.33.3.3.3 Intern-Cln-Prefix

Dieses Präfix wird bei einem eingehenden, internen Anruf der vorhandenen Calling Party ID vorangestellt, wenn der Anruf an einen Analog-Benutzer gerichtet ist. Sofern ein Leitungspräfix definiert ist, wird dieses der gesamten Rufnummer vorangestellt.

**SNMP-ID:** 2.33.3.3.3

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Analog-User

**Mögliche Werte Telnet:**

- max. 15 Ziffern oder *.

**Default:** *

### 2.33.3.3.5 Intern-Dial-Tone

Der Wählton bestimmt, welchen Ton ein Benutzer nach dem Abheben des Hörers hört. Der „interne Wählton" gleicht dem Ton, den ein Benutzer an einer TK-Anlage ohne spontane Amtsholung hört (drei kurze Töne gefolgt von einer Pause). Der „externe Wählton" gleicht folglich dem Ton, dass nach dem Abheben ein Amt anzeigt (anhaltender Ton ohne Unterbrechungen). Passen Sie den Wählton nach Bedarf an die Verwendung der spontanen Amtsholung an, um ein ähnliches Verhalten wie an einem externen Anschluss zu simulieren.

**SNMP-ID:** 2.33.3.3.5

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Analog-User

**Mögliche Werte Telnet:**

- Ja
- Nein

**Default:** Nein, es wird der externe Wählton verwendet

### 2.33.3.3.2 Users

Hier definieren Sie alle lokalen Analog-Benutzer (Endgeräte). Darüber hinaus können Sie Authentifizierungs-Daten zur SIP Anmeldung angeben.

**SNMP-ID:** 2.33.3.3.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Analog-User

#### 2.33.3.3.2.1 Number/Name

Interne Rufnummer des Analog-Telefons oder Name des Benutzers (SIP-URI).

**SNMP-ID:** 2.33.3.3.2.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Analog-User/Users

**Mögliche Werte Telnet:**

- max. 20 Zeichen

**Default:** Leer

#### 2.33.3.3.2.10 Active

Aktiviert oder deaktiviert den Eintrag.

**SNMP-ID:** 2.33.3.3.2.10

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Analog-User/Users

**Mögliche Werte Telnet:**

- Ein
- Aus

**Default:** Ein

#### 2.33.3.3.2.11 Kommentar

Kommentar zu diesem Eintrag.

**SNMP-ID:** 2.33.3.3.2.11

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Analog-User/Users

**Mögliche Werte Telnet:**

- max. 63 Zeichen

**Default:** Leer

#### 2.33.3.3.2.12 Device-Type

Typ des angeschlossenen Geräts.

Der Typ entscheidet, ob ggf. eine Umwandlung einer analogen Fax-Verbindung in SIP T.38 erfolgt. Bei Auswahl des Typs "Fax" oder "Telefon/Fax" wird eine Erkennung von Fax-Signalen aktiviert, die u.U. bei einem Telefon zu Beeinträchtigungen der Verbindungsqualität führen kann. Bitte wählen Sie daher den Typ entsprechend des angeschlossenen Gerätes, um die optimale Qualität zu erzielen.

**SNMP-ID:** 2.33.3.3.2.12

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Analog-User/Users

**Mögliche Werte Telnet:**

- Phone
- Fax
- Auto

**Default:** Phone/Telefon

#### 2.33.3.3.2.2 Ifc

Analoges-Interface, das für den Verbindungsaufbau verwendet werden soll.

**SNMP-ID:** 2.33.3.3.2.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Analog-User/Users

**Mögliche Werte Telnet:**

- Analog-1
- Analog-2
- keine

**Default:** Analog-1

#### 2.33.3.3.2.3 Display-Name

Name, der auf dem angerufenen Telefondisplay erscheinen soll.

**SNMP-ID:** 2.33.3.3.2.3

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Analog-User/Users

**Mögliche Werte Telnet:**

- max. 63 Zeichen

**Default:** Leer

#### 2.33.3.3.2.4 Auth-Name

Name zur Authentifizierung an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt.

**SNMP-ID:** 2.33.3.3.2.4

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Analog-User/Users

**Mögliche Werte Telnet:**

- max. 63 Zeichen

**Default:** leer

#### 2.33.3.3.2.5 Secret

Passwort zum Anmelden als SIP-Benutzer an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des Analog-Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt. Es ist möglich, dass sich ISDN-Benutzer an einer übergeordneten SIP-TK-Anlage mit einem gemeinsamen Passwort ("Standard-Passwort" an der SIP-PBX-Line) anmelden.

**SNMP-ID:** 2.33.3.3.2.5

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Analog-User/Users

**Mögliche Werte Telnet:**

- max. 32 Zeichen

**Default:** Leer

#### 2.33.3.3.2.6 Domain

Domäne einer übergeordneten SIP-TK-Anlage, wenn der Analog-Benutzer als SIP-Benutzer angemeldet werden soll. Die Domäne muss bei einer SIP-PBX-Line konfiguriert sein, damit eine übergeordnete Anmeldung erfolgt.

**SNMP-ID:** 2.33.3.3.2.6

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Analog-User/Users

**Mögliche Werte Telnet:**

- max. 63 Zeichen

**Default:** Leer

#### 2.33.3.3.2.8 CLIR

Schaltet die Übermittlung der Absenderinformationen ein oder aus.

**SNMP-ID:** 2.33.3.3.2.8

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Analog-User/Users

**Mögliche Werte Telnet:**

- Ja: Die Übermittlung der Absenderinformationen wird auf jeden Fall unterdrückt, unabhängig von den Einstellungen am Endgerät des Benutzers.
- Nein: Die Übermittlung der Absenderinformationen wird nicht im Gerät unterdrückt, die Einstellungen am Endgerät des Benutzers entscheiden über Übermittlung der Absenderinformationen.

**Default:** Nein

#### 2.33.3.3.2.9 Metering

Mit dem Gebührenimpuls (GBI) werden in analogen Telefonnetzen Informationen über die während einer Verbindung anfallenden Kosten zum Anrufer übermittelt. In dessen Endgerät (Telefon mit Gebührenanzeige, Gebührenanzeiger) wird der Gebührenimpuls aus dem übertragenen Gesamtsignal heraus gefiltert und in eine entsprechende Gebührenanzeige umgewandelt.

**SNMP-ID:** 2.33.3.3.2.9

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Analog-User/Users

**Mögliche Werte Telnet:**

- Ja
- Nein

**Default:** Nein

Mit dieser Option wird die Übertragung des Gebührenimpulses an den analogen Benutzer/das Endgerät ermöglicht. Dabei kann eine Gebühreninformation beispielsweise aus dem ISDN-Telefonnetz an eine ISDN-Leitung übermittelt und in einen analogen Gebührenimpuls umgesetzt werden.

### 2.33.3.4 Extensions

Hier können Sie erweiterte Benutzer-Einstellungen wie Anklopfen oder Anrufweiterschaltung festlegen.

**SNMP-ID:** 2.33.3.4

**Pfad Telnet:** /Setup/Voice-Call-Manager/User

#### 2.33.3.4.1 Name

Für diese Rufnummer bzw. diese SIP-ID gelten die Benutzer-Einstellungen.

**SNMP-ID:** 2.33.3.4.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Extensions

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

Anrufweiterschaltungen können für alle lokalen Benutzer (SIP, ISDN oder Analog) eingerichtet werden.

#### 2.33.3.4.10 Active

Aktiviert oder deaktiviert den Eintrag.

**SNMP-ID:** 2.33.3.4.10

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Extensions

**Mögliche Werte Telnet:**

- Ein
- Aus

**Default:** Ein

#### 2.33.3.4.11 Busy-on-Busy

Verhindert das Zustellen eines zweiten Anrufs zu einem Endgerät, unabhängig davon, ob „Anklopfen" (CW, Call Waiting Indication) auf dem Endgerät erlaubt oder unterbunden ist, d.h. auch das „Anklopfen" wird verhindert. Zudem erhält der zweite Anrufende einen Besetzt-Ton. Dies gilt auch, wenn sich bei der internen Rufnummer um eine Mehrfachanmeldung handelt und nur mit einem der möglichen Endgeräte telefoniert wird.

**SNMP-ID:** 2.33.3.4.11

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Extensions

**Mögliche Werte Telnet:**

- Ja
- Nein

**Default:** Nein

#### 2.33.3.4.12 CF-Set-Cln-Id

Stellen Sie hier ein, welche Rufnummer bei einer Weiterleitung (CF) signalisiert wird - zum Beispiel die aus CDIV - alternativ kann man auch eine eigene Rufnummer als Anrufernummer fest eintragen

**SNMP-ID:** 2.33.3.4.12

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Extensions

**Mögliche Werte Telnet:**

- Extension-ID:
- Calling-ID: signalisiert die eingehende Rufnummer. Bei der Weiterleitung an ein Handy kann ein Teilnehmer so die Original-Rufnummer des anrufenden Teilnehmers erkennen.
- Custom-ID: signalisiert die unter /Setup/Voice-Call-Manager/User/Extensions/Custom-ID eingetragene Rufnummer

**Default:** Extension-ID

#### 2.33.3.4.13 Custom-Id

Stellen Sie hier die Rufnummer ein, die bei einer Weiterleitung (CF) signalisiert wird.

**SNMP-ID:** 2.33.3.4.13

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Extensions

**Mögliche Werte Telnet:**

- maximal 64 Zeichen

**Default:** leer

Diese Rufnummer wird nur verwendet, wenn der Parameter /Setup/Voice-Call-Manager/User/Extensions/CF-Set-Cln-Id auf den Wetrt "Custom-ID" eingestellt ist.

#### 2.33.3.4.2 User modifiable

Aktiviert oder deaktiviert die Möglichkeit, die Benutzer-Einstellungen auch über das Telefon zu konfigurieren.

**SNMP-ID:** 2.33.3.4.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Extensions

**Mögliche Werte Telnet:**

- Ja
- Nein

**Default:** Ja

#### 2.33.3.4.3 CFU-Active

Aktiviert oder deaktiviert die sofortige Rufweiterschaltung (CFU) ohne Bedingung.

**SNMP-ID:** 2.33.3.4.3

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Extensions

**Mögliche Werte Telnet:**

- Ja
- Nein

**Default:** Nein

#### 2.33.3.4.4 CFU-Target

Ziel für die sofortige Rufweiterschaltung ohne Bedingung.

**SNMP-ID:** 2.33.3.4.4

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Extensions

**Mögliche Werte Telnet:**

- Maximal 64 Zeichen zur Bezeichnung lokaler Benutzer, von Rufgruppen oder externen Rufnummern

**Default:** Leer

#### 2.33.3.4.5 CFNR-Active

Aktiviert oder deaktiviert die verzögerte Rufweiterschaltung (bei Abwesenheit; CFNR).

**SNMP-ID:** 2.33.3.4.5

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Extensions

**Mögliche Werte Telnet:**

- Ja
- Nein

**Default:** Nein

#### 2.33.3.4.6 CFNR-Target

Ziel für die verzögerte Rufweiterschaltung.

**SNMP-ID:** 2.33.3.4.6

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Extensions

**Mögliche Werte Telnet:**

- Maximal 64 Zeichen zur Bezeichnung lokaler Benutzer, von Rufgruppen oder externen Rufnummern

**Default:** Leer

#### 2.33.3.4.7 CFNR-Timeout

Wartezeit für die verzögerte Rufweiterschaltung. Nach Ablauf dieser Zeit wird der Anruf an das Rufziel weitergeleitet, wenn der Teilnehmer den Anruf nicht annimmt.

**SNMP-ID:** 2.33.3.4.7

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Extensions

**Mögliche Werte Telnet:**

- max. 255 Sekunden

**Default:** 15 Sekunden

#### 2.33.3.4.8 CFB-Active

Aktiviert oder deaktiviert die Weiterschaltung bei „besetzt".

**SNMP-ID:** 2.33.3.4.8

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Extensions

**Mögliche Werte Telnet:**

- Ja
- Nein

**Default:** Nein

#### 2.33.3.4.9 CFB-Target

Ziel für die Weiterschaltung bei „besetzt".

**SNMP-ID:** 2.33.3.4.9

**Pfad Telnet:** /Setup/Voice-Call-Manager/User/Extensions

**Mögliche Werte Telnet:**

- Maximal 64 Zeichen zur Bezeichnung lokaler Benutzer, von Rufgruppen oder externen Rufnummern

**Default:** Leer

## 2.33.4 Line

Dieses Menü enthält die Leitungs-Einstellungen für den Voice-Call-Manager.

**SNMP-ID:** 2.33.4

**Pfad Telnet:** /Setup/Voice-Call-Manager

### 2.33.4.1 SIP-Provider

Dieses Menü enthält die SIP-Provider-Einstellungen für den Voice-Call-Manager.

**SNMP-ID:** 2.33.4.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line

#### 2.33.4.1.1 Line

Über diese Leitungen meldet das Gerät sich bei anderen SIP-Gegenstellen (in der Regel SIP-Provider oder als Remote Gateway bei SIP-TK-Anlagen) an. Die Verbindung erfolgt entweder über das Internet oder einen VPN-Tunnel. Es können bis zu 16 SIP-Leitungen eingetragen werden.

**SNMP-ID:** 2.33.4.1.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider

#### 2.33.4.1.1.1 Name

Name der Leitung, darf nicht identisch sein mit einer anderen in dem Gerät konfigurierten Leitung.

**SNMP-ID:** 2.33.4.1.1.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- max. 16 Zeichen

**Default:** leer

#### 2.33.4.1.1.10 Active

Aktiviert oder deaktiviert den Eintrag.

**SNMP-ID:** 2.33.4.1.1.10

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- Ein
- Aus

**Default:** Ein

#### 2.33.4.1.1.11 Comment

Kommentar zu diesem Eintrag

**SNMP-ID:** 2.33.4.1.1.11

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

#### 2.33.4.1.1.12 Codecs

Die beteiligten Endgeräte handeln beim Verbindungsaufbau aus, welche Codecs für die Komprimierung der Sprachdaten verwendeten werden sollen. Mit dem Codec-Filter können Sie die erlaubten Codecs einschränken und nur bestimmte Codecs zulassen.

**SNMP-ID:** 2.33.4.1.1.12

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- Neben den allgemein verfügbaren Codecs unterstützen einige Modelle für die SIP-Gateway-Funktion auch folgende Codecs:
- G.722 - 64 kBit/s (High-Quality-Codec nur von ISDN zu SIP und umgekehrt)
- G.729 - 8 kBit/s (Codec mit hoher Kompression für geringe Bandbreiten)
- Diese Codecs sind verfügbar für die Geräte LANCOM 1722 VoIP, LANCOM 1723 VoIP, LANCOM 1724 VoIP und LANCOM 1823 VoIP sowie für alle LANCOM-Modelle mit LANCOM Advanced VoIP Option.

**Default:** Alle

Falls die Schnittmenge an verfügbaren Codecs der beteiligten Endgeräte hier ausgeschaltet wird, kommt keine Verbindung zustande.

#### 2.33.4.1.1.13 Codec-Order

Mit diesem Parameter beeinflussen Sie die Reihenfolge, in der die möglichen Codecs beim Verbindungsaufbau angeboten werden.

**SNMP-ID:** 2.33.4.1.1.13

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider

**Mögliche Werte Telnet:**

- Unchanged: Lässt die Reihenfolge der Codecs unverändert.
- BestQuality: Verändert die Reihenfolge der angebotenen Codecs so, dass eine möglichst hohe Sprachqualität erreicht wird.
- LowestBandwidth: Verändert die Reihenfolge der angebotenen Codecs so, dass eine möglichst geringe Bandbreite benötigt wird.

**Default:** Unchanged

#### 2.33.4.1.1.14 Rtg-tag

Routing-Tag zur Auswahl einer bestimmten Route über die Routing-Tabelle für Verbindungen zu diesem SIP-Provider.

**SNMP-ID:** 2.33.4.1.1.14

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- max. 64 Ziffern

**Default:** 0

#### 2.33.4.1.1.15 Display-Name

Name, der auf dem angerufenen Telefondisplay erscheinen soll.

**SNMP-ID:** 2.33.4.1.1.15

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** Leer

Dieser Wert sollte im Normalfall nicht gesetzt werden, da bei eingehenden Rufen der SIP-Provider den Display-Namen setzt und bei ausgehenden Rufen der lokale Client bzw. die Rufquelle (ggf. überschrieben mit den Einstellungen zum Display-Namen des jeweiligen Benutzers). Oftmals werden hier zusätzliche Informationen übermittelt (z. B. Originalrufnummer bei einer Umleitung etc.), die für den Angerufenen hilfreich sein können. Im Fall von SIP-Einzel-Accounts verlangen manche Provider allerdings auch den in den Anmeldedaten

vorgegebenen Display-Namen bzw. einen zur SIP-ID identischen Eintrag (z. B. T-Online). Mit den Zugangsdaten wird die Leitung (Einzel-Account, Trunk, Link, Gateway) angemeldet, nicht jedoch einzelne lokale Benutzer mit ihren individuellen Anmeldedaten. Wenn einzelne Benutzer (SIP, ISDN, Analog) mit den dort bzw. auf dem Endgerät hinterlegten Daten bei einer übergeordneten Instanz registriert werden sollen, muss der Leitungstyp SIP-PBX-Leitung gewählt werden.

#### 2.33.4.1.1.16 Registrar

Der SIP-Registrar ist die Stelle, welche die Anmeldung mit den konfigurierten Authentifizierungsdaten für diesen Account beim SIP-Provider entgegen nimmt.

**SNMP-ID:** 2.33.4.1.1.16

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

Dieses Feld kann frei bleiben, sofern der SIP-Provider keine speziellen Angaben macht. Der Registrar wird dann über DNS-SRV-Anfragen zur konfigurierten SIP-Domäne/Realm ermittelt (bei SIP-Services im Firmennetz/VPN ist dies oftmals nicht der Fall, d.h. der Wert muss explizit gesetzt werden).

#### 2.33.4.1.1.17 Mode

Mit dieser Auswahl bestimmen Sie die Betriebsart der SIP-Leitung.

**SNMP-ID:** 2.33.4.1.1.17

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- provider: Verhält sich nach außen wie ein üblicher SIP-Account mit einer einzigen öffentlichen Nummer. Die Nummer wird beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt (wenn eine (Re-)Registrierung für diese SIP-Provider-Line aktiviert ist). Bei ausgehenden Rufen wird die Nummer des Rufenden (Absender) durch die registrierte Nummer ersetzt (maskiert). Eingehende Rufe werden der konfigurierten internen Ziel-Nummer zugestellt. Es kann nur maximal eine Verbindung zu einem Zeitpunkt bestehen.
- trunk: Verhält sich nach außen wie ein erweiterter SIP-Account mit einer Stamm- und mehreren Durchwahlnummern. Die SIP-ID wird als Stammnummer beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt (wenn eine (Re-)Registrierung für diese SIP-Provider-Line aktiviert ist). Bei ausgehenden Rufen fungiert die Stammnummer als Präfix, das jeder rufenden Nummer (Absender; SIP: “From:”) vorangestellt wird. Bei eingehenden Rufen wird das Präfix aus der Ziel-Nummer entfernt (SIP: “To:”). Die verbleibende Nummer wird als interne Durchwahl verwendet. Im Fehlerfall (Präfix nicht auffindbar, Ziel gleich Präfix) wird der Ruf an die konfigurierte interne Ziel-Nummer geleitet. Die maximale Anzahl der Verbindungen zu einem bestimmten Zeitpunkt ist nur durch die zur Verfügung stehende Bandbreite begrenzt.
- gateway: Sie verhält sich nach außen wie ein üblicher SIP-Account mit einer einzigen öffentlichen Nummer, der SIP-ID. Die Nummer (SIP-ID) wird beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt (wenn eine (Re-)Registrierung für diese SIP-Provider-Line aktiviert ist). Bei ausgehenden Rufen wird die Nummer des Rufenden (Absender) durch die registrierte Nummer (SIP-ID in SIP: “From:”) ersetzt (maskiert) und in einem separaten Feld (SIP: “Contact:”) übertragen. Bei eingehenden Rufen wird die gerufene Nummer (Ziel) nicht modifiziert. Die maximale Anzahl der Verbindungen zu einem bestimmten Zeitpunkt ist nur durch die zur Verfügung stehende Bandbreite begrenzt.
- link: Verhält sich nach außen wie ein üblicher SIP-Account mit einer einzigen öffentlichen Nummer (SIP-ID). Die Nummer wird beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt (wenn eine (Re-)Registrierung für diese SIP-Provider-Line aktiviert ist). Bei ausgehenden Rufen wird die Nummer des Rufenden (Absender; SIP: “From:”) nicht modifiziert. Bei eingehenden Rufen wird die gerufene Nummer (Ziel; SIP: “To:”) nicht

modifiziert. Die maximale Anzahl der Verbindungen zu einem bestimmten Zeitpunkt ist nur durch die zur Verfügung stehende Bandbreite begrenzt.

**Default:** provider

Der “Serviceprovider” kann ein Server im Internet, eine IP-Telefonanlage oder ein Voice-Gateway sein. Bitte beachten Sie auch die Hinweise zum ‘SIP-Mapping’.

#### 2.33.4.1.1.18 Refer-weiterleiten

Bei der Rufvermittlung (Verbindung) von zwei entfernten Gesprächsteilnehmern kann die Vermittlung im Gerät selbst gehalten (Media-Proxy) oder an die Vermittlungsstelle beim Provider übergeben werden, wenn beide zu verbindende Gesprächsteilnehmer über diese SIP-Provider-Leitung erreicht werden (andernfalls übernimmt der Media-Proxy im LANCOM die Vermittlung der Medienströme, z. B. beim Verbinden zwischen zwei SIP-Provider-Leitungen).

**SNMP-ID:** 2.33.4.1.1.18

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- Ja: Vermittlung wird an den Provider weitergeleitet.
- Nein: Die Verbindungen werden im Gerät selbst gehalten.

**Default:** Nein

Eine Übersicht über die wichtigsten SIP-Provider, die diese Funktion unterstützen, finden Sie im Support-Bereich auf der Internet-Seite.

#### 2.33.4.1.1.19 Lokale-Portnummer

Dies ist der Port des LANCOM-Proxies zur Kommunikation mit dem Provider.

**SNMP-ID:** 2.33.4.1.1.19

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- 1 bis 65536

**Default:** 0

**Besondere Werte:** 0: Dynamische Portauswahl, der Port wird automatisch aus dem Pool der freien Portnummern gewählt.

Wenn die (Re-)Registrierung der Leitung deaktiviert ist, muss der lokale Port fest vorgegeben und als Zielport auch auf der Providerseite eingetragen werden (z. B. bei Nutzung eines regsitrierungslosen Trunks im Firmen-VPN), damit sich beide Seiten SIP-Signalisierungen senden können.

#### 2.33.4.1.1.2 Domain

SIP-Domäne/Realm der übergeordneten Gegenstelle. Sofern die Gegenstelle DNS-Service Records für SIP unterstützt, genügt diese Angabe, um Proxy, Outbound-Proxy, Port, Registrar automatisch zu ermitteln - das ist bei typischen SIP-Provider-Angeboten i.d.R. der Fall.

**SNMP-ID:** 2.33.4.1.1.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

#### 2.33.4.1.1.20 (Re-)Registrierung

Hiermit wird die (wiederholte) Registrierung der SIP-Provider-Leitung aktiviert. Die Registrierung kann auch zur Leitungsüberwachung herangezogen werden.

**SNMP-ID:** 2.33.4.1.1.20

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- Ja
- Nein

**Default:** Ja

Für die Nutzung der (Re-)Registrierung muss die Methode der Leitungsüberwachung entsprechend auf "Registrierung" oder "Automatisch" gestellt werden. Die Registrierung wird jeweils nach Ablauf des Überwachungsintervalls wiederholt. Wenn der SIP-Registrar des Providers ein anderes Intervall vorschlägt, wird dieses automatisch übernommen.

#### 2.33.4.1.1.21 Leitungsüberwachung

Spezifiziert die Methode der Leitungsüberwachung. Die Leitungsüberwachung prüft die Verfügbarkeit einer SIP-Provider-Leitung. Der Status der Überwachung kann im Call Router zum Wechsel auf eine Backup-Leitung herangezogen werden. Die Überwachungsmethode legt fest, wie der Status geprüft wird.

**SNMP-ID:** 2.33.4.1.1.21

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- Auto: Die Methode wird automatisch ermittelt.
- Deaktiviert: Keine Überwachung, die Leitung wird stets als verfügbar gemeldet. In dieser Einstellung kann die tatsächliche Verfügbarkeit der Leitung nicht überwacht werden.
- Register: Überwachung mittels Register-Requests während des Registrierungsvorgangs. Für die Nutzung dieser Einstellung muss für diese Leitung ebenfalls die "(Re-)Registrierung" aktiviert sein.
- Options: Überwachung mittels Options-Requests. Dabei wird wie bei einem Polling regelmäßig eine Anfrage an die Gegenstelle verschickt, je nach Antwort wird die Leitung als verfügbar oder nicht verfügbar angesehen. Diese Einstellung eignet sich z. B. für registrierungslose Leitungen.

**Default:** Auto

#### 2.33.4.1.1.22 Überwachungsintervall

Das Intervall der Leitungsüberwachung in Sekunden. Dieser Wert wirkt sich sowohl auf die Leitungsüberwachung mit Register-Request als auch mit Option-Request aus. Das Überwachungsintervall muss mindestens 60 Sekunden betragen und legt fest, nach welcher Zeit die Überwachungsmethode erneut angewendet wird. Wenn die (Re-)Registrierung aktiviert ist, wird das Überwachungsintervall auch als Zeitraum bis zur nächsten Registrierung verwendet.

**SNMP-ID:** 2.33.4.1.1.22

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- max. 5 Ziffern

**Default:** 60

**Besondere Werte:** Werte kleiner als 60 Sekunden werden automatisch als 60 Sekunden angenommen.

Falls die Gegenstelle in der Antwort auf einen Option-Request einen anderen Wert für das Überwachungsintervall vorschlägt, so wird dieser akzeptiert und in der Folgezeit verwendet.

#### 2.33.4.1.1.23 Vertrauenswürdig

Spezifiziert die Zugehörigkeit der Gegenstelle dieser Leitung (Provider) zur “Trusted-Area”. In dieser vertrauenswürdigen Zone wird die Caller ID als Information über den Gesprächsteilnehmer nicht entfernt, selbst wenn das durch Einstellungen in der Leitung (CLIR) oder durch das Endgerät gewünscht ist. Bei einer Verbindung über eine vertrauenswürdige Leitung wird die Caller ID entsprechend der ausgewählten Privacy-Methode übertragen und erst in der letzten Vermittlungsstelle vor dem entfernten Gesprächsteilnehmer entfernt. Innerhalb der vertrauenswürdigen Zone kann so z. B. die Caller ID für Abrechnungszwecke ausgewertet werden. Diese Funktion ist u. a. für Provider interessant, die mit einem VoIP-Router direkt beim Kunden das von ihnen selbst verwaltete Netzwerk bis zum Anschluss der VoIP-Endgeräte ausdehnen.

**SNMP-ID:** 2.33.4.1.1.23

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- Ja: Vertrauenswürdig
- Nein: Nicht vertrauenswürdig

**Default:** Ja

Diese Funktion wird nicht von allen Providern unterstützt.

#### 2.33.4.1.1.24 Privacy-Methode

Spezifiziert die verwendete Methode zur Übermittlung der Caller ID im separaten SIP-Header-Feld.

**SNMP-ID:** 2.33.4.1.1.24

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- Keine
- RFC3325: mittels P-Preferred-Id/P-Asserted-Id
- IETF-Draft-Sip-Privacy-04: mittels RPID (Remote Party ID)

**Default:** Keine

#### 2.33.4.1.1.25 FROM-Benutzertypen-entfernen

Aktivieren Sie diese Option, um die Information "user=phone" aus dem From-Feld eines Rufes zu entfernen, der über eine Provider-Leitung abgeht. Einzelne VoIP-Proxies verarbeiten diese Information nicht standard-konform und lehnen daraufhin den Verbindungsaufbau ab.

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line/FROM-Benutzertypen-entfernen

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

#### 2.33.4.1.1.3 Port

TCP/UDP-Port beim SIP-Provider, an den die SIP-Pakete gesendet werden.

**SNMP-ID:** 2.33.4.1.1.3

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- Beliebieger freier TCP/IP-Port.

**Default:** 5060

In der Firewall muss dieser Port freigeschaltet sein, damit die Verbindung funktionieren kann.

#### 2.33.4.1.1.4 User-id

Telefonnummer des SIP-Accounts oder Name des Benutzers (SIP-URI).

**SNMP-ID:** 2.33.4.1.1.4

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

Mit den Zugangsdaten wird die Leitung (Einzel-Account, Trunk, Link, Gateway) angemeldet, nicht jedoch einzelne lokale Benutzer mit ihren individuellen Anmeldedaten. Wenn einzelne Benutzer (SIP, ISDN, Analog) mit den dort bzw. auf dem Endgerät hinterlegten Daten bei einer übergeordneten Instanz registriert werden sollen, muss der Leitungstyp SIP-PBX-Leitung gewählt werden.

#### 2.33.4.1.1.5 Auth-Name

Name zur Authentifizierung an der übergeordneten SIP-Gegenstelle (Provider/SIP-TK-Anlage).

**SNMP-ID:** 2.33.4.1.1.5

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

Mit den Zugangsdaten wird die Leitung (Einzel-Account, Trunk, Link, Gateway) angemeldet, nicht jedoch einzelne lokale Benutzer mit ihren individuellen Anmeldedaten. Wenn einzelne Benutzer (SIP, ISDN, Analog) mit den dort bzw. auf dem Endgerät hinterlegten Daten bei einer übergeordneten Instanz registriert werden sollen, muss der Leitungstyp SIP-PBX-Leitung gewählt werden.

#### 2.33.4.1.1.6 Secret

Das Passwort zur Authentifizierung beim SIP-Registrar und SIP-Proxy des Providers. Bei Leitungen ohne (Re-)Registrierung kann das Passwort unter Umständen entfallen.

**SNMP-ID:** 2.33.4.1.1.6

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

#### 2.33.4.1.1.7 Outb-proxy

Der Outbound-Proxy des SIP-Providers nimmt alle vom LANCOM ausgehenden SIP-Signalisierungen einer Verbindung zu diesem Provider für die Dauer der Verbindung entgegen.

**SNMP-ID:** 2.33.4.1.1.7

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

Dieses Feld kann frei bleiben, sofern der SIP-Provider keine speziellen Angaben macht. Der Outbound-Proxy wird dann über DNS-SRV-Anfragen zur konfigurierten SIP-Domäne/Realm ermittelt (bei SIP-Services im Firmennetz/VPN ist dies oftmals nicht der Fall, d.h. der Wert muss explizit gesetzt werden).

#### 2.33.4.1.1.8 Cln-Prefix

Das Anruf-Präfix ist eine Nummer, die den Anrufer-Nummern (CLI; SIP „From:“) aller ankommenden Anrufe auf dieser vorangestellt wird, um eindeutige Rückruf-Nummern zu erzeugen.

Beispielsweise kann hier eine Nummer ergänzt werden, die im Call-Router bei abgehenden Rufen (dem Rückruf) zur Leitungsauswahl ausgewertet und wieder entfernt wird.

**SNMP-ID:** 2.33.4.1.1.8

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- max. 9 Ziffern

**Default:** leer

#### 2.33.4.1.1.9 Name

Die Wirkung dieses Feldes hängt von der Einstellung des Modus der Leitung ab:

Wenn der Modus der Leitung „Einzel-Account“ ist, werden alle über die Leitung eingehenden Rufe mit dieser Nummer als Ruf-Ziel (SIP: „To:“) an den Call-Router übergeben.

Wenn der Modus „Trunk“ ist, wird die Ziel-Nummer durch Entfernen der für den Trunk definierten Stammnummer ermittelt – falls dabei ein Fehler auftritt, wird der Ruf mit der in diesem Feld eingetragenen Nummer versehen (SIP: „To:“) an den Call-Router übergeben.

Wenn der Modus auf „Gateway“ oder „Link“ eingestellt ist, hat der Eintrag in diesem Feld keine Wirkung.

**SNMP-ID:** 2.33.4.1.1.9

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

### 2.33.4.1.2 Mapping

Mit den Einträgen für das SIP-Mapping wird in Form von Regeln eine Rufnummernumsetzung auf SIP-Leitungen im Trunk- oder Gateway-Modus eingerichtet. Es können bis zu 40 SIP-Mapping-Regeln eingetragen werden.

Bei einer SIP-Leitung im Trunk-Modus wird eine Anpassung der intern verwendeten Rufnummern an den Rufnummernkreis des SIP-Accounts vorgenommen.

Bei ankommenden Rufen wird die Zielrufnummer (Called Party ID) verändert. Die interne Nummer wird eingesetzt, wenn die Called Party ID mit der externen Nummer übereinstimmt.

Bei abgehenden Rufen wird die Absenderrufnummer (Calling Party ID) verändert. Die externe Nummer wird eingesetzt, wenn die Calling Party ID mit der internen Nummer übereinstimmt.

**SNMP-ID:** 2.33.4.1.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider

#### 2.33.4.1.2.1 SIP-Provider

Name der Leitung, für welche die Rufnummernumsetzung gilt.

**SNMP-ID:** 2.33.4.1.2.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Mapping

**Mögliche Werte Telnet:**

- Alle definierten SIP-Leitungen.

**Default:** leer

#### 2.33.4.1.2.2 Ext-Number/Name

Rufnummer im Bereich des SIP-Trunk-Accounts bzw. im Bereich der übergeordneten SIP-TK-Anlage.

**SNMP-ID:** 2.33.4.1.2.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Mapping

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

#### 2.33.4.1.2.3 Number/Name

Rufnummer im Bereich des LANCOM VoIP Router.

**SNMP-ID:** 2.33.4.1.2.3

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Mapping

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

#### 2.33.4.1.2.4 Length

Dieser Wert gibt an, nach wie vielen Stellen eine gerufene Nummer als komplett angesehen wird. Er ist nur auf SIP-Gateway-Leitungen bei solchen Einträgen von Bedeutung, die mit einem #-Zeichen enden.

Bei einem abgehenden Ruf wird die von diesem Eintrag erzeugte externe Rufnummer automatisch nach der angegebenen Anzahl von Stellen als komplett betrachtet und weitergeleitet. Durch diesen Vorgang wird die Anwahl beschleunigt. Alternativ wird die Rufnummer als komplett betrachtet, wenn:

der Benutzer ein #-Zeichen als Abschluss der Rufnummer wählt oder

ein exakt passender Eintrag in der SIP-Mapping-Tabelle ohne #-Zeichen gefunden wurde oder

die eingestellte Wartezeit abgelaufen ist.

**SNMP-ID:** 2.33.4.1.2.4

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Mapping

**Mögliche Werte Telnet:**

- max. 9 Ziffern

**Default:** 0

**Besondere Werte:** Eine Rufnummern-Länge von '0' deaktiviert die vorzeitige Anwahl über die Rufnummernlänge.

#### 2.33.4.1.2.5 Active

Aktiviert oder deaktiviert den Eintrag.

**SNMP-ID:** 2.33.4.1.2.5

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Mapping

**Mögliche Werte Telnet:**

- Ein
- Aus

**Default:** Ein

#### 2.33.4.1.2.6 Kommentar

Kommentar zu diesem Eintrag

**SNMP-ID:** 2.33.4.1.2.6

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Mapping

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

#### 2.33.4.1.2.7 CLIR

Anzeige der eigenen Rufnummer wird beim angerufenen Teilnehmer unterdrückt.

**SNMP-ID:** 2.33.4.1.2.7

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-Provider/Mapping

**Mögliche Werte Telnet:**

- Ja
- Nein

**Default:** Nein

### 2.33.4.2 SIP-PBX

Dieses Menü enthält die SIP-PBX-Einstellungen für den Voice-Call-Manager.

**SNMP-ID:** 2.33.4.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line

#### 2.33.4.2.1 SIP-PBX

Über diese Leitungen werden Verbindungen zu übergeordneten SIP-TK-Anlagen konfiguriert, die in der Regel über VPN angebunden sind. Es können bis zu 4 SIP-TK-Anlagen eingetragen werden.

**SNMP-ID:** 2.33.4.2.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-PBX

#### 2.33.4.2.1.1 Name

Name der Leitung, darf nicht identisch sein mit einer anderen in dem Gerät konfigurierten Leitung.

**SNMP-ID:** 2.33.4.2.1.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

**Mögliche Werte Telnet:**

- max. 16 Zeichen

**Default:** leer

#### 2.33.4.2.1.10 Codecs

Die beteiligten Endgeräte handeln beim Verbindungsaufbau aus, welche Codecs für die Komprimierung der Sprachdaten verwendeten werden sollen. Mit dem Codec-Filter können Sie die erlaubten Codecs einschränken und nur bestimmte Codecs zulassen.

**SNMP-ID:** 2.33.4.2.1.10

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

**Mögliche Werte Telnet:**

- Neben den allgemein verfügbaren Codecs unterstützen einige Modelle für die SIP-Gateway-Funktion auch folgende Codecs:
- G.722 - 64 kBit/s (High-Quality-Codec nur von ISDN zu SIP und umgekehrt)
- G.729 - 8 kBit/s (Codec mit hoher Kompression für geringe Bandbreiten)
- Diese Codecs sind verfügbar für die Geräte LANCOM 1722 VoIP, LANCOM 1723 VoIP, LANCOM 1724 VoIP und LANCOM 1823 VoIP sowie für alle LANCOM-Modelle mit LANCOM Advanced VoIP Option.

**Default:** Alle

Falls die Schnittmenge an verfügbaren Codecs der beteiligten Endgeräte hier ausgeschaltet wird, kommt keine Verbindung zustande.

#### 2.33.4.2.1.11 Codec-Order

Mit diesem Parameter beeinflussen Sie die Reihenfolge, in der die möglichen Codecs beim Verbindungsaufbau angeboten werden.

**SNMP-ID:** 2.33.4.2.1.11

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

**Mögliche Werte Telnet:**

- Keine Optimierung: Lässt die Reihenfolge der Codecs unverändert.
- Beste Qualität: Verändert die Reihenfolge der angebotenen Codecs so, dass eine möglichst hohe Sprachqualität erreicht wird.
- Minimale Bandbreite: Verändert die Reihenfolge der angebotenen Codecs so, dass eine möglichst geringe Bandbreite benötigt wird.

**Default:** Keine Optimierung

#### 2.33.4.2.1.12 Rtg-tag

Routing-Tag zur Auswahl einer bestimmten Route über die Routing-Tabelle für Verbindungen zu dieser SIP-TK-Anlage.

**SNMP-ID:** 2.33.4.2.1.12

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

**Mögliche Werte Telnet:**

- max. 64 Ziffern.

**Default:** 0

#### 2.33.4.2.1.13 Registrar

Der SIP-Registrar ist die Stelle, welche die Anmeldung mit den konfigurierten Authentifizierungsdaten für diesen Account in der SIP-TK-Anlage entgegen nimmt.

**SNMP-ID:** 2.33.4.2.1.13

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

**Mögliche Werte Telnet:**

- max. 63 Zeichen

**Default:** leer

Dieses Feld kann frei bleiben, sofern der SIP-Provider keine speziellen Angaben macht. Die Adresse des Registrars wird dann über den Realm aufgelöst.

#### 2.33.4.2.1.14 Lokale-Portnummer

Dies ist der Port des LANCOM-Proxies zur Kommunikation mit der übergeordneten SIP-TK-Anlage.

**SNMP-ID:** 2.33.4.2.1.14

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

**Mögliche Werte Telnet:**

- 1 bis 65536

**Default:** 0

**Besondere Werte:** 0: Dynamische Portauswahl, der Port wird automatisch aus dem Pool der freien Portnummern gewählt.

Wenn die (Re-)Registrierung der Leitung deaktiviert ist, muss der lokale Port fest vorgegeben und als Zielport auch in der SIP-TK-Anlage eingetragen werden, damit sich beide Seiten SIP-Signalisierungen senden können.

#### 2.33.4.2.1.15 (Re-)Registrierung

Hiermit wird die (wiederholte) Registrierung der SIP-PBX-Leitung aktiviert. Die Registrierung kann auch zur Leitungsüberwachung herangezogen werden.

**SNMP-ID:** 2.33.4.2.1.15

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

**Mögliche Werte Telnet:**

- Ja
- Nein

**Default:** Ja

Für die Nutzung der (Re-)Registrierung muss die Methode der Leitungsüberwachung entsprechend auf "Registrierung" oder "Automatisch" gestellt werden. Die Registrierung wird jeweils nach Ablauf des Überwachungsintervalls wiederholt. Wenn der SIP-Registrar der SIP-TK-Anlage ein anderes Intervall vorschlägt, wird dieses automatisch übernommen.

#### 2.33.4.2.1.16 Leitungsüberwachung

Spezifiziert die Methode der Leitungsüberwachung. Die Leitungsüberwachung prüft die Verfügbarkeit einer SIP-PBX-Leitung. Der Status der Überwachung kann im Call Router zum Wechsel auf eine Backup-Leitung herangezogen werden. Die Überwachungsmethode legt fest, wie der Status geprüft wird.

**SNMP-ID:** 2.33.4.2.1.16

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

**Mögliche Werte Telnet:**

- Auto: Die Methode wird automatisch ermittelt.
- Deaktiviert: Keine Überwachung, die Leitung wird stets als verfügbar gemeldet. In dieser Einstellung kann die tatsächliche Verfügbarkeit der Leitung nicht überwacht werden.
- Register: Überwachung mittels Register-Requests während des Registrierungsvorgangs. Für die Nutzung dieser Einstellung muss für diese Leitung ebenfalls die "(Re-)Registrierung" aktiviert sein.
- Options: Überwachung mittels Options-Requests. Dabei wird wie bei einem Polling regelmäßig eine Anfrage an die Gegenstelle verschickt, je nach Antwort wird die Leitung als verfügbar oder nicht verfügbar angesehen. Diese Einstellung eignet sich z. B. für registrierungslose Leitungen.

**Default:** Auto

#### 2.33.4.2.1.17 Überwachungsintervall

Das Intervall der Leitungsüberwachung in Sekunden. Dieser Wert wirkt sich sowohl auf die Leitungsüberwachung mit Register-Request als auch mit Option-Request aus. Das Überwachungsintervall muss mindestens 60 Sekunden betragen und legt fest, nach welcher Zeit die Überwachungsmethode erneut angewendet wird. Wenn die (Re-)Registrierung aktiviert ist, wird das Überwachungsintervall auch als Zeitraum bis zur nächsten Registrierung verwendet.

**SNMP-ID:** 2.33.4.2.1.17

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

**Mögliche Werte Telnet:**

- max. 5 Ziffern

**Default:** 60

**Besondere Werte:** Werte kleiner als 60 Sekunden werden automatisch als 60 Sekunden angenommen.

Falls die Gegenstelle in der Antwort auf einen Option-Request einen anderen Wert für das Überwachungsintervall vorschlägt, so wird dieser akzeptiert und in der Folgezeit verwendet.

#### 2.33.4.2.1.18 Vertrauenswürdig

Spezifiziert die Zugehörigkeit der Gegenstelle dieser Leitung (Provider) zur "Trusted-Area". In dieser vertrauenswürdigen Zone wird die Caller ID als Information über den Gesprächsteilnehmer nicht entfernt, selbst wenn das durch Einstellungen in der Leitung (CLIR) oder durch das Endgerät gewünscht ist. Bei einer Verbindung über eine vertrauenswürdige Leitung wird die Caller ID entsprechend der ausgewählten Privacy-Methode übertragen und erst in der letzten Vermittlungsstelle vor dem entfernten Gesprächsteilnehmer entfernt. Innerhalb der vertrauenswürdigen Zone kann so z. B. die Caller ID für Abrechnungszwecke ausgewertet werden. Diese Funktion ist u. a. für Provider interessant, die mit einem VoIP-Router direkt beim Kunden das von ihnen selbst verwaltete Netzwerk bis zum Anschluss der VoIP-Endgeräte ausdehnen.

**SNMP-ID:** 2.33.4.2.1.18

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

**Mögliche Werte Telnet:**

- Ja: Vertrauenswürdig
- Nein: Nicht vertrauenswürdig

**Default:** Ja

Bitte beachten sie, dass diese Funktion nicht von allen Providern unterstützt wird.

#### 2.33.4.2.1.19 Privacy-Methode

Spezifiziert die verwendete Methode zur Übermittlung der Caller ID im separaten SIP-Header-Feld.

**SNMP-ID:** 2.33.4.2.1.19

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

**Mögliche Werte Telnet:**

- Keine
- RFC3325: mittels P-Preferred-Id/P-Asserted-Id
- IETF-Draft-Sip-Privacy-04: mittels RPID (Remote Party ID)

**Default:** Keine

#### 2.33.4.2.1.2 Domain

SIP-Domäne/Realm der übergeordneten SIP-TK-Anlage.

**SNMP-ID:** 2.33.4.2.1.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

#### 2.33.4.2.1.3 Port

TCP/UDP-Port der übergeordneten SIP-TK-Anlage, an den die SIP-Pakete vom LANCOM aus gesendet werden.

**SNMP-ID:** 2.33.4.2.1.3

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

**Mögliche Werte Telnet:**

- Beliebieger freier TCP/IP-Port.

**Default:** 5060

In der Firewall muss dieser Port freigeschaltet sein, damit die Verbindung funktionieren kann.

#### 2.33.4.2.1.4 Secret

Gemeinsames Passwort zum Anmelden an der SIP-TK-Anlage. Dieses Passwort wird nur benötigt, wenn sich SIP-Teilnehmer an der TK-Anlage anmelden sollen, die nicht als SIP-Benutzer mit eigenen Zugangsdaten in der Liste der SIP-Benutzer angelegt sind, oder keine lokale Authentifizierung erzwungen wird, so dass sich SIP-Benutzer ohne Passwort am LANCOM anmelden können, aber mit einem gemeinsamen Passwort bei der übergeordneten SIP-TK-Anlage angemeldet werden, wenn die Domäne der SIP-Benutzer mit der Domäne der SIP-PBX-Line übereinstimmt.

**SNMP-ID:** 2.33.4.2.1.4

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

#### 2.33.4.2.1.5 Outb-proxy

Ein SIP-Proxy nimmt Anfragen von SIP-Clients entgegen und agiert für, die Dauer des Verbindungsaufbaus als Stellvertreter (Proxy).

**SNMP-ID:** 2.33.4.2.1.5

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

Dieses Feld kann frei bleiben, sofern der SIP-Provider keine speziellen Angaben macht. Die Adresse des Proxies wird dann über den Realm aufgelöst.

#### 2.33.4.2.1.6 Active

Aktiviert oder deaktiviert den Eintrag.

**SNMP-ID:** 2.33.4.2.1.6

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

**Mögliche Werte Telnet:**

- Ein
- Aus

**Default:** Ein

#### 2.33.4.2.1.7 Kommentar

Kommentar zu diesem Eintrag

**SNMP-ID:** 2.33.4.2.1.7

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

#### 2.33.4.2.1.8 Cln-Prefix

Das Anruf-Präfix ist eine Nummer, die den Anrufer-Nummern (CLI; SIP „From:“) aller ankommenden Anrufe auf dieser SIP-PBX-Leitung vorangestellt wird, um eindeutige Rückruf-Nummern zu erzeugen.

Beispielsweise kann hier eine Nummer ergänzt werden, die im Call-Router bei abgehenden Rufen (dem Rückruf) zur Leitungsauswahl ausgewertet und wieder entfernt wird.

**SNMP-ID:** 2.33.4.2.1.8

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

**Mögliche Werte Telnet:**

- max. 9 Ziffern

**Default:** leer

#### 2.33.4.2.1.9 Line-Prefix

Bei ausgehenden Anrufen über diese Leitung wird der angerufenen Rufnummer dieses Präfix vorangestellt, um eine vollständige für diese Leitung gültige Rufnummer zu erzeugen. Bei ankommenden Rufen wird dieses Präfix entfernt, falls vorhanden.

**SNMP-ID:** 2.33.4.2.1.9

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

**Mögliche Werte Telnet:**

- max. 9 Ziffern

**Default:** leer

### 2.33.4.3 ISDN

Über diese Leitungen werden die ISDN-Anschlüsse konfiguriert. Dazu wird neben der zu verwendenden physikalische ISDN-Leitung auch eine Rufnummernumsetzung konfiguriert. Diese sorgt für eine Umsetzung der internen Rufnummer oder SIP-URL auf eine externe ISDN-Nummer.

**SNMP-ID:** 2.33.4.3

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line

#### 2.33.4.3.1 Interfaces

Hier werden die Leitungen zu ISDN-Vermittlungsstellen oder TK-Anlagen konfiguriert (Router ist Endgerät).

**SNMP-ID:** 2.33.4.3.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/ISDN

#### 2.33.4.3.1.1 Name

Dieser Name identifiziert die Leitung eindeutig. Er darf keiner weiteren Leitung zugeordnet werden.

**SNMP-ID:** 2.33.4.3.1.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/ISDN/Interfaces

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

Tragen Sie hier z. B. die Rufnummer einer Gruppe ein, die jeden eingehenden Anruf erhält und steuern Sie darüber flexibel, welche Telefone bei Rufen klingeln oder leiten Sie den Ruf nach einer Zeit auf eine Mobilnummer oder den Anrufbeantworter um.

#### 2.33.4.3.1.2 Ifc

Interface, an das die ISDN-Teilnehmer angeschlossen sind.

**SNMP-ID:** 2.33.4.3.1.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/ISDN/Interfaces

**Mögliche Werte Telnet:**

- Alle verfügbaren ISDN-Schnittstellen.

**Default:** Modellabhängig.

#### 2.33.4.3.1.3 Domain

Domäne, unter der die Anrufe von / zu der ISDN-Leitung in der SIP-Welt des LANCOM verwaltet werden.

**SNMP-ID:** 2.33.4.3.1.3

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/ISDN/Interfaces

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

#### 2.33.4.3.1.4 Cln-Prefix

Das Anruf-Präfix wird den Anrufer-Nummern (CLI) aller ankommenden Anrufe vorangestellt, um eine eindeutige Rückrufnummer zu erzeugen.

**SNMP-ID:** 2.33.4.3.1.4

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/ISDN/Interfaces

**Mögliche Werte Telnet:**

- max. 9 Ziffern

**Default:** leer

#### 2.33.4.3.1.5 Active

Aktiviert oder deaktiviert den Eintrag.

**SNMP-ID:** 2.33.4.3.1.5

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/ISDN/Interfaces

**Mögliche Werte Telnet:**

- Ein
- Aus

**Default:** Ein

#### 2.33.4.3.1.6 Kommentar

Kommentar zu diesem Eintrag

**SNMP-ID:** 2.33.4.3.1.6

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/ISDN/Interfaces

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

### 2.33.4.3.2 Mapping

Mit dem ISDN-Mapping wird eine Zuordnung von externen ISDN-Rufnummern (MSN oder DDI) zu den intern verwendeten Rufnummern vorgenommen. Es können bis zu 64 Rufnummernzuordnungen eingetragen werden.

**SNMP-ID:** 2.33.4.3.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/ISDN

#### 2.33.4.3.2.1 MSN/DDI

Externe Telefonnummer des Anschlusses im ISDN-Netz.

Für ankommende Rufe, die an diese Nummer gerichtet sind, wird die zugehörige interne Rufnummer als Zielnummer eingetragen. Für ausgehende Rufe wird diese Nummer als eigene Nummer des Anrufenden eingetragen, wenn dies nicht unterdrückt ist.

MSN: Nummer des Telefonanschluss

DDI (Direct Dialing in): Durchwahlnummer des Telefons, wenn der Anschluss als Anlagenanschluss konfiguriert ist.

**SNMP-ID:** 2.33.4.3.2.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/ISDN/Mapping

**Mögliche Werte Telnet:**

- max. 19 Ziffern

**Default:** leer

Mit dem #-Zeichen als Platzhalter können ganze Gruppen von Rufnummern z. B. bei der Verwendung von Durchwahlnummern in einem einzigen Eintrag erfasst werden.

#### 2.33.4.3.2.2 Ifc

ISDN-Schnittstelle(n), über die Endgeräte an den LANCOM VoIP Router angeschlossen sind. Diese Leitungen müssen als ISDN-NT konfiguriert sein.

**SNMP-ID:** 2.33.4.3.2.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/ISDN/Mapping

**Mögliche Werte Telnet:**

- Alle verfügbaren ISDN-Schnittstellen.

**Default:** Modellabhängig.

#### 2.33.4.3.2.3 Number/Name

Interne Telefonnummer des ISDN-Telefons oder Name des Benutzers (SIP-URL).

Für ankommende Rufe ist das der SIP-Name oder interne Telefonnummer des Telefons, an das der Ruf von diesem Interface mit der zugehörigen MSN/DDI vermittelt wird. Für ausgehende Rufe wird der SIP-Name durch die MSN/DDI des zugehörigen Eintrages ersetzt.

**SNMP-ID:** 2.33.4.3.2.3

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/ISDN/Mapping

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

Mit dem #-Zeichen als Platzhalter können ganze Gruppen von Rufnummern z. B. bei der Verwendung von Durchwahlnummern in einem einzigen Eintrag erfasst werden.

#### 2.33.4.3.2.4 CLIR

Anzeige der eigenen Rufnummer wird beim angerufenen Teilnehmer unterdrückt.

**SNMP-ID:** 2.33.4.3.2.4

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/ISDN/Mapping

**Mögliche Werte Telnet:**

- Ja
- Nein

**Default:** Nein

#### 2.33.4.3.2.5 Active

Aktiviert oder deaktiviert den Eintrag.

**SNMP-ID:** 2.33.4.3.2.5

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/ISDN/Mapping

**Mögliche Werte Telnet:**

- Ein
- Aus

**Default:** Ein

#### 2.33.4.3.2.6 Comment

Kommentar zu diesem Eintrag

**SNMP-ID:** 2.33.4.3.2.6

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/ISDN/Mapping

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

### 2.33.4.4 Predef-Dest.

Tabelle mit den vordefinierten Sonderfunktionen für die Ziel-Leitungen in den Call-Routing-Einträgen.

**SNMP-ID:** 2.33.4.4

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line

#### 2.33.4.4.1 Name

Vordefinierte Sonderfunktionen für die Ziel-Leitungen in den Call-Routing-Einträgen.

**SNMP-ID:** 2.33.4.4.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/Predef-Dest.

**Mögliche Werte Telnet:**

- REJECT markiert eine gesperrte Rufnummer.
- USER leitet den Ruf an lokale SIP- bzw. Analog- oder ISDN-Teilnehmer weiter.
- RESTART beginnt mit der zuvor gebildeten „Nummer/Name“ einen neuen Durchlauf in der Call-Routing-Tabelle. Dabei wird zuvor „Quell-Leitung“ gelöscht.

**Default:** REJECT

USER

RESTART

### 2.33.4.5 Source-Filters

Tabelle mit den vordefinierten Quell-Leitungen zum Filtern auf Anrufe von lokalen Benutzern.

**SNMP-ID:** 2.33.4.5

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line

#### 2.33.4.5.1 Name

Vordefinierte Quell-Leitungen zum Filtern auf Anrufe von lokalen Benutzern.

**SNMP-ID:** 2.33.4.5.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/Source-Filters

**Mögliche Werte Telnet:**

- USER.ANALOG für Rufe eines lokalen, analogen Teilnehmers
- USER.ISDN für Rufe eines lokalen ISDN-Teilnehmers
- USER.SIP für Rufe eines lokalen SIP-Teilnehmers
- USER# für Rufe eines lokalen Teilnehmers allgemein

**Default:** USER.ANALOG

USER.ISDN

USER.SIP

USER#

### 2.33.4.6 Analog

Über diese Leitungen werden die analogen Anschlüsse konfiguriert. Dazu wird neben der zu verwendenden physikalische analogen Leitung auch eine Rufnummernumsetzung konfiguriert.

**SNMP-ID:** 2.33.4.6

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line

#### 2.33.4.6.1 Interfaces

Hier werden die Leitungen zu analogen Vermittlungsstellen (Amts-Leitung) oder TK-Anlagen konfiguriert (Router ist Endgerät).

**SNMP-ID:** 2.33.4.6.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/Analog

#### 2.33.4.6.1.1 Name

Name der Leitung, darf nicht identisch sein mit einer anderen in dem Gerät konfigurierten Leitung.

**SNMP-ID:** 2.33.4.6.1.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/Analog/Interfaces

**Mögliche Werte Telnet:**

- ANALOG

**Default:** ANALOG

#### 2.33.4.6.1.10 Caller-ID Transmission Requirements

Neben der Auswahl des Modulationsverfahrens ist bei der Übertragung der Caller ID auch die zeitliche Steuerung der Signalisierung auf analogen Leitungen je nach Land und Anbieter unterschiedlich geregelt. Damit das gerufene Endgerät die Caller ID zum richtigen Zeitpunkt erwartet, wird das vom Anbieter genutzte Verfahren entsprechend eingestellt.

**SNMP-ID:** 2.33.4.6.1.10

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/Analog/Interfaces

**Mögliche Werte Telnet:**

- Default: In dieser Einstellung werden die Standardwerte für das Land verwendet
- in dem das Gerät eingesetzt wird.
- During-Ringing: Die Caller ID wird während des Klingel-Vorgangs übertragen
- und zwar zwischen dem ersten und zweiten Klingelton.
- RP-AS: Die Übertragung der Caller ID ist zeitlich nicht mit dem Klingeln verbunden
- sondern wird durch ein spezielles "Alarmsignal" angekündigt. Dieses Alarmsignal wird durch Klingelimpulse dargestellt (Ringing Pulse Alerting Signal
- RP-AS). Nach dem Klingelimpuls kann die Caller ID übertragen werden.
- Line-Reversal: Die Übertragung der Caller ID ist zeitlich nicht mit dem Klingeln verbunden
- sondern wird durch ein spezielles "Alarmsignal" angekündigt. Das Alarmsignal wird durch das kurzzeitige Vertauschen der Polarität auf der Leitung dargestellt (Line Reversal). Nach dem Line Reversal kann die Caller ID übertragen werden.

**Default:** Länderspezifische Default-Werte:

Österreich: During-Ringing

Belgien: Ringing Pulse Alerting Signal, RP-AS

Frankreich: During-Ringing

Italien: During-Ringing

Schweiz: During-Ringing

Niederlande: Line-Reversal

Spanien: Ringing Pulse Alerting Signal, RP-AS

United Kingdom: Line-Reversal

Deutschland: During-Ringing

#### 2.33.4.6.1.2 Domain

Domänen-Name der Analog-Leitung, der für die Adressierung in SIP verwendet wird.

**SNMP-ID:** 2.33.4.6.1.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/Analog/Interfaces

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

#### 2.33.4.6.1.3 Cln-Prefix

Das Anruf-Präfix ist eine Nummer, die den Anrufer-Nummern (CLI; SIP „From:") aller ankommenden Anrufe auf dieser Analog-Leitung vorangestellt wird, um eindeutige Rückruf-Nummern zu erzeugen.

Beispielsweise kann hier eine Nummer ergänzt werden, die im Call-Router bei abgehenden Rufen (dem Rückruf) zur Leitungsauswahl ausgewertet und wieder entfernt wird.

**SNMP-ID:** 2.33.4.6.1.3

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/Analog/Interfaces

**Mögliche Werte Telnet:**

- max. 9 Ziffern

**Default:** leer

#### 2.33.4.6.1.4 Number/Name

Interne Rufnummer/SIP-URI, den jeder Anruf auf diese Analog-Leitung als Rufziel erhält. Diese Rufnummer kann sich von der tatsächlichen Rufnummer des Telefonie-Anbieters für den analogen Leitungs-Anschluss unterscheiden (Mapping).

**SNMP-ID:** 2.33.4.6.1.4

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/Analog/Interfaces

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

#### 2.33.4.6.1.5 Active

Aktiviert oder deaktiviert den Eintrag.

**SNMP-ID:** 2.33.4.6.1.5

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/Analog/Interfaces

**Mögliche Werte Telnet:**

- Ein
- Aus

**Default:** Ein

#### 2.33.4.6.1.6 Kommentar

Kommentar zu diesem Eintrag

**SNMP-ID:** 2.33.4.6.1.6

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/Analog/Interfaces

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

#### 2.33.4.6.1.7 Line-type

Der Line Type stellt eine vereinfachtes Modell einer analogen Leitung dar.

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/Analog/Interfaces/Line-type

**Mögliche Werte:**

- Default
- EIA0
- EIA1
- EIA2
- EIA3

- EIA4
- EIA5
- EIA6
- EIA7

**Default:** Default

Die Einstellungen für den Line-Type werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diesen Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

#### 2.33.4.6.1.8 Central Office-Termination

Die Central Office Termination ist der komplexe Abschlusswiderstand, mit dem die Vermittlungsstelle Leitung abschließt. Dieser ist länderabhängig.

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/Analog/Interfaces/Central Office-Termination .

**Mögliche Werte:**

- Default
- 220Ohm+820Ohm|115nF
- 200Ohm+560Ohm|100nF
- 270Ohm+750Ohm|150nF
- 370Ohm+620Ohm|310nF
- 220Ohm+120Ohm|115nF
- 600Ohm
- 220Ohm+82Ohm|120nF
- 300Ohm+1000Ohm|220nF
- 600Ohm+1.5uF
- 150Ohm+510Ohm|47nF
- 1200Ohm+376Ohm|112nF

**Default:** Default

Die Einstellungen für die Central Office Termination werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diesen Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

#### 2.33.4.6.1.9 Caller-ID Signaling

Die Anbieter von analogen Telefonanschlüssen unterstützen unterschiedliche Dienstmerkmale, zu denen auch die Übertragung der Caller ID, also die Anzeige des anrufenden Teilnehmers auf dem Display des gerufenen Endgerätes gehört. Dieser Dienst ist auch als Calling Line Identification Presentation (CLIP) bekannt. Die Caller ID wird je nach Land und Anbieter durch zwei verschiedene Modulationsverfahren über die analoge Verbindung übertragen (FSK oder DTMF).

**SNMP-ID:** 2.33.4.6.1.9

**Pfad Telnet:** /Setup/Voice-Call-Manager/Line/Analog/Interfaces

**Mögliche Werte Telnet:**

- Default: In dieser Einstellung werden die Standardwerte für das Land verwendet
- in dem das Gerät eingesetzt wird.
- FSK: Übertragung der Caller ID mit dem FSK-Verfahren (Frequency Shift Keying)
- DTMF: Übertragung der Caller ID mit dem DMTF-Verfahren (Dual Tone Multi Frequency)

**Default:** Länderspezifische Default-Werte:

Niederlande: DTMF

Alle anderen Länder: V.23 (FSK)

## 2.33.5 Call-Router

Dieses Menü enthält die Call-Router-Einstellungen für den Voice-Call-Manager.

**SNMP-ID:** 2.33.5

**Pfad Telnet:** /Setup/Voice-Call-Manager

### 2.33.5.1 Call-Routing

Hier können Sie Regeln definieren, um Rufe zu bestimmten Rufzielen oder Leitungen umzuleiten oder abzulehnen.

**SNMP-ID:** 2.33.5.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/Call-Router

#### 2.33.5.1.1 Called-Id

Der gewählte Called Party Name bzw. die Ziel-Rufnummer (ohne Domänen-Angabe).

**SNMP-ID:** 2.33.5.1.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/Call-Router/Call-Routing

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

**Besondere Werte:** Das #-Zeichen wird als Platzhalter für beliebige Zeichenfolgen verwendet. Alle Zeichen vor dem # werden entfernt, die restlichen Zeichen werden im Feld „Nummer/Name“ anstelle der #-Zeichens für den weiteren Verbindungsaufbau verwendet.

Beispiel: In der Call-Routing-Tabelle enthält ein Eintrag die '00049#' als gerufene Nummer/Name und die '00#' als Nummer/Name. Bei allen Rufen mit einer führenden Null für die Amtsholung und der kompletten Vorwahl für Deutschland wird als Nummer/Name nur die führende Null für die Amtsholung und die führende Null für die Ortsnetzvorwahl beibehalten, die Landeskennung wird entfernt. Aus '00049 2405 123456' wird also die '0 02405 123456'.

#### 2.33.5.1.10 Kommentar

Kommentar zu diesem Eintrag

**SNMP-ID:** 2.33.5.1.10

**Pfad Telnet:** /Setup/Voice-Call-Manager/Call-Router/Call-Routing

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

#### 2.33.5.1.11 Dest-Id-2

Diese Rufnummer wird für den weiteren Verbindungsaufbau verwendet, wenn unter „Nummer/Name“ nichts eingetragen ist oder die zugehörige „Leitung“ nicht erreichbar ist. Kann über diese 2. Rufnummer und die zugehörige 2. Leitung keine Verbindung hergestellt werden, werden die 3. Rufnummer und die 3. Leitung verwendet.

**SNMP-ID:** 2.33.5.1.11

**Pfad Telnet:** /Setup/Voice-Call-Manager/Call-Router/Call-Routing

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

#### 2.33.5.1.12 Dest-Line-2

Über diese Leitung wird die Verbindung aufgebaut, wenn die 2. Rufnummer für den Verbindungsaufbau verwendet wird. Hier können die gleichen Leitungen ausgewählt werden wir bei „Leitung".

**SNMP-ID:** 2.33.5.1.12

**Pfad Telnet:** /Setup/Voice-Call-Manager/Call-Router/Call-Routing

**Mögliche Werte Telnet:**

- Analog
- ISDN
- Alle definierten SIP Leitungen.
- Folgende Sonderfunktionen können als Ziel-Leitung eingetragen werden:
- REJECT markiert eine gesperrte Rufnummer.
- USER leitet den Ruf an lokale SIP- bzw. Analog- oder ISDN-Teilnehmer weiter.
- RESTART beginnt mit der zuvor gebildeten „Nummer/Name" einen neuen Durchlauf in der Call-Routing-Tabelle. Dabei wird zuvor „Quell-Leitung" gelöscht.

**Default:** leer

#### 2.33.5.1.13 Dest-Id-3

Bedeutung analog zu 2. Nummer.

**SNMP-ID:** 2.33.5.1.13

**Pfad Telnet:** /Setup/Voice-Call-Manager/Call-Router/Call-Routing

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

#### 2.33.5.1.14 Dest-Line-3

Bedeutung analog zu 2. Leitung.

**SNMP-ID:** 2.33.5.1.14

**Pfad Telnet:** /Setup/Voice-Call-Manager/Call-Router/Call-Routing

**Mögliche Werte Telnet:**

- Analog
- ISDN
- Alle definierten SIP Leitungen.
- Folgende Sonderfunktionen können als Ziel-Leitung eingetragen werden:
- REJECT markiert eine gesperrte Rufnummer.
- USER leitet den Ruf an lokale SIP- bzw. Analog- oder ISDN-Teilnehmer weiter.
- RESTART beginnt mit der zuvor gebildeten „Nummer/Name" einen neuen Durchlauf in der Call-Routing-Tabelle. Dabei wird zuvor „Quell-Leitung" gelöscht.

**Default:** leer

#### 2.33.5.1.15 Prio

Der Call-Manager sortiert alle Einträge mit gleicher Priorität automatisch so, dass die Tabelle sinnvoll von oben nach unten durchlaufen werden kann. Bei einigen Einträgen muss jedoch (z. B. zur Rufnummernumsetzung) die Reihenfolge der Einträge vorgegeben werden. Die Einträge mit der höchsten Priorität werden automatisch nach oben sortiert.

**SNMP-ID:** 2.33.5.1.15

**Pfad Telnet:** /Setup/Voice-Call-Manager/Call-Router/Call-Routing

**Mögliche Werte Telnet:**

- 0 bis 999

**Default:** 0

#### 2.33.5.1.2 Cld-Domain

Dieser Eintrag filtert auf die gerufene Domäne, die „Called Party Domain“. Der Call-Router-Eintrag wird nur dann als übereinstimmend gewertet, wenn die Called Party Domain des anliegenden Rufes mit der hier eingetragenen Domain übereinstimmt. Wird hier nichts angegeben, wird jede Zieldomäne akzeptiert.

**SNMP-ID:** 2.33.5.1.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/Call-Router/Call-Routing

**Mögliche Werte Telnet:**

- Analog
- ISDN
- Die interne VoIP-Domäne des LANCOM VoIP Router.
- Alle bei den SIP- und SIP-PBX-Leitungen eingetragenen Domänen.

**Default:** leer

#### 2.33.5.1.3 Calling-Id

Dieser Eintrag filtert auf die rufende Nummer/Name, die „Calling Party ID“. Die Angabe erfolgt entweder als interne Nummer, nationale oder internationale Rufnummer. Die Domäne wird nicht mit angegeben. Es wird keine „0“ oder anderes Zeichen für eine Leitungskennung vorangestellt, die ID wird wie von der Leitung bzw. wie von internen Rufen kommend verwendet.

Der Call-Router-Eintrag wird nur dann als übereinstimmend gewertet, wenn die Calling Party ID des anliegenden Rufes mit der hier eingetragenen Nummer übereinstimmt. Ab einem „#“ können beliebige Ziffern akzeptiert werden.

**SNMP-ID:** 2.33.5.1.3

**Pfad Telnet:** /Setup/Voice-Call-Manager/Call-Router/Call-Routing

**Mögliche Werte Telnet:**

- interne Nummer
- nationale
- internationale Rufnummer.
- LOCAL schränkt auf interne Rufnummern ein (ohne führende „0“).
- EMPTY kann für nicht angegebene Calling Party IDs verwendet werden.

**Default:** leer

Wird hier nichts angegeben, wird jede Calling Party ID akzeptiert.

#### 2.33.5.1.4 Cln-Domain

Dieser Eintrag filtert auf die rufende Domäne, die „Calling Domain". Der Call-Router-Eintrag wird nur dann als übereinstimmend gewertet, wenn die Calling Domain des anliegenden Rufes mit der hier eingetragenen Domain übereinstimmt. Wird hier nichts angegeben, wird jede rufende Domäne akzeptiert.

**SNMP-ID:** 2.33.5.1.4

**Pfad Telnet:** /Setup/Voice-Call-Manager/Call-Router/Call-Routing

**Mögliche Werte Telnet:**

- Analog
- ISDN
- Die interne VoIP-Domäne des LANCOM VoIP Router.
- Alle bei den SIP- und SIP-PBX-Leitungen eingetragenen Domänen.

**Default:** leer

SIP-Telefone verfügen üblicherweise über mehrere Leitungstasten, für die verschiedene Domänen konfiguriert werden können. Mit diesem Filter kann der Auswahl entsprechend eine bestimmte Behandlung der Rufe über unterschiedliche Leitungstasten vorgenommen werden.

#### 2.33.5.1.5 Src-Line

Dieser Eintrag filtert auf die Quell-Leitung. Der Call-Router-Eintrag wird nur dann als übereinstimmend gewertet, wenn die Quell-Leitung des anliegenden Rufes mit der hier eingetragenen Leitung übereinstimmt. Wird hier nichts angegeben, wird jede rufende Leitung akzeptiert.

**SNMP-ID:** 2.33.5.1.5

**Pfad Telnet:** /Setup/Voice-Call-Manager/Call-Router/Call-Routing

**Mögliche Werte Telnet:**

- USER.ANALOG für Rufe eines lokalen, analogen Teilnehmers
- USER.ISDN für Rufe eines lokalen ISDN-Teilnehmers
- USER.SIP für Rufe eines lokalen SIP-Teilnehmers
- USER# für Rufe eines lokalen Teilnehmers allgemein
- Alle eingetragenen ISDN,- SIP- und SIP-PBX-Leitungen.

**Default:** leer

#### 2.33.5.1.7 Dest-Id-1

Diese Rufnummer wird für den weiteren Verbindungsaufbau verwendet. Kann über diese Rufnummer und die zugehörige Leitung keine Verbindung hergestellt werden, werden die Backup-Rufnummern mit den zugehörigen Leitungen verwendet.

**SNMP-ID:** 2.33.5.1.7

**Pfad Telnet:** /Setup/Voice-Call-Manager/Call-Router/Call-Routing

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

Mindestens eines der „Nummer/Name", „1. Backup-Nr." oder „2.Backup-Nr." muss einen Inhalt haben. Die Auswertung erfolgt in dieser Reihenfolge. Ein leeres Feld wird übersprungen.

#### 2.33.5.1.8 Dest-Line-1

Über die Zielleitung wird die Verbindung aufgebaut.

ISDN

Alle definierten SIP Leitungen.

Folgende Sonderfunktionen können als Ziel-Leitung eingetragen werden:

REJECT markiert eine gesperrte Rufnummer.

USER leitet den Ruf an lokale SIP- bzw. ISDN-Teilnehmer weiter.

RESTART beginnt mit der zuvor gebildeten „Nummer/Name“ einen neuen Durchlauf in der Call-Routing-Tabelle. Dabei wird zuvor „Quell-Leitung“ gelöscht.

**SNMP-ID:** 2.33.5.1.8

**Pfad Telnet:** /Setup/Voice-Call-Manager/Call-Router/Call-Routing

**Mögliche Werte Telnet:**

- Analog
- ISDN
- Alle definierten SIP Leitungen.
- Folgende Sonderfunktionen können als Ziel-Leitung eingetragen werden:
- REJECT markiert eine gesperrte Rufnummer.
- USER leitet den Ruf an lokale SIP- bzw. Analog- oder ISDN-Teilnehmer weiter.
- RESTART beginnt mit der zuvor gebildeten „Nummer/Name“ einen neuen Durchlauf in der Call-Routing-Tabelle. Dabei wird zuvor „Quell-Leitung“ gelöscht.

**Default:** leer

Dieses Feld muss ausgefüllt werden, sonst wird der Eintrag nicht verwendet!

#### 2.33.5.1.9 Active

Der Routingeintrag kann aktiviert, deaktiviert oder aber als Default-Eintrag gekennzeichnet werden. Alle über die ersten Durchläufe nicht über die Call-Routing-Tabelle bzw. lokale Teilnehmertabelle auflösbaren Anrufe werden dann automatisch über diese Default-Einträge aufgelöst. Zielname und Zieldomain sind dann beliebig, nur die ggf. gesetzten Quellfilter werden berücksichtigt.

**SNMP-ID:** 2.33.5.1.9

**Pfad Telnet:** /Setup/Voice-Call-Manager/Call-Router/Call-Routing

**Mögliche Werte Telnet:**

- Aktiv
- Inaktiv
- Standard-Leitung

**Default:** Aktiv

## 2.33.7 Groups

Dieses Menü enthält die Benutzergruppen-Einstellungen für den Voice-Call-Manager.

**SNMP-ID:** 2.33.7

**Pfad Telnet:** /Setup/Voice-Call-Manager

### 2.33.7.1 Groups

Hier können Gruppen definiert werden, die eine automatische Verteilung eingehender Rufe zu zwei oder mehr Teilnehmern ermöglichen.

**SNMP-ID:** 2.33.7.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/Groups

#### 2.33.7.1.1 Name

Unter dieser Rufnummer bzw. dieser SIP-ID ist die Rufgruppe erreichbar.

**SNMP-ID:** 2.33.7.1.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/Groups/Groups

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

Namen für Rufgruppen dürfen nicht mit Namen von Benutzern (SIP, ISDN oder Analog) übereinstimmen.

#### 2.33.7.1.2 Members

Kommaseparierte Liste der Mitglieder dieser Rufgruppe. Als Mitglieder können Benutzer, Rufgruppen oder auch externe Rufnummern eingetragen werden, so dass eine unbegrenzte Skalierung möglich ist.

**SNMP-ID:** 2.33.7.1.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/Groups/Groups

**Mögliche Werte Telnet:**

- Benutzer
- Rufgruppen
- externe Rufnummern

**Default:** leer

Rufgruppen können sich nicht selbst oder einen Vorgänger in der hierarchischen Struktur enthalten – es sind also keine Rekursionen durch den Eintrag der Mitglieder möglich! Schleifen zu einem Vorgänger in der Struktur sind jedoch über das 'Weiterleitungs-Ziel' möglich.

#### 2.33.7.1.3 Distribution-method

Bestimmt die Art der Ruf-Verteilung.

**SNMP-ID:** 2.33.7.1.3

**Pfad Telnet:** /Setup/Voice-Call-Manager/Groups/Groups

**Mögliche Werte Telnet:**

- Simultan: Der Anruf wird aufgeteilt und an alle Gruppenmitglieder gleichzeitig weitergeleitet. Wenn ein Mitglied den Anruf innerhalb der Weiterleitungs-Zeit annimmt, wird die Anrufsignalisierung für die anderen Mitglieder beendet. Wenn kein Mitglied den Anruf innerhalb der Weiterleitungs-Zeit annimmt, wird der Anruf zum Weiterleitungs-Ziel weitergeleitet.
- Sequentiell: Der Anruf wird der Reihe nach an die Gruppenmitglieder weitergeleitet. Wenn ein Mitglied den Anruf innerhalb der Weiterleitungs-Zeit nicht annimmt, wird der Anruf an das jeweils folgende Mitglied weitergeleitet.

Wenn auch das letzte Gruppenmitglied den Anruf innerhalb der Weiterleitungs-Zeit nicht annimmt, wird der Anruf zum Weiterleitungs-Ziel weitergeleitet.

**Default:** Simultan

#### 2.33.7.1.4 Forwarding-time

Wenn ein anliegender Ruf von einem Gruppenmitglied nicht innerhalb der Weiterleitungs-Zeit angenommen wird, wird der Ruf je nach Art der Ruf-Verteilung weitergeleitet:

Bei simultaner Ruf-Verteilung wird der Anruf zum Weiterleitungs-Ziel weitergeleitet.

Bei sequentieller Ruf-Verteilung wird der Anruf an das nächste Gruppenmitglied in der gültigen Reihenfolge weitergeleitet. Wenn das Gruppenmitglied das letzte Mitglied der Reihenfolge ist, wird der Anruf an das Weiterleitungs-Ziel weitergeleitet.

**SNMP-ID:** 2.33.7.1.4

**Pfad Telnet:** /Setup/Voice-Call-Manager/Groups/Groups

**Mögliche Werte Telnet:**

- max. 255 Sekunden

**Default:** 15

**Besondere Werte:** 0 Sekunden. Der Ruf wird sofort zum Weiterleitungs-Ziel geleitet (temporäres Überspringen einer Rufgruppe in einer Hierarchie).

Sind alle Mitglieder der Gruppe besetzt oder aus anderen Gründen nicht erreichbar, wird der Anruf an das Weiterleitungs-Ziel weitergeleitet, ohne die Weiterleitungs-Zeit abzuwarten.

#### 2.33.7.1.5 Forwarding-target

Wenn keines der Gruppenmitglieder den Anruf innerhalb der Weiterleitungs-Zeit annimmt, wird der Anruf an das hier eingetragene Weiterleitungs-Ziel weitergeleitet. Sowohl Benutzer, Rufgruppen als auch externe Rufnummern können als Weiterleitungs-Ziel eingetragen werden. Es kann dabei nur genau ein Weiterleitungs-Ziel angegeben werden.

**SNMP-ID:** 2.33.7.1.5

**Pfad Telnet:** /Setup/Voice-Call-Manager/Groups/Groups

**Mögliche Werte Telnet:**

- Benutzer
- Rufgruppen
- externe Rufnummern

**Default:** leer

Wenn kein Weiterleitungs-Ziel angegeben wird, wird der Anruf zurückgewiesen, sobald die Liste der Mitglieder abgearbeitet ist bzw. wenn alle Mitglieder besetzt oder nicht erreichbar sind.

Das Weiterleitungs-Ziel wird erst aktiv, wenn die Weiterleitungs-Zeit der Gruppe vollständig abgelaufen ist bzw. kein Mitglied erreichbar ist. Aus diesem Grund sind hier auch Verweise auf eine höhere Stelle einer Rufgruppenstruktur möglich, anders als beim Eintrag der 'Mitglieder'.

#### 2.33.7.1.6 Active

Aktiviert oder deaktiviert den Eintrag.

**SNMP-ID:** 2.33.7.1.6

**Pfad Telnet:** /Setup/Voice-Call-Manager/Groups/Groups

**Mögliche Werte Telnet:**

- Ein
- Aus

**Default:** Ein

#### 2.33.7.1.7 Kommentar

Kommentar zu diesem Eintrag

**SNMP-ID:** 2.33.7.1.7

**Pfad Telnet:** /Setup/Voice-Call-Manager/Groups/Groups

**Mögliche Werte Telnet:**

- max. 64 Zeichen

**Default:** leer

## 2.33.8 Protokollierung

Dieses Menü enthält die Protokollierung-Einstellungen für den Voice-Call-Manager.

**SNMP-ID:** 2.33.8

**Pfad Telnet:** /Setup/Voice-Call-Manager

### 2.33.8.1 Call-Data-Records

Dieses Menü enthält die Protokollierung-Einstellungen für den Voice-Call-Manager.

**SNMP-ID:** 2.33.8.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/Protokollierung

#### 2.33.8.1.2 E-Mail-Adresse

E-Mail-Adresse für den Versand der Nachrichten.

**SNMP-ID:** 2.33.8.1.2

**Pfad Telnet:** /Setup/Voice-Call-Manager/Protokollierung/Call-Data-Records

**Mögliche Werte Telnet:**

- Gültige E-Mail-Adresse

**Default:** leer

#### 2.33.8.1.1 E-Mail-Benachrichtigung

Bei Bedarf können Sie sich per E-Mail über alle Anrufe informieren lassen, die über den LANCOM VoIP Router geführt werden. Für jeden Anruf, der zu einem Verbindungsaufbau führt (intern oder extern, ankommende und abgehende Anrufe) wird dann eine entsprechende Nachricht mit Angabe verschiedener Informationen wie Quell- und Ziel-Rufnummern sowie Start- und Endzeit des Anrufs etc. verschickt.

**SNMP-ID:** 2.33.8.1.1

**Pfad Telnet:** /Setup/Voice-Call-Manager/Protokollierung/Call-Data-Records

**Mögliche Werte Telnet:**

- Ein
- Aus

**Default:** Aus

Zur Nutzung dieser Benachrichtigungen muss ein SMTP-Konto eingerichtet sein.

#### 2.33.8.1.3 Syslog

Bei Bedarf können Sie sich per SYSLOG (Facility: Accounting; Level: Info) über alle Anrufe informieren lassen, die über den LANCOM VoIP Router geführt werden. Für jeden Anruf, der zu einem Verbindungsaufbau führt (intern oder extern, ankommende und abgehende Anrufe) wird dann eine entsprechende Nachricht mit Angabe verschiedener Informationen wie Quell- und Ziel-Rufnummern sowie Start- und Endzeit des Anrufs etc. verschickt.

**SNMP-ID:** 2.33.8.1.3

**Pfad Telnet:** /Setup/Voice-Call-Manager/Protokollierung/Call-Data-Records

**Mögliche Werte Telnet:**

- Ein
- Aus

**Default:** Aus

Zur Nutzung dieser Benachrichtigungen muss ein SYSLOG-Client eingerichtet sein.

## 2.34 Drucker

Dieses Menü enthält die Einstellungen für Drucker.

**SNMP-ID:** 2.34

**Pfad Telnet:** /Setup

## 2.34.1 Drucker

Hier können Sie Einstellungen am Netzwerk-Drucker vornehmen

**SNMP-ID:** 2.34.1

**Pfad Telnet:** /Setup/Drucker

### 2.34.1.1 Drucker

Der Name des Druckers.

**SNMP-ID:** 2.34.1.1

**Pfad Telnet:** /Setup/Drucker/Drucker

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** *

### 2.34.1.2 RawIp-Port

Über diesen Port können Druckaufträge über RawIP angenommen werden.

**SNMP-ID:** 2.34.1.2

**Pfad Telnet:** /Setup/Drucker/Drucker

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 9100

### 2.34.1.3 LPD-Port

Über diesen Port können Druckaufträge über LDP angenommen werden.

**SNMP-ID:** 2.34.1.3

**Pfad Telnet:** /Setup/Drucker/Drucker

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 515

### 2.34.1.4 Aktiv

Aktiviert oder deaktiviert diesen Eintrag.

**SNMP-ID:** 2.34.1.4

**Pfad Telnet:** /Setup/Drucker/Drucker

**Mögliche Werte:**

- Ja: Der Printserver ist aktiv.
- Nein: Der Printserver ist nicht aktiv.

**Default:** Nein

### 2.34.1.5 Bidirektional

Dieser Parameter aktiviert oder deaktiviert den bidirektionalen Modus des Druckers.

**SNMP-ID:** 2.34.1.5

**Pfad Telnet:** /Setup/Drucker/Drucker

Der bidirektionale Modus des Druckers wird nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diesen Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

### 2.34.1.6 Reset-beim-Oeffnen

Wenn diese Option aktiviert ist, sendet das Gerät von dem Öffnen einer Drucker-Session einen Reset-Befehl an den Drucker.

**SNMP-ID:** 2.34.1.6

**Pfad Telnet:** /Setup/Drucker/Drucker

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

Aktivieren Sie diese Option, wenn der Verbindungsaufbau zum Drucker nicht wie erwartet funktioniert.

## 2.34.2 Zugangs-Liste

Legen Sie hier diejenigen Netzwerke fest, die Zugriff auf den Drucker haben.

**SNMP-ID:** 2.34.2

**Pfad Telnet:** /Setup/Drucker

### 2.34.2.1 IP-Adresse

IP-Adresse des Netzwerks, dessen Clients Zugriff auf den Drucker haben dürfen.

**SNMP-ID:** 2.34.2.1

**Pfad Telnet:** /Setup/Drucker/Zugangs-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.34.2.2 IP-Netzmaske

Netzmaske zu den erlaubten Netzwerken.

**SNMP-ID:** 2.34.2.2

**Pfad Telnet:** /Setup/Drucker/Zugangs-Liste

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** 0.0.0.0

### 2.34.2.3 Rtg-Tag

Wenn sie ein Routing-Tag für diese Zugriffs-Regel angeben, so werden nur solche Pakete angenommen, die entweder in der Firewall mit dem gleichen Tag markiert oder über ein Netzwerk mit passendem Schnittstellen-Tag empfangen wurden. Wenn als Routing-Tag 0 angegeben ist, wird jeder Zugriff einer passenden IP-Adresse zugelassen.

**SNMP-ID:** 2.34.2.3

**Pfad Telnet:** /Setup/Drucker/Zugangs-Liste/Rtg-Tag

**Mögliche Werte:**

- max. 5 Zeichen

**Default:** leer

Die Verwendung von Routing-Tags macht folglich nur in Kombination mit entsprechend begleitenden Regeln in der Firewall oder getaggten Netzwerken Sinn.

# 2.35 ECHO-Server

Dieses Menü enthält die Konfiguration des ECHO-Servers.

**SNMP-ID:** 2.35

**Pfad Telnet:** /Setup

## 2.35.1 Aktiv

Der Echo-Server wird für die Überwachung der Leitungsqualität durch Messung von RTT und Jitter benötigt.

**SNMP-ID:** 2.35.1

**Pfad Telnet:** /Setup/ECHO-Server

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

## 2.35.3 TCP-Timeout

Wenn eine zum ECHO-Server aufgebaute TCP-Sitzung 10 (Default) Sekunden inaktiv ist, baut der Server sie wieder ab. Normalerweise räumt TCP selbsttätig "liegengebliebene" Verbindungen ab, aber das dauert deutlich länger.

**SNMP-ID:** 2.35.3

**Pfad Telnet:** /Setup/ECHO-Server

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 10

## 2.35.2 Zugriffstabelle

Diese Tabelle legt die Zugriffsrechte für die Nutzung des ECHO-Servers fest.

**SNMP-ID:** 2.35.2

**Pfad Telnet:** /Setup/ECHO-Server

### 2.35.2.1 IP-Adresse

IP-Adresse der Gegenstelle.

**SNMP-ID:** 2.35.2.1

**Pfad Telnet:** /Setup/ECHO-Server/Zugriffstabelle

**Mögliche Werte:**

- Gültige IP-Adresse.

### 2.35.2.2 Netzmaske

IP-Adresse der Gegenstelle.

**SNMP-ID:** 2.35.2.2

**Pfad Telnet:** /Setup/ECHO-Server/Zugriffstabelle

**Mögliche Werte:**

- Gültige IP-Adresse.

### 2.35.2.3 Protokoll

Für die Messung verwendetes Protokoll.

**SNMP-ID:** 2.35.2.3

**Pfad Telnet:** /Setup/ECHO-Server/Zugriffstabelle

**Mögliche Werte:**

- Kein
- TCP
- UDP
- TCP+UDP

### 2.35.2.4 Aktiv

Aktiviert oder deaktiviert diesen Eintrag der Tabelle.

**SNMP-ID:** 2.35.2.4

**Pfad Telnet:** /Setup/ECHO-Server/Zugriffstabelle

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

### 2.35.2.5 Kommentar

Kommentar zu diesem Eintrag.

**SNMP-ID:** 2.35.2.5

**Pfad Telnet:** /Setup/ECHO-Server/Zugriffstabelle

## 2.36 Performance-Monitoring

Dieses Menü enthält die Konfiguration des Performance-Monitoring.

**SNMP-ID:** 2.36

**Pfad Telnet:** /Setup

## 2.36.2 RttMonAdmin

Diese Tabelle zeigt Informationen über die Art der Messvorgänge.

**SNMP-ID:** 2.36.2

**Pfad Telnet:** /Setup/Performance-Monitoring

### 2.36.2.1 Index

Gemeinsamer Index der Messung

**SNMP-ID:** 2.36.2.1

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonAdmin

### 2.36.2.4 Messungsart

Art der Messung.

**SNMP-ID:** 2.36.2.4

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonAdmin

### 2.36.2.6 Frequenz

Zeit bis zur Wiederholung der Messung in Millisekunden. Kann als einziger Parameter verändert werden, während der Status Actrive ist. Dann ist allerdings nur der Wert 0 erlaubt, mit dem eine weitere Wiederholung unterbunden wird.

**SNMP-ID:** 2.36.2.6

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonAdmin

### 2.36.2.7 Timeout

Timeout einer Messung in Millisekunden. Das Timeout muss kleiner sein, als die Zeit bis zur Messungswiederholung.

**SNMP-ID:** 2.36.2.7

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonAdmin

### 2.36.2.9 Status

Status der Messung.

**SNMP-ID:** 2.36.2.9

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonAdmin

**Mögliche Werte:**

- Active: Messung wird durchgeführt. Dieser Wert kenn nur gesetzt werden, wenn Status den Weret Not_In_Service hat. Solange der Status Active ist, können keine Messparameter geändert werden.
- Not_In_Service: Alle benötigten Parameter sind gesetzt, es wird aktuell keine Messung durchgeführt.
- Not_Ready: Nicht alle benötigten Parameter sind gesetzt.
- Create: Anlegen einer Tabellenzeile. Per SNMP-Set wird eine Tabellenzeile angelegt, indem mit dem gewünschten Index der Status auf Create gesetzt wird. Auch bei der Konfiguration per Menüsystem muß der Status zunächst auf Create gesetzt werden. Wird eine neue Tabellenzeile angelegt, werden automatisch auch die zugehörigen Zeilen in den anderen Tabellen erzeugt.
- Destroy: Löschen einer Tabellenzeile. Ist nur möglich, wenn der Status nicht Active ist. Die zugehörigen Zeilen in den anderen Tabellen werden automatisch mit gelöscht.

## 2.36.3 RttMonEchoAdmin

Diese Tabelle zeigt Informationen über die Messvorgänge.

**SNMP-ID:** 2.36.3

**Pfad Telnet:** /Setup/Performance-Monitoring

### 2.36.3.1 Protokoll

Zu verwendendes Protokoll

**SNMP-ID:** 2.36.3.1

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonEchoAdmin

### 2.36.3.17 Intervall

Zeit zwischen zwei Messpaketen in Millisekunden

**SNMP-ID:** 2.36.3.17

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonEchoAdmin

### 2.36.3.18 Paketzahl

Anzahl Messpakete je Messung

**SNMP-ID:** 2.36.3.18

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonEchoAdmin

### 2.36.3.2 Zieldresse

Adresse des Responders

**SNMP-ID:** 2.36.3.2

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonEchoAdmin

**Mögliche Werte:**

- Gültige IP-Adresse.

### 2.36.3.255 Index

Gemeinsamer Index der Messung

**SNMP-ID:** 2.36.3.255

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonEchoAdmin

### 2.36.3.3 Paketgroese

Länge der Messpakete in Byte. Das Paket wird auf die zur Messung benötigte Mindestgröße vergrößert.

**SNMP-ID:** 2.36.3.3

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonEchoAdmin

### 2.36.3.5 Zielport

Zielport. Wird derzeit ignoriert.

**SNMP-ID:** 2.36.3.5

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonEchoAdmin

## 2.36.4 RttMonStatistics

Diese Tabelle zeigt die Statistik über die beim Performance-Monitoring ermittelten Werte.

**SNMP-ID:** 2.36.4

**Pfad Telnet:** /Setup/Performance-Monitoring

### 2.36.4.10 Jitter-Min-Pos-SD

Minimaler positiver Jitterwert Sender zu Responder in uSec

**SNMP-ID:** 2.36.4.10

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.11 Jitter-Max-Pos-SD

maximaler positiver Jitterwert Sender zu Responder in uSec

**SNMP-ID:** 2.36.4.11

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.12 Jitter-Count-Pos-SD

Anzahl ermittelter positiver Jitterwerte Sender zu Responder

**SNMP-ID:** 2.36.4.12

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.13 Jitter-Sum-Pos-SD

Summe aller positiven Jitterwerte Sender zu Responder in uSec

**SNMP-ID:** 2.36.4.13

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.16 Jitter-Min-Pos-DS

Minimaler positiver Jitterwert Responder zu Sender in uSec

**SNMP-ID:** 2.36.4.16

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.17 Jitter-Max-Pos-DS

maximaler positiver Jitterwert Responder zu Sender in uSec

**SNMP-ID:** 2.36.4.17

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.18 Jitter-Count-Pos-DS

Anzahl ermittelter positiver Jitterwerte Responder zu Sender

**SNMP-ID:** 2.36.4.18

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.19 Jitter-Sum-Pos-DS

Summe aller positiven Jitterwerte Responder zu Sender in uSec

**SNMP-ID:** 2.36.4.19

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.2 Completions

Anzahl durchgeführter Messungen

**SNMP-ID:** 2.36.4.2

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.22 Jitter-Min-Neg-SD

Minimaler negativer Jitterwert Sender zu Responder in uSec, Absolutwert

**SNMP-ID:** 2.36.4.22

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.23 Jitter-Max-Neg-SD

maximaler negativer Jitterwert Sender zu Responder in uSec, Absolutwert

**SNMP-ID:** 2.36.4.23

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.24 Jitter-Count-Neg-SD

Anzahl ermittelter negativer Jitterwerte Sender zu Responder

**SNMP-ID:** 2.36.4.24

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.25 Jitter-Sum-Neg-SD

Summe aller negativen Jitterwerte Sender zu Responder in uSec, Absolutwert

**SNMP-ID:** 2.36.4.25

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.255 Index

Gemeinsamer Index der Messung

**SNMP-ID:** 2.36.4.255

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.28 Jitter-Min-Neg-DS

Minimaler negativer Jitterwert Responder zu Sender in uSec, Absolutwert

**SNMP-ID:** 2.36.4.28

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.29 Jitter-Max-Neg-DS

maximaler negativer Jitterwert Responder zu Sender in uSec, Absolutwert

**SNMP-ID:** 2.36.4.29

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.30 Jitter-Count-Neg-DS

Anzahl ermittelter negativer Jitterwerte Responder zu Sender

**SNMP-ID:** 2.36.4.30

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.31 Jitter-Sum-Neg-DS

Summe aller negativen Jitterwerte Responder zu Sender in uSec, Absolutwert

**SNMP-ID:** 2.36.4.31

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.34 Packet-Loss-SD

Anzahl verlorener Pakete Sender zu Responder

**SNMP-ID:** 2.36.4.34

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.35 Packet-Loss-DS

Anzahl verlorener Pakete Responder zu Sender

**SNMP-ID:** 2.36.4.35

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.4 RTT-Count

Gesamtzahl ermittelter RTT-Werte

**SNMP-ID:** 2.36.4.4

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.5 RTT-Sum

Summe aller ermittelten RTT-Werte

**SNMP-ID:** 2.36.4.5

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.62 Average-Jitter

Durchschnitt aller absoluten Jitterwerte

**SNMP-ID:** 2.36.4.62

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.63 Average-Jitter-SD

Durchschnitt aller absoluten Jitterwerte Sender zu Responder

**SNMP-ID:** 2.36.4.63

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.64 Average-Jitter-DS

Durchschnitt aller absoluten Jitterwerte Responder zu Sender

**SNMP-ID:** 2.36.4.64

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.8 RTT-Min

Minimale Roundtrip-Zeit in uSec

**SNMP-ID:** 2.36.4.8

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.9 RTT-Max

maximale Roundtrip-Zeit in uSec

**SNMP-ID:** 2.36.4.9

**Pfad Telnet:** /Setup/Performance-Monitoring/RttMonStatistics

## 2.37 WLAN-Management

Dieses Menü enthält die Konfiguration des WLAN-Managements für WLAN-Controller.

## 2.37.6 AP-automatisch-einbinden

Ermöglicht dem WLAN Controller, allen neuen Access Points eine Konfiguration zuzuweisen, auch wenn diese nicht über ein gültiges Zertifikat verfügen.

Ermöglicht dem WLAN Controller, allen neuen Access Points ohne gültiges Zertifikat ein solches Zertifikat zuzuweisen. Dazu muss eine der beiden Bedingungen erfüllt sein:

- Für den Access Point ist unter seiner MAC-Adresse eine Konfiguration in der AP-Tabelle eingetragen.

- Die Option 'Automatische Zuweisung der Default-Konfiguration' ist aktiviert.

**SNMP-ID:** 2.37.6

**Pfad Telnet:** /Setup/WLAN-Management

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

Mit der Kombination der Einstellungen für Auto-Accept und Default-Konfiguration können Sie verschiedene Situationen für die Einrichtung und den Betrieb der Access Points abdecken:

Auto-Accept EIN, Default-Konfiguration EIN: Rollout-Phase: Verwenden Sie diese Kombination nur dann, wenn keine Access Points unkontrolliert mit dem LAN verbunden werden können und so unbeabsichtigt in die WLAN-Struktur aufgenommen werden.

Auto-Accept EIN, Default-Konfiguration AUS: Kontrollierte Rollout-Phase: Verwenden Sie diese Kombination, wenn Sie alle erlaubten Access Points mit ihrer MAC-Adresse in die AP-Tabelle eingetragen haben und diese automatisch in die WLAN-Struktur aufgenommen werden sollen.

Auto-Accept AUS, Default-Konfiguration AUS: Normalbetrieb: Es werden keine neuen Access Points ohne Zustimmung der Administratoren in die WLAN-Struktur aufgenommen.

## 2.37.7 AP-einbinden

Do-Kommando zum Akzeptieren von neuen Aps. Als Parameter muss die MAC-Adresse angegeben werden. Optional kann auch ein Profil-Name hinter der MAC-Adresse angegeben werden.

**SNMP-ID:** 2.37.7

**Pfad Telnet:** /Setup/WLAN-Management

**Mögliche Werte:**

- Syntax: do AP-einbinden [-c] <WTP-MAC> [<Profile>]
- -c: do not generate config entry

**Default:** leer

## 2.37.9 AP-Verbindung-trennen

Do-Kommando zum Trennen von Aps. Als Parameter muss die MAC-Adresse angegeben werden.

**SNMP-ID:** 2.37.9

**Pfad Telnet:** /Setup/WLAN-Management

**Mögliche Werte:**

- Syntax: do AP-Verbindung-trennen <WTP-MAC>

**Default:** leer

## 2.37.5 CAPWAP-Port

Port-Nummer für den CAPWAP Dienst

**SNMP-ID:** 2.37.5

**Pfad Telnet:** /Setup/WLAN-Management

**Mögliche Werte:**

- 0 bis 65535

**Default:** 1027

Nicht per LANconfig konfigurierbar

## 2.37.8 Defaultkonfiguration-verwenden

Ermöglicht dem WLAN Controller, allen neuen Access Points (also ohne gültiges Zertifikat) eine Default-Konfiguration zuzuweisen, auch wenn für diese keine explizite Konfiguration hinterlegt wurde. Im Zusammenspiel mit dem Auto-Accept kann der WLAN Controller alle im LAN gefundenen Access Points im Managed-Modus automatisch in die von ihm verwaltete WLAN-Struktur aufnehmen (bis zur maximalen Anzahl der auf einem WLAN Controller verwalteten Access Points).

**SNMP-ID:** 2.37.8

**Pfad Telnet:** /Setup/WLAN-Management

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

Mit dieser Option können möglicherweise auch unbeabsichtigte Access Points in die WLAN-Struktur aufgenommen werden. Daher sollte diese Option nur während der Startphase bei der Einrichtung einer zentral verwalteten WLAN-Struktur aktiviert werden.

## 2.37.31 Intervall-zur-Bereinigung-der-Statustabellen

Der WLAN-Controller bereinigt regelmäßig die Statustabellen des Background-Scans und der gesehenen WLAN-Clients. Bei einem solchen Durchlauf entfernt der WLAN-Controller alle Einträge, die älter als das hier eingetragene Intervall in Minuten sind.

**Pfad Telnet:** /Setup/WLAN-Management/Intervall-zur-Bereinigung-der-Statustabellen

**Mögliche Werte:**

- maximal 11 numerische Zeichen

**Default:** 1440 Minuten

## 2.37.33 Lizenzlimit

Dieser Wert zeigt die maximal mögliche Anzahl von Lizenzen für den WLAN-Controller, die Sie auf diesem Gerät nutzen können.

**Pfad Telnet:** /Setup/WLAN-Management/Lizenzlimit

Dieser Wert dient nur zu Ihrer Information, Sie können diesen Wert nicht verändern.

## 2.37.32 Lizenzzahl

Dieser Wert zeigt die aktuelle Anzahl von Lizenzen für den WLAN-Controller, die Sie auf diesem Gerät nutzen können.

**SNMP-ID:** 2.37.32

**Pfad Telnet:** /Setup/WLAN-Management/Lizenzzahl

Dieser Wert dient nur zu Ihrer Information, Sie können diesen Wert nicht verändern.

## 2.37.19 Starte-automatische-Funkfeldoptimierung

automatisch Funktfeldoptimierung starten. Optional kann die Optimierung auf eine AP eingeschränkt werden, indem man dessen MAC-Adresse als Parameter angibt.

**SNMP-ID:** 2.37.19

**Pfad Telnet:** /Setup/WLAN-Management

**Mögliche Werte:**

- Syntax: do Starte-automatische-Funkfeldoptimierung [<WTP-MAC>]

**Default:** leer

## 2.37.30 WTP-Password-synchron-halten

Bei Aktivierung dieser Funktion wird das Haupt-Geräte-Passwort des Access-Points bei jeder Anmeldung gesetzt, um dieses synchron zum Passwort des WLAN-Controllers zu halten. Ist die Funktion deaktiviert, wird das Haupt-Geräte-Passwort nur dann gesetzt, wenn im Access-Point bei der Anmeldung kein Passwort gesetzt ist. Ein einmal gesetztes Passwort wird niemals überschrieben.

**SNMP-ID:** 2.37.30

**Pfad Telnet:** /Setup/WLAN-Management/WTP-Password-synchron-halten

**Mögliche Werte:**

- ja
- nein

**Default:** ja

## 2.37.1 AP-Konfiguration

Dieses Menü enthält die Einstellungen der Access-Point-Konfiguration.

**SNMP-ID:** 2.37.1

**Pfad Telnet:** /Setup/WLAN-Management

**Default:** Leer

### 2.37.1.7 Kontrollkanalverschluesselungs-Default

Verschlüsselung für die Kommunikation über den Kontrollkanal. Ohne Verschlüsselung werden die Kontrolldaten im Klartext ausgetauscht. Eine Authentifizierung mittels Zertifikat findet in beiden Fällen statt.

**SNMP-ID:** 2.37.1.7

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration

**Mögliche Werte:**

- DTLS
- Nein

**Default:** DTLS (1)

### 2.37.1.8 Laendereinstellungs-Default

Land, in dem die Access Points betrieben werden sollen. Aufgrund dieser Information werden landesspezifische Einstellungen wir die erlaubten Kanäle etc. festgelegt.

**SNMP-ID:** 2.37.1.8

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration

**Mögliche Werte:**

- Albanien
- Argentinien
- Australien
- Oesterreich
- Bahrain
- Bangladesh
- Weissrussland

- Belgien
- Bosnien-Herzegovina
- Brasilien
- Brunei-Daressalam
- Bulgarien
- Kanada
- Chile
- China
- Kolumbien
- Costa-Rica
- Kroatien
- Zypern
- Tschechei
- Daenemark
- Ecuador
- Egalistan
- Aegypten
- Estland
- Finland
- Frankreich
- Deutschland
- Ghana
- Griechenland
- Guatemala
- Honduras
- Hong-Kong
- Ungarn
- Island
- Indien
- Indonesien
- Irland
- Israel
- Italien
- Japan
- Jordanien
- Sued-Korea
- Kuwait
- Lettland
- Libanon
- Liechentstein
- Litauen
- Luxemburg
- Macao
- Mazedonien
- Malaysia
- Malta
- Mexiko
- Moldavien
- Marokko

- Niederlande
- Neuseeland
- Nicaragua
- Norwegen
- Oman
- Pakistan
- Panama
- Paraguay
- Peru
- Philippinen
- Polen
- Portugal
- Puerto-Rico
- Qatar
- Rumaenien
- Russland
- Saudi-Arabien
- Singapur
- Slowakei
- Slovenien
- Suedafrika
- Spanien
- Schweden
- Schweiz
- Taiwan
- Tansania
- Thailand
- Tunesien
- Tuerkei
- Uganda
- Ukraine
- Vereinigte-Arabische-Emirate
- Grossbritannien
- Vereinigte-Staaten-FCC
- Uruguay
- Venezuela

**Default:** Deutschland (276)

### 2.37.1.5 WLAN-Modul-1-Default

Frequenzband für das erste WLAN-Modul. Mit diesem Parameter kann das WLAN-Modul auch deaktiviert werden.

**SNMP-ID:** 2.37.1.5

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration

**Mögliche Werte:**

- 2,4GHz
- 5GHz
- Aus

**Default:** 2,4GHz

### 2.37.1.6 WLAN-Modul-2-Default

Frequenzband für das zweite WLAN-Modul. Mit diesem Parameter kann das WLAN-Modul auch deaktiviert werden.

**SNMP-ID:** 2.37.1.6

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration

**Mögliche Werte:**

- 2,4GHz
- 5GHz
- Aus

**Default:** 5GHz

### 2.37.1.1 Netzwerkprofile

Hier definieren Sie die logischen WLAN-Netzwerke, die auf den angemeldeten Access-Points (APs) aktiviert und betrieben werden können.

**SNMP-ID:** 2.37.1.1

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration

#### 2.37.1.1.1 Name

Name des logischen WLAN-Netzwerks, unter dem die Einstellungen gespeichert werden. Dieser Name wird nur für die interne Verwaltung der logischen Netze verwendet.

**SNMP-ID:** 2.37.1.1.1

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- max. 31 ASCII-Zeichen

**Default:** Leer

#### 2.37.1.1.2 Abgeleitet-von

Mit einem LANCOM WLAN Controller können sehr viele unterschiedliche Access Points an verschiedenen Standorten verwaltet werden. Nicht alle Einstellungen in einem WLAN-Profil eignen sich dabei für jeden der verwalteten Access Points gleichermaßen. Unterschiede gibt es z. B. in den Ländereinstellungen oder bei den Geräteeigenschaften.

Damit auch in komplexen Anwendungen die WLAN-Parameter nicht in mehreren Profilen redundant je nach Land oder Gerätetyp gepflegt werden müssen, können die logischen WLAN-Netzwerke ausgewählte Eigenschaften von anderen Einträgen „erben“.

**SNMP-ID:** 2.37.1.1.2

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- max. 31 ASCII-Zeichen

**Default:** Leer

#### 2.37.1.1.3 Lokale-Werte

Legen Sie hier fest, welche logischen WLAN-Parameter bei der Vererbung vom Eltern-Element übernommen werden sollen. Alle nicht geerbten Parameter können lokal für diese Profil eingestellt werden.

**SNMP-ID:** 2.37.1.1.3

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- Bitfeld als HEX-Zahl. Gesetzte Bits spezifizieren zu vererbende Spalten. Auswahl aus der Liste der logischen WLAN-Netzwerke (GUI).

**Default:** Alle Werte werden vom Eltern-Element übernommen.

#### 2.37.1.1.21 SSID

Stellen Sie für jedes benötigte logische Funknetzwerk eine eindeutige SSID (den Netzwerknamen) ein. Nur solche WLAN-Clients, die über die gleiche SSID verfügen, können sich in diesem Funknetzwerk anmelden.

**SNMP-ID:** 2.37.1.1.21

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- max. 32 Zeichen

**Default:** BLANK

#### 2.37.1.1.4 Aktiv

Schaltet das logische WLAN separat ein- oder aus.

**SNMP-ID:** 2.37.1.1.4

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- Ein
- Aus

**Default:** Ein

#### 2.37.1.1.30 VLAN-Modus

Wählen Sie hier die VLAN-Modus für dieses WLAN-Netzwerks (SSID) aus.

**SNMP-ID:** 2.37.1.1.30

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- tagged: Der Access Point markiert die Pakete dieser SSID mit der unter *2.37.1.1.34 VLAN-Id* konfigurierten ID.
- untagged: Der Access Point leitet die Pakete dieser SSID ohne zusätzliche VLAN-ID weiter.

**Default:** untagged

Der Access Point verwendet die VLAN-Einstellungen für das logische WLAN nur dann, wenn Sie das VLAN-Modul des Access Points in den physikalischen WLAN-Parametern aktivieren. Mit der Einstellung 'untagged' für ein spezielles WLAN können Sie auch bei aktiviertem VLAN ein WLAN ohne VLAN betreiben.

#### 2.37.1.1.5 VLAN-Id

VLAN-ID für dieses logische WLAN-Netzwerk

**SNMP-ID:** 2.37.1.1.5

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- 0 bis 4094

**Default:** 0

**Besondere Werte:** 0: schaltet die Verwendung von VLAN für dieses WLAN-Netzwerk aus.

#### 2.37.1.1.6 Verschluesselung

Wählt das Verschlüsselungs-Verfahren bzw. bei WEP die Schlüssellänge aus, die bei der Verschlüsselung von Datenpaketen auf dem Wireless-LAN verwendet wird.

**SNMP-ID:** 2.37.1.1.6

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- 802.11i-WPA-PSK
- 802.11i-WPA-802.1x
- WEP-104-Bit
- WEP-40-Bit
- WEP-104-Bit-802.1x
- WEP-40-Bit-802.1x
- keine

**Default:** 802.11i-WPA-PSK (0)

Beachten Sie, dass nicht jedes Verschlüsselungs-Verfahren von jeder Wireless-Karte unterstützt wird.

#### 2.37.1.1.7 WPA1-Sitzungsschluessel

Wählen Sie hier die Verfahren aus, welche zur Generierung der WPA-Sitzungs- bzw -Gruppen-Schlüssel angeboten werden sollen. Es können das Temporal Key Integrity Protokoll (TKIP), der Advanced Encryption Standard (AES) oder beide angeboten werden.

**SNMP-ID:** 2.37.1.1.7

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- TKIP/AES
- AES
- TKIP

**Default:** TKIP/AES

#### 2.37.1.1.27 WPA2-Sitzungsschluessel

Wählen Sie hier die Verfahren aus, welche zur Generierung der WPA-Sitzungs- bzw -Gruppen-Schlüssel angeboten werden sollen. Es können das Temporal Key Integrity Protokoll (TKIP), der Advanced Encryption Standard (AES) oder beide angeboten werden.

**SNMP-ID:** 2.37.1.1.27

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- TKIP/AES
- AES

- TKIP

**Default:** TKIP/AES

#### 2.37.1.1.8 WPA-Version

Mit dieser WPA-Version werden die Daten in diesem logischen WLAN verschlüsselt.

**SNMP-ID:** 2.37.1.1.8

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- WPA1/2
- WPA1
- WPA2

**Default:** WPA1/2 (0)

#### 2.37.1.1.9 Schluessel

Sie können die Schlüssel oder Passphrases als ASCII-Zeichenkette eingeben. Bei WEP ist alternativ die Eingabe einer Hexadezimalzahl durch ein vorangestelltes 'Ox' möglich. Folgende Langen ergeben sich für die verwendeten Formate: Verfahren Länge WPA-PSK 8 bis 63 ASCII-Zeichen WEP152 (128 bit) 16 ASCII-oder 32 HEX-Zeichen WEP128 (104 bit) 13 ASCII-oder 26 HEX-Zeichen WEP64 (40 bit) 5 ASCII-oder 10 HEX-Zeichen

**SNMP-ID:** 2.37.1.1.9

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- ASCII-Zeichenkette oder Hexadezimalzahl

**Default:** Leer

#### 2.37.1.1.10 Band

Mit der Auswahl des Frequenzbandes legen Sie fest, ob die WLAN-Karte im 2,4 GHz- oder im 5 GHz-Band arbeitet, und damit gleichzeitig die möglichen Funkkanäle.

**SNMP-ID:** 2.37.1.1.10

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- 2,4GHz/5GHz
- 2,4GHz
- 5GHz

**Default:** 2,4GHz/5GHz

#### 2.37.1.1.11 Weiterbetrieb

Zeit in Minuten, für die der Access Point im Managed-Modus mit seiner aktuellen Konfiguration weiterarbeitet.

Die Konfiguration wird dem Access Point vom WLAN Controller zugewiesen und optional im Flash gespeichert (in einem Bereich, der nicht mit LANconfig oder anderen Tools auszulesen ist). Falls die Verbindung zum WLAN Controller unterbrochen wird, arbeitet der Access Points für die hier eingestellte Zeit mit seiner Konfiguration aus dem Flash weiter. Auch nach einem eigenen Stromausfall kann der Access Point mit der Konfiguration aus dem Flash weiterarbeiten.

Wenn die eingestellte Zeit abgelaufen ist und die Verbindung zum WLAN Controller noch nicht wiederhergestellt wurde, wird die Konfiguration im Flash gelöscht – der Access Point stellt seinen Betrieb ein. Sobald der WLAN Controller wieder erreichbar ist, wird die Konfiguration erneut vom WLAN Controller zum Access Point übertragen.

Durch diese Option kann der Access Point auch dann weiter arbeiten, wenn die Verbindung zum WLAN Controller kurzfristig unterbrochen wird. Außerdem stellt diese Maßnahme einen wirksamen Schutz gegen Diebstahl dar, da die sicherheitsrelevanten Parameter der Konfiguration nach Ablauf der eingestellten Zeit automatisch gelöscht werden.

**SNMP-ID:** 2.37.1.1.11

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- 0 bis 9999

**Default:** 0

**Besondere Werte:** 0: Schaltet das WLAN-Modul des Gerätes sofort aus, wenn die Verbindung zum Controller unterbrochen wird. Die vom WLAN Controller zugewiesene Konfiguration wird in diesem Fall nicht im Flash, sondern im RAM abgelegt und geht damit bei einer Trennung vom Stromnetz sofort verloren.

9999: Arbeitet unbegrenzt mit der aktuellen Konfiguration weiter, auch wenn der WLAN Controller dauerhaft unerreichbar ist. Erst mit einem Reset wird die WLAN-Konfiguration im Flash gelöscht.

Alle weiteren Parameter der WLAN-Netzwerke entsprechen denen der üblichen Konfiguration für Access Points.

Stellt der Access Point im Backupfall eine Verbindung zu einem sekundären WLAN Controller her, so wird der Ablauf der Zeit für den autarken Weiterbetrieb unterbrochen. Der Access Point bleibt also mit seinen WLAN-Netzwerken auch über diese eingestellte Zeit hinaus aktiv, solange er eine Verbindung zu einem WLAN Controller hat.

Bitte beachten Sie, dass die Konfigurationsdaten im Flash erst nach Ablauf der eingestellten Zeit für den autarken Weiterbetrieb gelöscht werden, nicht jedoch durch die Trennung vom Stromnetz!

#### 2.37.1.1.12 Min-Tx-Rate

Der Access Point handelt mit den angeschlossenen WLAN-Clients die Geschwindigkeit für die Datenübertragung normalerweise fortlaufend dynamisch aus. Dabei passt der Access Point die Übertragungsgeschwindigkeit an die Empfangslage aus. Alternativ können Sie hier die minimale Übertragungsgeschwindigkeit fest vorgeben, wenn Sie die dynamische Geschwindigkeitsanpassung verhindern wollen.

**SNMP-ID:** 2.37.1.1.12

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- Auto
- 1M
- 2M
- 5,5M
- 11M
- 6M
- 9M
- 12M
- 18M
- 24M
- 36M
- 48M

- 54M
- T-72M
- T-96M
- T-108M

**Default:** Auto

#### 2.37.1.1.13 Max-Tx-Rate

Der Access Point handelt mit den angeschlossenen WLAN-Clients die Geschwindigkeit für die Datenübertragung normalerweise fortlaufend dynamisch aus. Dabei passt der Access Point die Übertragungsgeschwindigkeit an die Empfangslage aus. Alternativ können Sie hier die maximale Übertragungsgeschwindigkeit fest vorgeben, wenn Sie die dynamische Geschwindigkeitsanpassung verhindern wollen.

**SNMP-ID:** 2.37.1.1.13

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- Auto
- 1M
- 2M
- 5,5M
- 11M
- 6M
- 9M
- 12M
- 18M
- 24M
- 36M
- 48M
- 54M
- T-72M
- T-96M
- T-108M

**Default:** Auto

#### 2.37.1.1.14 Basis-Rate

Die eingestellte Broadcastgeschwindgkeit sollte es auch unter ungünstigen Bedingungen erlauben, die langsamsten Clients im WLAN zu erreichen. Stellen Sie hier nur dann eine höhere Geschwindigkeit ein, wenn alle Clients in diesem logischen WLAN auch „schneller" zu erreichen sind.

**SNMP-ID:** 2.37.1.1.14

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- 1M
- 2M
- 5,5M
- 11M
- 6M
- 9M
- 12M

- 18M
- 24M
- 36M
- 48M
- 54M
- T-72M
- T-96M
- T-108M

**Default:** 2M

#### 2.37.1.1.15 11b-Praeambel

Normalerweise handeln die Clients im 802.11b-Modus die Länge der zu verwendenden Präambel mit dem Access Point selbst aus. Stellen Sie hier die „lange Präambel" nur dann fest ein, wenn die Clients diese feste Einstellung verlangen.

**SNMP-ID:** 2.37.1.1.15

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- Auto
- Lang

**Default:** Auto

#### 2.37.1.1.16 MAC-Filter

In der MAC-Filterliste werden die MAC-Adressen der Clients hinterlegt, die sich bei einem Access Point einbuchen dürfen. Mit dem Schalter 'MAC-Filter aktiviert' kann die Verwendung der MAC-Filterliste gezielt für einzelne logische Netzwerke ausgeschaltet werden.

**SNMP-ID:** 2.37.1.1.16

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

Die Verwendung der MAC-Filterliste ist auf jeden Fall erforderlich für logische Netzwerke, in denen sich die Clients mit einer individuellen Passphrase über LEPS anmelden. Die bei LEPS verwendete Passphrase wird ebenfalls in der MAC-Filterliste eingetragen. Für die Anmeldung mit einer individuellen Passphrase wird daher immer die MAC-Filterliste beachtet, auch wenn diese Option hier deaktiviert ist.

#### 2.37.1.1.17 Cl.-Brg.-Support

Während mit der Adress-Anpassung ('Adress-Anpassung' Æ Seite 480) nur die MAC-Adresse eines einzigen angeschlossenen Gerätes für den Access Point sichtbar gemacht werden kann, werden über die Client-Bridge-Unterstützung alle MAC-Adressen der Stationen im LAN hinter der Clientstationen transparent an den Access Point übertragen.

Dazu werden in dieser Betriebsart nicht die beim Client-Modus üblichen drei MAC-Adressen verwendet (in diesem Beispiel für Server, Access Point und Clientstation), sondern wie bei Punkt-zu-Punkt-Verbindungen vier Adressen (zusätzlich die MAC-Adresse der Station im LAN der Clientstation). Die volltransparente Anbindung eines LANs an der Clientstation ermöglicht die gezielte Übertragung der Datenpakete im WLAN und damit Funktionen wie TFTP-Downloads, die über einen Broadcast angestoßen werden.

**SNMP-ID:** 2.37.1.1.17

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- Ja: Aktiviert die Client-Bridge-Unterstützung für dieses logische WLAN.
- Nein: Deaktiviert die Client-Bridge-Unterstützung für dieses logische WLAN.
- Exklusiv: Akzeptiert nur Clients, die ebenfalls den Client-Bridge-Modus unterstützen.

**Default:** Nein

Der Client-Bridge-Modus kann ausschließlich zwischen zwei LANCOM-Geräten verwendet werden.

#### 2.37.1.1.18 Maximum-Stationen

Legen Sie hier die maximale Anzahl der Clients fest, die sich bei diesem Access Point einbuchen dürfen. Weitere Clients, die sich über diese Anzahl hinaus anmelden wollen, werden abgelehnt.

**SNMP-ID:** 2.37.1.1.18

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- 0 bis 65535

**Default:** 0

#### 2.37.1.1.19 SSID-Broadcast

Sie können Ihr Funk-LAN entweder in einem öffentlichen oder in einem privaten Modus betreiben. Ein Funk-LAN im öffentlichen Modus kann von Mobilstationen in der Umgebung ohne weiteres kontaktiert werden. Durch Aktivieren der Closed-Network-Funktion versetzen Sie Ihr Funk-LAN in einen privaten Modus. In dieser Betriebsart sind Mobilstationen ohne Kenntnis des Netzwerknamens (SSID) von der Teilnahme am Funk-LAN ausgeschlossen.

Schalten Sie den 'Closed-Network-Modus' ein, wenn Sie verhindern möchten, dass sich WLAN-Clients mit der SSID 'Any' in Ihrem Funknetzwerk anmelden.

**SNMP-ID:** 2.37.1.1.19

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

#### 2.37.1.1.22 Min.-HT-MCS

Eine bestimmte MCS-Nummer bezeichnet eine eindeutige Kombination aus Modulation der Einzelträger (BPSK, QPSK, 16QAM, 64QAM), Coding-Rate (d. h. Anteil der Fehlerkorrekturbits an den Rohdaten) und Anzahl der Spatial Streams. 802.11n verwendet diesen Begriff anstelle „Datenrate“ bei älteren WLAN-Standards, weil die Rate keine eindeutige Beschreibung mehr ist.

Die Auswahl des MCS gibt also an, welche Modulationsparameter minimal bzw. maximal verwendet werden sollen. Innerhalb dieser Grenzen wird das passende MCS je nach den vorliegenden Bedingungen beim Verbindungsaufbau gewählt und während der Verbindung bei Bedarf angepasst. Damit wird auch der maximal erreichbare Datendurchsatz definiert. Eine Liste mit den Werte der verschiedenen MCS finden Sie im Referenzhandbuch.

Die erste Ziffer gibt die Modulationsparameter für einen Spatial Stream an, die zweite Ziffer die Modulationsparameter für zwei Spatial Streams.

**SNMP-ID:** 2.37.1.1.22

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- Auto
- MCS-0/8
- MCS-1/9
- MCS-2/10
- MCS-3/11
- MCS-4/12
- MCS-5/13
- MCS-6/14
- MCS-7/15

**Default:** Auto

In der Standardeinstellung wählt die Station automatisch die für den jeweiligen Stream optimalen MCS entsprechend den derzeitigen Kanalbedingungen aus. Wenn sich wahrend des Betriebs beispielsweise Interferenzen durch Bewegung des Senders oder Abschwächung des Signals ergeben und sich dadurch die jeweiligen Kanalbedingungen ändern, wird das MCS dynamisch an die neuen Bedingungen angepasst.

#### 2.37.1.1.23 Max.-HT-MCS

Eine bestimmte MCS-Nummer bezeichnet eine eindeutige Kombination aus Modulation der Einzelträger (BPSK, QPSK, 16QAM, 64QAM), Coding-Rate (d. h. Anteil der Fehlerkorrekturbits an den Rohdaten) und Anzahl der Spatial Streams. 802.11n verwendet diesen Begriff anstelle „Datenrate“ bei älteren WLAN-Standards, weil die Rate keine eindeutige Beschreibung mehr ist.

Die Auswahl des MCS gibt also an, welche Modulationsparameter minimal bzw. maximal verwendet werden sollen. Innerhalb dieser Grenzen wird das passende MCS je nach den vorliegenden Bedingungen beim Verbindungsaufbau gewählt und während der Verbindung bei Bedarf angepasst. Damit wird auch der maximal erreichbare Datendurchsatz definiert. Eine Liste mit den Werte der verschiedenen MCS finden Sie im Referenzhandbuch.

Die erste Ziffer gibt die Modulationsparameter für einen Spatial Stream an, die zweite Ziffer die Modulationsparameter für zwei Spatial Streams.

**SNMP-ID:** 2.37.1.1.23

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- Auto
- MCS-0/8
- MCS-1/9
- MCS-2/10
- MCS-3/11
- MCS-4/12
- MCS-5/13
- MCS-6/14
- MCS-7/15

**Default:** Auto

In der Standardeinstellung wählt die Station automatisch die für den jeweiligen Stream optimalen MCS entsprechend den derzeitigen Kanalbedingungen aus. Wenn sich wahrend des Betriebs beispielsweise Interferenzen durch Bewegung des Senders oder Abschwächung des Signals ergeben und sich dadurch die jeweiligen Kanalbedingungen ändern, wird das MCS dynamisch an die neuen Bedingungen angepasst.

#### 2.37.1.1.24 Kurzes-Guard-Intervall

Mit dieser Option wird die Sendepause zwischen zwei Signalen von 0,8 µs (Standard) auf 0,4 µs (Short Guard Interval) reduziert. Dadurch steigt die effektiv für die Datenübertragung genutzte Zeit und damit der Datendurchsatz. Auf der anderen Seite wird das WLAN-System anfälliger für Störungen, welche durch die Interferenzen zwischen zwei aufeinanderfolgenden Signalen auftreten können.

Im Automatik-Modus wird das kurze Guard-Intervall aktiviert, sofern die aktuellen Betriebsbedingungen das zulassen. Alternativ kann die Nutzung des kurzen Guard-Intervalls auch ausgeschaltet werden.

**SNMP-ID:** 2.37.1.1.24

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- Auto
- Nein

**Default:** Auto

#### 2.37.1.1.25 Max.-Spatiale-Stroeme

Mit der Funktion des Spatial-Multiplexing können mehrere separate Datenströme über separate Antennen übertragen werden, um so den Datendurchsatz zu verbessern. Der Einsatz dieser Funktion ist nur dann zu empfehlen, wenn die Gegenstelle die Datenströme mit entsprechenden Antennen verarbeiten kann.

**SNMP-ID:** 2.37.1.1.25

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- Auto
- Einer
- Zwei

**Default:** Auto

**Besondere Werte:**

- **Auto:** Mit der Einstellung 'Auto' werden alle Spatial-Streams genutzt, die von dem jeweiligen WLAN-Modul unterstützt werden.

#### 2.37.1.1.26 Sende-Aggregate

Bei der Frame-Aggregation werden mehrere Datenpakete (Frames) zu einem größeren Paket zusammengefasst und gemeinsam versendet. Durch dieses Verfahren kann der Overhead der Pakete reduziert werden, der Datendurchsatz steigt.

Die Frame-Aggregation eignet sich weniger gut bei schnell bewegten Empfängern oder für zeitkritische Datenübertragungen wie Voice over IP.

**SNMP-ID:** 2.37.1.1.26

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

#### 2.37.1.1.28 RADIUS-Accounting aktiviert

Stellen Sie hier ein, ob das RADIUS-Accounting in diesem logischen WLAN-Netzwerk aktiviert werden soll.

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- ja, nein

**Default:** nein

Die Access Points, die der WLAN-Controller mit diesem logischen WLAN-Netzwerk konfiguriert, müssen eine Firmware der LCOS-Version 8.00 oder höher verwenden.

#### 2.37.1.1.30 VLAN-Modus

Wählen Sie hier die VLAN-Modus für dieses WLAN-Netzwerks (SSID) aus.

**SNMP-ID:** 2.37.1.1.30

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- tagged: Der Access Point markiert die Pakete dieser SSID mit der unter *2.37.1.1.34 VLAN-Id* konfigurierten ID.
- untagged: Der Access Point leitet die Pakete dieser SSID ohne zusätzliche VLAN-ID weiter.

**Default:** untagged

Der Access Point verwendet die VLAN-Einstellungen für das logische WLAN nur dann, wenn Sie das VLAN-Modul des Access Points in den physikalischen WLAN-Parametern aktivieren. Mit der Einstellung 'untagged' für ein spezielles WLAN können Sie auch bei aktiviertem VLAN ein WLAN ohne VLAN betreiben.

#### 2.37.1.1.32 Verbinde-SSID-mit

Stellen Sie hier ein, an welche logische Schnittstelle der Access Point die Nutzdaten aus diesem WLAN-Netzwerk (SSID) überträgt.

**SNMP-ID:** 2.37.1.1.32

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- LAN: Der Access Point leitet die Nutzdaten aus diesem WLAN-Netzwerk über die Bridge an die eigene lokale LAN-Schnittstelle weiter. Konfigurieren Sie in diesem Fall die weitere Verarbeitung der Datenpakete durch entsprechende Routen direkt auf dem Access Point, z. B. durch einen separaten Internet-Zugang.
- WLC-Tunnel-1 bis WLC-Tunnel-x (modellabhängig): Der Access Point leitet die Nutzdaten aus diesem WLAN-Netzwerk über die Bridge an eine der virtuellen Schnittstellen für den WLAN-Controller weiter (WLC-Tunnel). Konfigurieren Sie in diesem Fall die weitere Verarbeitung der Datenpakete durch entsprechende Routen zentral auf dem WLAN-Controller, z. B. durch einen gemeinsam genutzten Internet-Zugang.

**Default:** LAN

Die Weiterleitung der Nutzdaten aus mehreren SSIDs an den WLAN-Controller steigert die CPU-Last und die benötigte Bandbreite der zentralen Geräte. Berücksichtigen Sie die erforderlichen Leistungswerte beim zentralen WLAN-Management mit Layer-3-Tunneling.

Sie können für jeden Access Point bis zu 7 SSIDs mit einem WLC-Tunnel verbinden. Der WLAN-Controller verbindet auf dem jeweiligen Access Point den WLC-Tunnel und damit die verbundene SSID mit einer freien Bridge-Gruppe. Da eine der verfügbaren 8 Bridge-Gruppen für andere Zwecke reserviert ist, verbleiben 7 Bridge-Gruppen für die Zuordnung der WC-Tunnel.

#### 2.37.1.1.33 Inter-Stations-Verkehr

Je nach Anwendungsfall ist es gewünscht oder eben auch nicht erwünscht, dass die an einem Access Point angeschlossenen WLAN-Clients mit anderen Clients kommunizieren. Stellen Sie für jedes logische WLAN separat ein, ob die Clients in dieser SSID untereinander Daten austauschen können.

**SNMP-ID:** 2.37.1.1.33

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

#### 2.37.1.1.34 VLAN-Id

Stellen Sie hier die VLAN-ID für dieses logische WLAN-Netzwerk ein. Der Access Point überträgt die Daten aus diesem WLAN-Netzwerk (SSID) mit der hier eingestellten VLAN-ID, wenn der VLAN-Modus auf 'tagged' eingestellt ist.

**SNMP-ID:** 2.37.1.1.34

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

**Mögliche Werte:**

- 2 bis 4094

**Default:** 2

### 2.37.1.10 Predef.-Intranets

Diese Tabelle enthält die Liste der vordefinierten AP-Intranets.

**SNMP-ID:** 2.37.1.10

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Predef.-Intranets

Die Einstellungen für vordefinierte Intranets werden nur für interne Zwecke bei der Kommunikation des Geräts mit LANconfig verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

#### 2.37.1.10.1 Name

Hier sehen Sie den Namen des vordefinierten AP-Intranets.

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/WLAN-Modul-2-Default/Name

Die Einstellungen für vordefinierte Intranets werden nur für interne Zwecke bei der Kommunikation des Geräts mit LANconfig verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

### 2.37.1.2 Radioprofile

Hier definieren Sie physikalische WLAN-Parameter, die auf allen logischen WLAN-Netzen eines gemanagten Access-Points gemeinsam gelten.

**SNMP-ID:** 2.37.1.2

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration

#### 2.37.1.2.1 Name

Eindeutiger Name für diese Zusammenstellung von physikalischen WLAN-Parametern.

**SNMP-ID:** 2.37.1.2.1

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

**Mögliche Werte:**

- max. 31 ASCII-Zeichen

**Default:** Leer

#### 2.37.1.2.10 DTIM-Periode

Dieser Wert gibt an, nach welcher Anzahl von Beacons die gesammelten Multicasts ausgesendet werden. Höhere Werte erlauben längere Sleep-Intervalle der Clients, verschlechtern aber die Latenzzeiten.

**SNMP-ID:** 2.37.1.2.10

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

**Mögliche Werte:**

- 0 bis 255

**Default:** 0

#### 2.37.1.2.11 Hintergrund-Scan

Zur Erkennung anderer Access Points in der eigenen Funkreichweite können LANCOM Wireless Router die empfangenen Beacons (Management-Frames) aufzeichnen und in der Scan-Tabelle speichern. Da diese Aufzeichnung im Hintergrund neben der „normalen" Funktätigkeit der Access Points abläuft, wird diese Funktion auch als „Background Scan" bezeichnet.

Wird hier ein Wert angegeben, so sucht der LANCOM Wireless Router innerhalb dieses Intervalls zyklisch die aktuell ungenutzten Frequenzen des aktiven Bandes nach erreichbaren Access Points ab.

Für LANCOM Wireless Router im Access-Point-Modus wird die Background-Scan-Funktion üblicherweise zur Rogue AP Detection eingesetzt. Das Scan-Intervall sollte hier der Zeitspanne angepasst werden, innerhalb derer unbefugte Access Points erkannt werden sollen, z. B. 1 Stunde.

Für LANCOM Wireless Router im Client-Modus wird die Background-Scan-Funktion hingegen meist für ein besseres Roaming von mobilen WLAN-Clients genutzt. Um ein schnelles Roaming zu erzielen, wird die Scan-Zeit hierbei auf z. B. 260 Sekunden beschränkt.

**SNMP-ID:** 2.37.1.2.11

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

**Mögliche Werte:**

- 0 bis 4294967296

**Default:** 0

**Besondere Werte:** 0: Mit einer Hintergrund-Scan-Zeit von '0' wird die Funktion des Background-Scanning ausgeschaltet.

#### 2.37.1.2.12 Antennengewinn

Wenn Antennen mit einer höheren Sendeleistung eingesetzt werden, als in dem jeweiligen Land zulässig, ist ein Dämpfung der Leistung auf den zulässigen Wert erforderlich.

In das Feld 'Antennen-Gewinn' wird der Gewinn der Antenne abzüglich der tatsächlichen Kabeldämpfung eingetragen. Aus diesem tatsächlichen Antennengewinn wird dann dynamisch unter Berücksichtigung der anderen eingestellten Parameter wie Land, Datenrate und Frequenzband die maximal mögliche Leistung berechnet und abgestrahlt.

Im Gegensatz dazu reduziert der Eintrag im Feld 'Sendeleistungs-Reduktion' die Leistung immer statisch um den dort eingetragenen Wert, ohne Berücksichtigung der anderen Parameter. Siehe dazu auch ‘Geometrische Auslegung von Outdoor-Funknetz-Strecken’ Æ Seite 512.

**SNMP-ID:** 2.37.1.2.12

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

**Mögliche Werte:**

- minus 128 bis 127

**Default:** 0

#### 2.37.1.2.13 Sende-Leistungs-Reduktion

Im Gegensatz zum Antennen-Gewinn reduziert der Eintrag im Feld 'Sendeleistungs-Reduktion' die Leistung immer statisch um den dort eingetragenen Wert, ohne Berücksichtigung der anderen Parameter.

**SNMP-ID:** 2.37.1.2.13

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

**Mögliche Werte:**

- 0 bis 255

**Default:** 0

Durch die Sendeleistungsreduktion wird nur die abgestrahlte Leistung reduziert. Die Empfangsempfindlichkeit (der Empfangs-Antennengewinn) der Antennen bleibt davon unberührt. Mit dieser Variante können z. B. bei Funkbrücken große Entfernungen durch den Einsatz von kürzeren Kabeln überbrückt werden. Der Empfangs-Antennengewinn wird erhöht, ohne die gesetzlichen Grenzen der Sendeleistung zu übersteigen. Dadurch wird die maximal mögliche Distanz und insbesondere die erreichbare Datenübertragungsgeschwindigkeit verbessert.

#### 2.37.1.2.14 Mgmt-VLAN-Id

VLAN-ID für das Management-Netzwerk

**SNMP-ID:** 2.37.1.2.14

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

**Mögliche Werte:**

- 0 bis 4094

**Default:** 0

**Besondere Werte:** 0: Schaltet die Verwendung von VLAN aus.

1: Schaltet die Verwendung von VLAN ein, das Management-Netz bleibt jedoch ungetaggt.

2 bis 4094: Schaltet die Verwendung von VLAN ein, das Management-Netz verwendet die hier eingestellte VLAN-ID.

Alle weiteren physikalischen WLAN-Parameter entsprechen denen der üblichen Konfiguration für Access Points.

Die Management-VLAN-ID muss (!) auf einen Wert ungleich null eingestellt werden, um VLANs auf den WLAN-Netzwerken nutzen zu können. Das gilt auch dann, wenn das Management-Netz selbst nicht mit VLAN-IDs getaggt werden soll (Mgmt-VLAN-ID = 1). Die VLAN-Aktivierung gilt jeweils nur für diejenigen WLAN-Netzwerke, die mit diesen physikalischen WLAN-Parametern verbunden sind.

#### 2.37.1.2.16 Nur-Indoor-Betrieb

Bestimmen Sie ob nur der Indoor-Betrieb zugelassen werden soll.

**SNMP-ID:** 2.37.1.2.16

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/WLAN-Modul-2-Default/Nur-Indoor-Betrieb

**Mögliche Werte:**

- ja
- nein

**Default:** nein

#### 2.37.1.2.2 Abgeleitet-von

Mit einem LANCOM WLAN Controller können sehr viele unterschiedliche Access Points an verschiedenen Standorten verwaltet werden. Nicht alle Einstellungen in einem WLAN-Profil eignen sich dabei für jeden der verwalteten Access Points gleichermaßen. Unterschiede gibt es z. B. in den Ländereinstellungen oder bei den Geräteeigenschaften.

Damit auch in komplexen Anwendungen die WLAN-Parameter nicht in mehreren Profilen redundant je nach Land oder Gerätetyp gepflegt werden müssen, können die physikalischen WLAN-Parameter ausgewählte Eigenschaften von anderen Einträgen „erben".

**SNMP-ID:** 2.37.1.2.2

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

**Mögliche Werte:**

- max. 31 ASCII-Zeichen

**Default:** Leer

#### 2.37.1.2.3 Lokale-Werte

Legen Sie hier fest, welche physikalischen WLAN-Parameter bei der Vererbung vom Eltern-Element übernommen werden sollen. Alle nicht geerbten Parameter können lokal für diese Profil eingestellt werden.

**SNMP-ID:** 2.37.1.2.3

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

**Mögliche Werte:**

- Bitfeld als HEX-Zahl . Gesetzte Bits spezifizieren zu vererbende Spalten. Auswahl aus der Liste der logischen WLAN-Netzwerke (GUI).

**Default:** Alle Werte werden vom Elterne-Element übernommen.

#### 2.37.1.2.4 Land

Damit ein WLAN mit den richtigen Parametern betrieben werden kann, muss das Gerat seinen nationalen Standort kennen.

**SNMP-ID:** 2.37.1.2.4

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

**Mögliche Werte:**

- Albanien
- Argentinien
- Australien
- Oesterreich

- Bahrain
- Bangladesh
- Weissrussland
- Belgien
- Bosnien-Herzegovina
- Brasilien
- Brunei-Daressalam
- Bulgarien
- Kanada
- Chile
- China
- Kolumbien
- Costa-Rica
- Kroatien
- Zypern
- Tschechei
- Daenemark
- Ecuador
- Egalistan
- Aegypten
- Estland
- Finland
- Frankreich
- Deutschland
- Ghana
- Griechenland
- Guatemala
- Honduras
- Hong-Kong
- Ungarn
- Island
- Indien
- Indonesien
- Irland
- Israel
- Italien
- Japan
- Jordanien
- Sued-Korea
- Kuwait
- Lettland
- Libanon
- Liechentstein
- Litauen
- Luxemburg
- Macao
- Mazedonien
- Malaysia
- Malta

- Mexiko
- Moldavien
- Marokko
- Niederlande
- Neuseeland
- Nicaragua
- Norwegen
- Oman
- Pakistan
- Panama
- Paraguay
- Peru
- Philippinen
- Polen
- Portugal
- Puerto-Rico
- Qatar
- Rumaenien
- Russland
- Saudi-Arabien
- Singapur
- Slowakei
- Slovenien
- Suedafrika
- Spanien
- Schweden
- Schweiz
- Taiwan
- Tansania
- Thailand
- Tunesien
- Tuerkei
- Uganda
- Ukraine
- Vereinigte-Arabische-Emirate
- Grossbritannien
- Vereinigte-Staaten-FCC
- Uruguay
- Venezuela

**Default:** Default

**Besondere Werte:** Default: übernimmt die Verschlüsselung von der Definition im Bereich 'Optionen'.

#### 2.37.1.2.5 Kanalliste

Standardmäßig können die Access Points alle Kanäle nutzen, die aufgrund der Ländereinstellung erlaubt sind. Um die Auswahl auf bestimmte Kanäle zu beschränken, können hier die gewünschten Kanäle als kommaseparierte Liste eingetragen werden. Dabei ist auch die Angabe von Bereichen (z. B. '7-9') möglich.

**SNMP-ID:** 2.37.1.2.5

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

**Mögliche Werte:**

- Kommaseparierte Liste mit max. 48 Zeichen

**Default:** Leer

#### 2.37.1.2.6 2.4GHz-Modus

Im 2,4 GHz-Band gibt es zwei verschiedene Funk-Standards: den IEEE 802.11b-Standard mit einer Übertragungsgeschwindigkeit von bis zu 11 MBit/s und den IEEE 802.11g-Standard mit bis zu 54 MBit/s. Wenn als Frequenzband das 2,4 GHz-Band ausgewählt ist, kann zusätzlich die Übertagungsgeschwindigkeit eingestellt werden.

Um eine möglichst hohe Übertragungsgeschwindigkeit zu erreichen, gleichzeitig aber auch langsamere Clients nicht auszuschließen, bietet sich der 802.11g/b-Kompatibilitätsmodus an. In diesem Modus arbeitet die WLAN-Karte im Access Point grundsätzlich nach dem schnelleren Standard, fällt aber auf den langsameren Modus zurück, wenn sich entsprechende Clients im WLAN anmelden. Im '2-MBit-Kompatibilitätsmodus' unterstützt der Access Point auch die älteren 802.11b-Karten mit einer maximalen Übertragungsgeschwindigkeit von 2 MBit/s.

**SNMP-ID:** 2.37.1.2.6

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

**Mögliche Werte:**

- 11bg-gemischt
- nur-11b
- nur-11g
- 108Mbps
- 11bgn-gemischt
- 11gn-gemischt
- Greenfield

**Default:** 11bg-gemischt (0)

Bitte beachten Sie, dass sich Clients, die nur einen langsameren Standard unterstützen, sich ggf. nicht mehr in Ihrem WLAN anmelden können, wenn Sie die Übertragungsgeschwindigkeit auf einen hohen Wert einstellen.

#### 2.37.1.2.7 5GHz-Modus

Wenn Sie gleichzeitig zwei benachbarte, freie Kanäle für die Funkübertragung nutzen, können Sie die Übertragungsgeschwindigkeit mit dem Turbo-Modus auf bis zu 108 MBit/s steigern.

**SNMP-ID:** 2.37.1.2.7

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

**Mögliche Werte:**

- normal
- 108Mbps
- 11an-gemischt
- Greenfield

**Default:** Normal

#### 2.37.1.2.8 Unterbaender

Im 5 GHz-Band kann neben dem Frequenzband ein Unterband gewählt werden, an das wiederum bestimmte Funkkanäle und maximale Sendeleistungen geknüpft sind.

**SNMP-ID:** 2.37.1.2.8

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

**Mögliche Werte:**

- Band-1
- Band-2
- Band-3
- Band-1+2
- Band-1+3
- Band-2+3
- Band-1+2+3

**Default:** Band-1+2+3 (0)

#### 2.37.1.2.9 QoS

Mit der Erweiterung der 802.11-Standards um 802.11e können auch für WLAN-Übertragungen definierte Dienst-güten angeboten werden (Quality of Service). 802.11e unterstützt u. a. eine Priorisierung von bestimmten Datenpaketen. Die Erweiterung stellt damit eine wichtige Basis für die Nutzung von Voice-Anwendungen im WLAN dar (Voiceoder WLAN – VoWLAN).Die Wi-Fi-Alliance zertifiziert Produkte, die Quality of Service nach 802.11e unterstützen, unter dem Namen WMM(Wi-Fi Multimedia, früher WME für Wireless Multimedia Extension). WMM definiert vier Kategorien (Sprache, Video,Best Effort und Hintergrund) die in Form separater Warteschlangen zur Prioritätensteuerung genutzt werden. Der 802.11e-Standard nutzt Steuerung der Prioritäten die VLAN-Tags bzw. die DiffServ-Felder von IP-Paketen, wenn keine VLAN-Tags vorhanden sind. Die Verzögerungszeiten (Jitter) bleiben mit weniger als zwei Millisekunden in einem Bereich, der vom menschlichen Gehör nicht wahrgenommen wird. Zur Steuerung des Zugriffs auf das Übertragungsmedium nutzt der 802.11e-Standard die Enhanced Distributed Coordination Function (EDCF).

**SNMP-ID:** 2.37.1.2.9

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

Die Steuerung der Prioritäten ist nur möglich, wenn sowohl der WLAN-Client als auch der Access Point den802.11e-Standard bzw. WMM unterstützen und die Anwendungen die Datenpakete mit den entsprechen-den Prioritäten kennzeichnen.

#### 2.37.1.2.17 VLAN-Modul-der-verwalteten-APs-aktivieren

Aktivieren oder deaktivieren Sie hier das VLAN-Modul der verwalteten Access Points. Ist das VLAN aus, dann werden alle VLAN-Einstellungen in den logischen Netzen ignoriert.

**SNMP-ID:** 2.37.1.2.17

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

**Mögliche Werte:**

- ja
- nein

**Default:** nein

#### 2.37.1.2.18 Mgmt-VLAN-Modus

VLAN-Modus für das Management-Netzwerk. VLAN wird nur benutzt, wenn das VLAN-Modul des Access Points aktiviert ist. Das Mangement-Netzwerk kann trotz aktiviertem VLAN auch ungetaggt betrieben werden.

**SNMP-ID:** 2.37.1.2.18

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

**Mögliche Werte:**

- untagged: Die Management-Pakete des Access Points werden nicht mit einer VLAN-ID markiert.
- tagged: Die Management-Pakete des Access Points werden mit der als Management-VLAN-ID in diesem Radioprofil konfigurierten VLAN-ID markiert.

**Default:** untagged

#### 2.37.1.2.19 Mgmt-VLAN-ID

VLAN-ID für das Management-Netzwerk. Mit der Management-VLAN-ID wird das Management-Netzwerk getaggt, auf dem der WLAN-Controller mit den Access Points kommuniziert. VLAN wird nur benutzt, wenn das VLAN-Modul des APs aktiviert ist. Das Mangement-Netzwerk kann trotz aktiviertem VLAN auch ungetaggt betrieben werden, indem die entsprechende Einstellung für den Managment-VLAN-Modus gewählt wird. Hierzu wird intern die VLAN-ID '1' reserviert.

**SNMP-ID:** 2.37.1.2.19

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

**Mögliche Werte:**

- 2 bis 4094

**Default:** 2

### 2.37.1.3 Gesamtprofile

Hier definieren Sie ganze WLAN-Profile, die alle WLAN-Einstellungen zusammenfassen, welche auf die gemanagten APs angewendet werden können. Dazu gehören zum Beispiel bis zu 16 logische WLAN-Netze sowie ein Satz physikalische WLAN-Parameter.

**SNMP-ID:** 2.37.1.3

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration

#### 2.37.1.3.1 Name

Name des Profils, unter dem die Einstellungen gespeichert werden.

**SNMP-ID:** 2.37.1.3.1

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Gesamtprofile

**Mögliche Werte:**

- max. 31 ASCII-Zeichen

**Default:** Leer

#### 2.37.1.3.2 Netze

Liste der logischen WLAN-Netzwerke, die über dieses Profil zugewiesen werden.

**SNMP-ID:** 2.37.1.3.2

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Gesamtprofile

**Mögliche Werte:**

- max. 251 ASCII-Zeichen mehrere Werte durch Kommata getrennt.

**Default:** Leer

Die Access Points nutzen aus dieser Liste nur die ersten acht Einträge, die mit der eigenen Hardware kompatibel sind. Somit können in einem Profil z. B. jeweils acht WLAN-Netzwerke für reinen 2,4 GHz-Betrieb und acht für reinen 5 GHz-Betrieb definiert werden. Für jeden LANCOM Access Point – sowohl Modelle mit 2,4 GHz- als auch die mit 5 GHz-Unterstützung – stehen damit die maximal möglichen acht logischen WLAN-Netzwerke zur Verfügung.

#### 2.37.1.3.3 AP-Parameter

Ein Satz von physikalischen Parametern, mit denen die WLAN-Module der Access Points arbeiten sollen.

**SNMP-ID:** 2.37.1.3.3

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Gesamtprofile

**Mögliche Werte:**

- Auswahl aus der Liste der physikalischen WLAN-Parameter (GUI) oder maximal 31 ASCII-Zeichen

**Default:** Leer

#### 2.37.1.3.4 Controller

Liste der WLAN Controller, bei denen der Access Point eine Verbindung versuchen soll. Der Access Point leitet die Suche nach einem WLAN Controller über einen Broadcast ein. Wenn nicht alle WLAN Controller über einen solchen Broadcast erreicht werden können (WLAN Controller steht z. B. in einem anderen Netz), dann ist die Angabe von alternativen WLAN Controller sinnvoll.

**SNMP-ID:** 2.37.1.3.4

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Gesamtprofile

**Mögliche Werte:**

- IP-Adressen, mehrere Werte getrennt durch Kommata. max. 159 Zeichen, also je nach Länge der IP-Adressen etwa 9 bis 10 Einträge.

**Default:** Leer

### 2.37.1.4 Basisstationen

Hier definieren Sie alle gemanagten Access-Points, die von diesem WLAN-Controller (WLC) verwaltet werden sollen. Dabei weisen Sie dem AP sein WLAN-Profil zu.

**SNMP-ID:** 2.37.1.4

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration

#### 2.37.1.4.1 MAC-Adresse

MAC-Adresse des Access Points.

**SNMP-ID:** 2.37.1.4.1

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

**Mögliche Werte:**

- Gültige MAC-Adresse

**Default:** Leer

**Besondere Werte:** FFFFFFFFFFFF: definiert die Default-Konfiguration

#### 2.37.1.4.2 Name

Name des Access Point im Managed-Modus.

**SNMP-ID:** 2.37.1.4.2

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

**Mögliche Werte:**

- max. 16 ASCII-Zeichen

**Default:** Leer

#### 2.37.1.4.3 Standort

Standort des Access Point im Managed-Modus.

**SNMP-ID:** 2.37.1.4.3

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

**Mögliche Werte:**

- max. 251 ASCII-Zeichen

**Default:** Leer

#### 2.37.1.4.11 Aktiv

Aktiviert bzw. deaktiviert diesen Eintrag.

**SNMP-ID:** 2.37.1.4.11

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

#### 2.37.1.4.4 Profil

WLAN-Profil aus der Liste der definierten Profile, welches für diesen Access Point verwendet werden soll.

**SNMP-ID:** 2.37.1.4.4

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

**Mögliche Werte:**

- Auswahl aus der Liste der definierten WLAN-Profile, max. 31 ASCII-Zeichen.

**Default:** Leer

#### 2.37.1.4.6 Kontrollkanalverschluesselung

Verschlüsselung für die Kommunikation über den Kontrollkanal. Ohne Verschlüsselung werden die Kontrolldaten im Klartext ausgetauscht. Eine Authentifizierung mittels Zertifikat findet in beiden Fällen statt.

**SNMP-ID:** 2.37.1.4.6

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

**Mögliche Werte:**

- default
- DTLS
- Nein

**Default:** Default

**Besondere Werte:** Default: übernimmt die Verschlüsselung von der Definition im Bereich 'Optionen'.

#### 2.37.1.4.7 WLAN-Modul-1

Frequenzband für das erste WLAN-Modul. Mit diesem Parameter kann das WLAN-Modul auch deaktiviert werden.

**SNMP-ID:** 2.37.1.4.7

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

**Mögliche Werte:**

- default
- 2,4 GHz
- 5 GHz
- Aus

**Default:** Default

**Besondere Werte:** Default: übernimmt die Verschlüsselung von der Definition im Bereich 'Optionen'.

#### 2.37.1.4.15 Erlaube-40MHz

Normalerweise nutzt das WLAN-Modul einen Frequenzbereich von 20 MHz, in dem die zu übertragenen Daten auf die Trägersignale aufmoduliert werden. 802.11a/b/g nutzen 48 Trägersignale in einem 20 MHz-Kanal. Durch die Nutzung des doppelten Frequenzbereiches von 40 MHz können 96 Trägersignale eingesetzt werden, was zu einer Verdoppelung des Datendurchsatzes führt.

802.11n kann in einem 20 MHz-Kanal 52, in einem 40 MHz-Kanal sogar 108 Trägersignale zur Modulation nutzen. Für 802.11n bedeutet die Nutzung der 40 MHz-Option also einen Performance-Gewinn auf mehr als das Doppelte.

**SNMP-ID:** 2.37.1.4.15

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

**Mögliche Werte:**

- Auto
- Nein

**Default:** Auto

#### 2.37.1.4.16 Antennen-Maske

LANCOM Access Points mit 802.11-Unterstützung können bis zu drei Antennen zum Senden und Empfangen der Daten einsetzen. Je nach Anwendung kann die Nutzung der Antennen eingestellt werden.

**SNMP-ID:** 2.37.1.4.16

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

**Mögliche Werte:**

- 1+2+3: Beim Einsatz des Geräts im Access-Point-Modus zur Anbindung von WLAN-Clients ist in der Regel die parallele Nutzung aller drei Antennen zu empfehlen
- um eine gute Netzabdeckung zu erzielen.
- 1+3: Für die Nutzung von zwei parallelen Datenströmen z. B. bei Point-to-Point-Verbindungen mit einer entsprechenden Dual-Slant-Antenne werden die Antennen-Anschlüsse 1 und 3 verwendet. Der dritte Antennen-Anschluss wird dabei deaktiviert.
- 1: Bei Anwendungen mit nur einer Antenne (z. B. Outdoor-Anwendung mit einer Antenne) wird die Antennen an den Anschluss 1 angeschlossen
- die Anschlüsse 2 und 3 werden deaktiviert.

- Auto: automatische Auswahl der Antennen

**Default:** Auto

**Besondere Werte:** Auto: Mit der Einstellung 'Auto' werden alle verfügbaren Antennen genutzt.

#### 2.37.1.4.9 Module-1-Kanalliste

Mit dem Funkkanal wird ein Teil des theoretisch denkbaren Frequenzbandes für die Datenübertragung im Funknetz ausgewählt.

**SNMP-ID:** 2.37.1.4.9

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

**Mögliche Werte:**

- Kommaseparierte Liste mit max. 48 Zeichen

**Default:** Leer

Im 2,4 GHz-Band müssen zwei getrennte Funknetze mindestens drei Kanäle auseinander liegen, um Störungen zu vermeiden.

#### 2.37.1.4.20 Module-1-Ant-Gewinn

Mit diesem Eintrag können Sie den Antennen-Verstärkungsfaktor (Gewinn in dBi) abzüglich der Dämpfungen für Kabel und ggf. Blitzschutz angeben. Hieraus errechnet Ihre Basisstation die in Ihrem Land und für das jeweilige Frequenzband maximal zulässige Sendeleistung.

Lassen Sie das Feld leer, wird die Default-Einstellung verwendet, die bei der Konfigurationsgruppe des verwendeten WLAN-Profils eingestellt ist.

Die Sendeleistung kann auf minimal 0,5dBm im 2,4GHz-Band bzw. 6,5dBm im 5GHz Band reduziert werden. Das begrenzt den maximal einzutragenden Wert im 2,4GHz-Band auf 17,5dBi, im 5GHz-Band auf 11,5dBi. Bitte achten Sie darauf, dass Ihr Antennen/Kabel/Blitzschutz-Setup unter diesen Bedingungen den Regulierungsanforderungen des Landes entspricht, in dem Sie das System einsetzen.

Die Empfindlichkeit des Empfängers bleibt hiervon unbeeinflusst.

Beispiel: AirLancer O-18a: Antennengewinn: 18dBi, Kabeldämfung: 4dB --> Einzutragender Wert = 18dBi - 4dB = 14dBi.

**SNMP-ID:** 2.37.1.4.20

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen/Module-1-Ant-Gewinn

**Mögliche Werte Telnet:**

- 0 bis 999 dBi

**Default:** leer

Die aktuelle Sendeleistung können Sie mit Hilfe des Web-Interfaces des Gerätes oder per Telnet unter 'Status->WLAN-Statistik->WLAN-Parameter->Sendeleistung' oder per LANmonitor unter 'System-Informationen->WLAN-Karte->Sendeleistung' einsehen.

#### 2.37.1.4.22 Module-1-TX-Redukt.

Wenn Sie eine Antenne mit einem hohen Verstärkungsfaktor verwenden, dann können Sie mit diesem Eintrag die Sendeleistung Ihrer Basisstation auf die in Ihrem Land und die im jeweiligen Frequenzband zulässige Sendeleistung herunterdämpfen.

Lassen Sie das Feld leer, wird die Default-Einstellung verwendet, die bei der Konfigurationsgruppe des verwendeten WLAN-Profils eingestellt ist.

Die Sendeleistung kann auf minimal 0,5dBm im 2,4GHz-Band bzw. 6,5dBm im 5GHz Band reduziert werden. Das begrenzt den maximal einzutragenden Wert im 2,4GHz-Band auf 17,5dBi, im 5GHz-Band auf 11,5dBi. Bitte achten Sie darauf, dass Ihr Antennen/Kabel/Blitzschutz-Setup unter diesen Bedingungen den Regulierungsanforderungen des Landes entspricht, in dem Sie das System einsetzen.

Die Empfindlichkeit des Empfängers bleibt hiervon unbeeinflusst.

**SNMP-ID:** 2.37.1.4.22

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

**Mögliche Werte Telnet:**

- 0 bis 999 dBi

**Default:** leer

Die aktuelle Sendeleistung können Sie mit Hilfe des Web-Interfaces des Gerätes oder per Telnet unter 'Status->WLAN-Statistik->WLAN-Parameter->Sendeleistung' oder per LANmonitor unter 'System-Informationen->WLAN-Karte->Sendeleistung' einsehen.

#### 2.37.1.4.8 WLAN-Modul-2

Frequenzband für das zweite WLAN-Modul. Mit diesem Parameter kann das WLAN-Modul auch deaktiviert werden.

**SNMP-ID:** 2.37.1.4.8

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

**Mögliche Werte:**

- default
- 2,4 GHz
- 5 GHz
- Aus

**Default:** Default

**Besondere Werte:** Default: übernimmt die Verschlüsselung von der Definition im Bereich 'Optionen'.

#### 2.37.1.4.21 Module-2-Ant-Gewinn

Mit diesem Eintrag können Sie den Antennen-Verstärkungsfaktor (Gewinn in dBi) abzüglich der Dämpfungen für Kabel und ggf. Blitzschutz angeben. Hieraus errechnet Ihre Basisstation die in Ihrem Land und für das jeweilige Frequenzband maximal zulässige Sendeleistung.

Lassen Sie das Feld leer, wird die Default-Einstellung verwendet, die bei der Konfigurationsgruppe des verwendeten WLAN-Profils eingestellt ist.

Die Sendeleistung kann auf minimal 0,5dBm im 2,4GHz-Band bzw. 6,5dBm im 5GHz Band reduziert werden. Das begrenzt den maximal einzutragenden Wert im 2,4GHz-Band auf 17,5dBi, im 5GHz-Band auf 11,5dBi. Bitte achten Sie darauf, dass Ihr Antennen/Kabel/Blitzschutz-Setup unter diesen Bedingungen den Regulierungsanforderungen des Landes entspricht, in dem Sie das System einsetzen.

Die Empfindlichkeit des Empfängers bleibt hiervon unbeeinflusst.

Beispiel: AirLancer O-18a: Antennengewinn: 18dBi, Kabeldämfung: 4dB --> Einzutragender Wert = 18dBi - 4dB = 14dBi.

**SNMP-ID:** 2.37.1.4.21

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen/Module-2-Ant-Gewinn

**Mögliche Werte Telnet:**

- 0 bis 999 dBi

**Default:** leer

Die aktuelle Sendeleistung können Sie mit Hilfe des Web-Interfaces des Gerätes oder per Telnet unter 'Status->WLAN-Statistik->WLAN-Parameter->Sendeleistung' oder per LANmonitor unter 'System-Informationen->WLAN-Karte->Sendeleistung' einsehen.

#### 2.37.1.4.10 Module-2-Kanalliste

Mit dem Funkkanal wird ein Teil des theoretisch denkbaren Frequenzbandes für die Datenübertragung im Funknetz ausgewählt.

**SNMP-ID:** 2.37.1.4.10

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

**Mögliche Werte:**

- Kommaseparierte Liste mit max. 48 Zeichen

**Default:** Leer

Im 2,4 GHz-Band müssen zwei getrennte Funknetze mindestens drei Kanäle auseinander liegen, um Störungen zu vermeiden.

#### 2.37.1.4.23 Module-2-TX-Redukt.

Wenn Sie eine Antenne mit einem hohen Verstärkungsfaktor verwenden, dann können Sie mit diesem Eintrag die Sendeleistung Ihrer Basisstation auf die in Ihrem Land und die im jeweiligen Frequenzband zulässige Sendeleistung herunterdämpfen.

Lassen Sie das Feld leer, wird die Default-Einstellung verwendet, die bei der Konfigurationsgruppe des verwendeten WLAN-Profils eingestellt ist.

Die Sendeleistung kann auf minimal 0,5dBm im 2,4GHz-Band bzw. 6,5dBm im 5GHz Band reduziert werden. Das begrenzt den maximal einzutragenden Wert im 2,4GHz-Band auf 17,5dBi, im 5GHz-Band auf 11,5dBi. Bitte achten Sie darauf, dass Ihr Antennen/Kabel/Blitzschutz-Setup unter diesen Bedingungen den Regulierungsanforderungen des Landes entspricht, in dem Sie das System einsetzen.

Die Empfindlichkeit des Empfängers bleibt hiervon unbeeinflusst.

**SNMP-ID:** 2.37.1.4.23

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

**Mögliche Werte Telnet:**

- 0 bis 999 dBi

**Default:** leer

Die aktuelle Sendeleistung können Sie mit Hilfe des Web-Interfaces des Gerätes oder per Telnet unter 'Status->WLAN-Statistik->WLAN-Parameter->Sendeleistung' oder per LANmonitor unter 'System-Informationen->WLAN-Karte->Sendeleistung' einsehen.

#### 2.37.1.4.12 IP-Adresse

Statische IP-Adresse für den AP, wenn kein DHCP genutzt werden kann/soll.

**SNMP-ID:** 2.37.1.4.12

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** Leer

#### 2.37.1.4.13 Netz-Maske

Statisches Netzmaske, wenn kein DHCP genutzt werden kann/soll.

**SNMP-ID:** 2.37.1.4.13

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** Leer

nicht per LANconfig konfigurierbar

#### 2.37.1.4.14 Gateway

Statisches IP-Adresse des Gateways, wenn kein DHCP genutzt werden kann/soll.

**SNMP-ID:** 2.37.1.4.14

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** Leer

Nicht per LANconfig konfigurierbar

#### 2.37.1.4.17 AP-Intranet

Hier wird auf eine Zeile in der AP-Intranets Tabelle verwiesen.

**SNMP-ID:** 2.37.1.4.17

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

**Mögliche Werte:**

- max. 31 ASCII-Zeichen

**Default:** Leer

#### 2.37.1.4.18 Verwalte-Firmware

Hier kann der automatische Firmware Upload für diesen AP abgeschaltet werden. Bei bestimmten Fehlern wird dies auch automatisch durch den Kontroller abgeschaltet. Der Grund für die automatische Abschaltung wird in der Spalte "Verwalte-Firmware-Zusätzliche-Information" angezeigt.

**SNMP-ID:** 2.37.1.4.18

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

nicht per LANconfig konfigurierbar

#### 2.37.1.4.19 Verwalte-Firmware-Zusätzliche-Information

Hier kann der automatische Firmware Upload für diesen AP abgeschaltet werden. Bei bestimmten Fehlern wird dies auch automatisch durch den Kontroller abgeschaltet. Der Grund für die automatische Abschaltung wird in der Spalte "Verwalte-Firmware-Zusätzliche-Information" angezeigt.

**SNMP-ID:** 2.37.1.4.19

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

**Mögliche Werte:**

- Leer
- Ausgeschaltet_aufgrund_eines_Fehlers_während_des_Updates
- Ausgeschaltet_aufgrund_eines_manuellen_Updates

**Default:** Leer

nicht per LANconfig konfigurierbar

### 2.37.1.9 AP-Intranets

Definieren Sie hier bei Bedarf IP-Parameter-Profile zur Verwendung in der Access-Point-Tabelle, wenn bestimmten Access-Points ihre IP-Adressen nicht per DHCP zugewiesen werden.

**SNMP-ID:** 2.37.1.9

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration

#### 2.37.1.9.1 Name

Name des Intranetz, in dem AP betrieben werden. Dieser Name wird nur für die interne Verwaltung der Intranetze verwendet.

**Mögliche Werte:**

- max. 31 ASCII-Zeichen

**Default:** Leer

#### 2.37.1.9.2 Abgeleitet-von

Mit einem LANCOM WLAN Controller können sehr viele unterschiedliche Access Points an verschiedenen Standorten verwaltet werden. Nicht alle Einstellungen in einem WLAN-Profil eignen sich dabei für jeden der verwalteten Access Points gleichermaßen. Unterschiede gibt es z. B. in den Ländereinstellungen oder bei den Geräteeigenschaften.

Damit auch in komplexen Anwendungen die Intranet-Parameter nicht in mehreren Profilen redundant gepflegt werden müssen, können die Intranetze ausgewählte Eigenschaften von anderen Einträgen „erben“.

**Mögliche Werte:**

- max. 31 ASCII-Zeichen

**Default:** Leer

#### 2.37.1.9.3 Lokale-Werte

Legen Sie hier fest, welche Intranet-Parameter bei der Vererbung vom Eltern-Element übernommen werden sollen. Alle nicht geerbten Parameter können lokal für diese Profil eingestellt werden.

**Mögliche Werte:**

- Bitfeld als HEX-Zahl . Gesetzte Bits spezifizieren zu vererbende Spalten. Auswahl aus der Liste der Intranetzwerke (GUI).

**Default:** 0

#### 2.37.1.9.4 Domainname

Domain-Name welche vom AccessPoint bei der Auflösung von WLC-Adressen benutzt wird.

**Mögliche Werte:**

- max. 63 ASCII-Zeichen

**Default:** Leer

#### 2.37.1.9.5 Netz-Maske

Statisches Netzmaske, wenn kein DHCP genutzt werden kann/soll.

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** Leer

#### 2.37.1.9.6 Gateway

Statisches IP-Adresse des Gateways, wenn kein DHCP genutzt werden kann/soll.

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** Leer

#### 2.37.1.9.7 Primärer-DNS-Srv

Statisches IP-Adresse des ersten DNS Servers, wenn kein DHCP genutzt werden kann/soll.

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** Leer

#### 2.37.1.9.8 Sekundärer-DNS-Srv

Statisches IP-Adresse des zweiten DNS Servers, wenn kein DHCP genutzt werden kann/soll.

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** Leer

### 2.37.1.12 DSCP-für-Kontrollpakete

Wählen Sie hier die passende Einstellung für die Priorisierung der Kontrollpakete über DiffServ (Differentiated Services) aus.

**SNMP-ID:** 2.37.1.12

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration

**Mögliche Werte:**

- Best-Effort
- Assured-Forwarding-11
- Assured-Forwarding-12
- Assured-Forwarding-13
- Assured-Forwarding-21
- Assured-Forwarding-22
- Assured-Forwarding-23
- Assured-Forwarding-31
- Assured-Forwarding-32
- Assured-Forwarding-33
- Assured-Forwarding-41
- Assured-Forwarding-42
- Assured-Forwarding-43
- Expedited-Forwarding

**Default:** Best-Effort

### 2.37.1.13 DSCP-für-Datenpakete

Wählen Sie hier die passende Einstellung für die Priorisierung der Datenpakete über DiffServ (Differentiated Services) aus.

**SNMP-ID:** 2.37.1.13

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration

**Mögliche Werte:**

- Best-Effort
- Assured-Forwarding-11
- Assured-Forwarding-12
- Assured-Forwarding-13
- Assured-Forwarding-21
- Assured-Forwarding-22
- Assured-Forwarding-23
- Assured-Forwarding-31
- Assured-Forwarding-32
- Assured-Forwarding-33
- Assured-Forwarding-41
- Assured-Forwarding-42
- Assured-Forwarding-43
- Expedited-Forwarding

**Default:** Best-Effort

### 2.37.1.14 Multicast-Netzwerke

Diese Tabelle enthält die Einstellungen für die Übertragung von CAPWAP-Multicast-Paketen über die jeweiligen Bridge-Schnittstellen.

Wenn ein WLAN-Controller ein Broadcast- oder Multicast-Paket für ein Netzwerk einer SSID empfängt, so muss er dieses Paket an alle Access Points weiterleiten, welche die betreffende SSID anbieten. Der WLAN-Controller hat zwei Möglichkeiten, alle betroffenen Access Points zu erreichen:

- Der WLAN-Controller kopiert das Paket und sendet es als Unicast an die jeweiligen Access Points. Die Vervielfältigung der Pakete steigert die CPU-Last auf dem Controller und die benötigte Bandbreite, was sich besonders auf WAN-Verbindungen negativ auf die Performance auswirkt.
- Der WLAN-Controller sendet das Paket als Multicast. In diesem Falle reicht in den meisten Fällen ein einziges Paket. Allerdings erreicht der Controller mit diesen Multicast-Paketen nur die Access Points in der eigenen Broadcast-Domäne. Access Points, die über eine geroutete WAN-Strecke angebunden sind, können diese Multicast-Pakete des Controllers nicht empfangen.

Die Weiterleitung der Multicast-Pakete ist abhängig von den verwendeten Routern auf der WAN-Strecke.

Der WLAN-Controller versendet regelmäßig Keep-Alive-Multicast-Pakete an die Multicast-Gruppe. Wenn ein Access Point diese Pakete beantwortet, kann der Controller diesen Access Point über Multicast-Pakete erreichen. Für alle anderen Access Points kopiert der Controller die bei ihm eingehenden Multicast-Pakete und versendet sie als Unicast an die entsprechenden Access Points.

Wenn die Übertragung von CAPWAP-Multicast-Paketen aktiviert ist und für die Bridge-Schnittstelle eine gültige Multicast-IP-Adresse mit Port definiert ist, sendet das Gerät die eingehenden Broadcast- und Multicast-Pakete als Multicast weiter an diese Adresse.

Um Informationen über die Mitgliedschaften in Multicastgruppen der eingebuchten WLAN-Clients auch beim Wechsel zu einem anderen Access Points aufrecht zu erhalten, schalten die Geräte bei der Aktivierung von Multicast auch gleichzeitig das IGMP Snooping ein, welches die Informationen über die Multicast-Struktur aktuell hält.

In Anwendungen mit mehreren WLAN-Controllern führen Multicast-Pakete möglicherweise zu Schleifen. Um Schleifen durch Multicasts bei Verwendung der Bridge zu vermeiden nutzt der WLAN-Controller die folgenden Maßnahmen:

- Der WLAN-Controller beachtet die CAPWAP-Multicast-Pakete nicht. Wenn ein WLC-Datentunnel verwendet wird, sendet der Controller die Pakete als Unicast.
- Der WLAN-Controller leitet keine Pakete weiter, die eine CAPWAP-Multicast-Adresse als Empfänger tragen.
- Der WLAN-Controller aktiviert automatisch IGMP-Snooping auf allen verwalteten Access Points, wenn CAPWAP selbst Multicast verwendet.

#### 2.37.1.14.1 Bridge-Schnittstelle

Wählen Sie hier eine Bridge-Schnittstelle für die Multicast-Einstellungen aus.

**SNMP-ID:** 2.37.1.14.1

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Multicast-Netzwerke

**Mögliche Werte:**

- Auswahl aus einer der definierten Bridge-Schnittstellen

#### 2.37.1.14.2 Aktiv

Mit dieser Option aktivieren oder deaktivieren Sie die Nutzung von CAPWAP-Multicast-Paketen für diese Bridge-Schnittstelle.

**SNMP-ID:** 2.37.1.14.2

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Multicast-Netzwerke

**Mögliche Werte:**

- ja
- nein

**Default:** nein

#### 2.37.1.14.3 Multicast-Adresse

Wählen Sie hier eine IP-Adresse, an welche das Gerät für die gewählte Bridge-Schnittstelle die CAPWAP-Multicast-Pakete übermittelt.

**SNMP-ID:** 2.37.1.14.3

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Multicast-Netzwerke

**Mögliche Werte:**

- Maximal 15 Zeichen zur Definition einer gültigen IP-Adresse

**Default:** 233.252.124.1 bis 233.252.124.32 (IP-Adressen aus dem nicht zugewiesenen Bereich)

#### 2.37.1.14.4 Multicast-Port

Wählen Sie hier einen Port für die Übertragung von CAPWAP-Multicast-Paketen über die gewählte Bridge-Schnittstelle.

**SNMP-ID:** 2.37.1.14.4

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Multicast-Netzwerke

**Mögliche Werte:**

- Maximal 5 Ziffern zur Bezeichnung einer gültigen Port-Nummer

**Default:** 20000 bis 20031

#### 2.37.1.14.5 Loopback-Addr.

Hier können Sie optional eine Absenderadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absenderadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absenderadresse angeben.

**SNMP-ID:** 2.37.1.14.5

**Pfad Telnet:** /Setup/WLAN-Management/AP-Konfiguration/Multicast-Netzwerke

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige, gültige IP-Adresse

**Default:** 0.0.0.0

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, wird die zugehörige IP-Adresse verwendet. Name einer Loopback- Adresse.

## 2.37.10 Benachrichtigung

Dieses Menü enthält die Konfiguration des Benachrichtungs-Systems des WLAN-Managements.

**SNMP-ID:** 2.37.10

**Pfad Telnet:** /Setup/WLAN-Management

### 2.37.10.1 E-Mail

Aktiviert die Benachrichtigung über E-Mail.

**SNMP-ID:** 2.37.10.1

**Pfad Telnet:** /Setup/WLAN-Management/Benachrichtigung

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

### 2.37.10.3 E-Mail-Empfaenger

An diese E-Mail-Adresse werden die Benachrichtigungen über die Ereignisse im WLAN Controller gesendet.

**SNMP-ID:** 2.37.10.3

**Pfad Telnet:** /Setup/WLAN-Management/Benachrichtigung

**Mögliche Werte:**

- Gültige E-Mail-Adresse bis zu 63 ASCII-Zeichen

**Default:** Leer

Zur Nutzung der Benachrichtigung über E-Mail muss ein SMTP-Konto eingerichtet sein.

### 2.37.10.5 Sende-SNMP-Trap-fuer-Stationstabellenereignis

Geben Sie hier an, wann Sie über Ereignisse bezüglich der Einträge der Stationstabelle informiert werden.

**Pfad Telnet:** /Setup/WLAN-Management/Benachrichtigung/Sende-SNMP-Trap-fuer-Stationstabellenereignis

**Mögliche Werte:**

- Hinzufuegen/loeschen_eines_Eintrags
- alle_Ereignisse

**Default:** Hinzufuegen/loeschen_eines_Eintrags

### 2.37.10.2 Syslog

Aktiviert die Benachrichtigung über SYSLOG.

**SNMP-ID:** 2.37.10.2

**Pfad Telnet:** /Setup/WLAN-Management/Benachrichtigung

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

### 2.37.10.4 Erweitert

Hier definieren Sie, über welche Ereignisse Sie informiert werden möchten.

**SNMP-ID:** 2.37.10.4

**Pfad Telnet:** /Setup/WLAN-Management/Benachrichtigung

#### 2.37.10.4.1 Name

Wählt die Ereignisse, die über die eine Benachrichtigung erfolgen soll.

**SNMP-ID:** 2.37.10.4.1

**Pfad Telnet:** /Setup/WLAN-Management/Benachrichtigung/Erweitert

**Mögliche Werte:**

- E-Mail
- Syslog

**Default:** leer

**Besondere Werte:** Wert ist Fix

#### 2.37.10.4.2 Aktive-Radios

Aktiviert die Benachrichtigung über aktive Access Points.

**SNMP-ID:** 2.37.10.4.2

**Pfad Telnet:** /Setup/WLAN-Management/Benachrichtigung/Erweitert

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

#### 2.37.10.4.3 Fehlende-AP

Aktiviert die Benachrichtigung über verlorene Access Points.

**SNMP-ID:** 2.37.10.4.3

**Pfad Telnet:** /Setup/WLAN-Management/Benachrichtigung/Erweitert

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

#### 2.37.10.4.4 Neue-AP

Aktiviert die Benachrichtigung über neue Access Points.

**SNMP-ID:** 2.37.10.4.4

**Pfad Telnet:** /Setup/WLAN-Management/Benachrichtigung/Erweitert

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

## 2.37.34 WLC-Cluster

Dieses Menü enthält die Einstellungen für die Datenverbindungen und Statusverbindungen zwischen mehreren WLAN-Controllern.

**SNMP-ID:** 2.37.34

**Pfad Telnet:** /Setup/WLAN-Management

## 2.37.34.4 WLC-Discovery

In dieser Tabelle können Sie für jedes IP-Netzwerk separat die automatische Suche nach weiteren WLCs aktivieren oder deaktivieren.

**SNMP-ID:** 2.37.34.4

**Pfad Telnet:** /Setup/WLAN-Management/WLC-Cluster

### 2.37.34.4.1 Netzwerk

Wählen Sie hier eines der im Gerät definierten IP-Netzwerke aus, für welches Sie die automatische Suche nach weiteren WLAN-Controllern einstellen möchten.

**SNMP-ID:** 2.37.34.4.1

**Pfad Telnet:** /Setup/WLAN-Management/WLC-Cluster/WLC-Discovery

**Mögliche Werte:**

- Auswahl aus der Liste der definierten IP-Netzwerke, maximal 16 Zeichen.
- nein

**Default:** INTRANET: nein, DMZ: nein

### 2.37.34.4.2 Aktiv

Mit dieser Option aktivieren oder deaktivieren Sie die automatische Suche nach anderen WLAN-Controllern in dem ausgewählten IP-Netzwerk.

**SNMP-ID:** 2.37.34.4.2

**Pfad Telnet:** /Setup/WLAN-Management/WLC-Cluster/WLC-Discovery

**Mögliche Werte:**

- ja
- nein

**Default:** INTRANET: ja, DMZ: nein

Die automatische Suche nach anderen WLAN-Controllern ist eine Möglichkeit für den Aufbau des Datentunnels zwischen zwei WLCs. Wenn Sie diese Option deaktivieren, kann der WLAN-Controller über dieses Netzwerk keinen Datenkanal zu einem anderen WLC automatisch aufbauen, auch wenn Sie die Nutzung der Datentunnel generell aktiviert haben. Alternativ können Sie die gewünschten Gegenstellen in der statischen WLC-Liste definieren.

## 2.37.34.3 Statische WLC Liste

In dieser Tabelle können Sie weitere WLAN-Controller als Gegenstellen definieren, zu denen eine Verbindung aufgebaut werden kann. Der Controller baut zunächst einen Kontroll-Tunnel zu dieser Gegenstelle auf. Wenn Sie die Option für den Datentunnel aktiviert haben, baut der Controller anschließend automatisch einen Daten-Tunnel zu dieser Gegenstelle auf.

**SNMP-ID:** 2.37.34.3

**Pfad Telnet:** /Setup/WLAN-Management/WLC-Cluster

Die beiden WLAN-Controller können nur dann einen Daten-Tunnel aufbauen, wenn die Geräte die folgenden Voraussetzungen erfüllen:

- Sie haben die jeweilige Gegenstelle in beiden Geräten definiert.
- Die beiden Controller verfügen über ein Zertifikat der gleichen CA.

#### 2.37.34.3.1 IP-Adresse

Definieren Sie hier die IP-Adresse eines weiteren WLAN-Controllers, zu dem der konfigurierte Controller einen Daten-Tunnel aufbauen kann.

**SNMP-ID:** 2.37.34.3.1

**Pfad Telnet:** /Setup/WLAN-Management/WLC-Cluster/Statische WLC Liste

Die beiden WLAN-Controller können nur dann einen Daten-Tunnel aufbauen, wenn die Geräte die folgenden Voraussetzungen erfüllen:

- Sie haben die jeweilige Gegenstelle in beiden Geräten statisch oder über die automatische Suche definiert.
- Die beiden Controller verfügen über ein Zertifikat der gleichen CA.

#### 2.37.34.3.2 Loopback-Addr.

Hier können Sie optional eine Absenderadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absenderadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absenderadresse angeben.

**SNMP-ID:** 2.37.34.3.2

**Pfad Telnet:** /Setup/WLAN-Management/WLC-Cluster/Statische WLC Liste

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige, gültige IP-Adresse

**Default:** 0.0.0.0

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, wird die zugehörige IP-Adresse verwendet. Name einer Loopback- Adresse.

### 2.37.34.2 WLC-Daten-Tunnel-aktiviert

Mit dieser Option aktivieren oder deaktivieren Sie die Nutzung von Datentunneln zwischen mehreren WLAN-Controllern.

**SNMP-ID:** 2.37.34.2

**Pfad Telnet:** /Setup/WLAN-Management

**Mögliche Werte:**

- ja
- nein

**Default:** nein

## 2.37.27 Zentrales-Firmware-Management

Dieses Menü enthält die Konfiguration des zentralen Firmware-Managements.

**SNMP-ID:** 2.37.27

**Pfad Telnet:** /Setup/WLAN-Management

## 2.37.27.15 Firmware-Versionsverwaltung

Tabelle mit Gerätetyp, MAC-Adresse und Firmware-Version zur gezielten Steuerung der verwendeten Firmware-Dateien.

**SNMP-ID:** 2.37.27.15

**Pfad Telnet:** /Setup/WLAN-Management/Zentrales-Firmware-Management

### 2.37.27.15.2 Geraet

Wählen Sie hier aus, für welchen Gerätetyp die in diesem Eintrag spezifizierte Firmware-Version verwendet werden soll.

**SNMP-ID:** 2.37.27.15.2

**Pfad Telnet:** /Setup/WLAN-Management/Zentrales-Firmware-Management/Firmware-Versionsverwaltung

**Mögliche Werte:**

- Alle bzw. Auswahl aus der Liste der verfügbaren Gerätetypen.

**Default:** Alle-Geraete

### 2.37.27.15.3 MAC-Adresse

Wählen Sie hier aus, für welches Gerät (identifiziert anhand der MAC-Adresse) die in diesem Eintrag spezifizierte Firmware-Version verwendet werden soll.

**SNMP-ID:** 2.37.27.15.3

**Pfad Telnet:** /Setup/WLAN-Management/Zentrales-Firmware-Management/Firmware-Versionsverwaltung

**Mögliche Werte:**

- Gültige MAC-Adresse

**Default:** Leer

### 2.37.27.15.4 Version

Firmware-Version, welche für die in diesem Eintrag spezifizierten Geräte oder Gerätetypen verwendet werden soll.

**SNMP-ID:** 2.37.27.15.4

**Pfad Telnet:** /Setup/WLAN-Management/Zentrales-Firmware-Management/Firmware-Versionsverwaltung

**Mögliche Werte:**

- Firmware-Version in der Form X.XX

**Default:** Leer

## 2.37.27.16 Skriptverwaltung

Tabelle mit Skript-Dateiname und WLAN-Profil zur Zuordnung der Skripte zu einem WLAN-Profil.

Die Konfiguration eines Wireless Routers und Access Points in der Betriebsart "Managed" erfolgt über WLAN-Profile. Mit einem Skript können auch diejenigen Detail-Parameter der gemanagten Geräte eingestellt werden, die nicht im Rahmen der vorgegebenen Parameter eines WLAN-Profils verwaltet werden. Dabei erfolgt die Zuordnung ebenfalls über die WLAN-Profile, um für die Wireless Router und Access Points mit gleicher WLC-Konfiguration auch das gleiche Skript zu verwenden.

Da für jedes WLAN-Profil nur eine Skript-Datei angegeben werden kann, ist hier keine Versionierung möglich. Bei der Zuweisung eines Skripts zu einem Wireless Router oder Access Point wird allerdings eine MD5-Prüfsumme der Skript-Datei

gespeichert. Über diese Prüfsumme kann der WLAN-Controller bei einer neuen oder geänderten Skript-Datei mit gleichem Dateinamen daher feststellen, ob die Skript-Datei erneut übertragen werden muss.

**SNMP-ID:** 2.37.27.16

**Pfad Telnet:** /Setup/WLAN-Management/Zentrales-Firmware-Management

#### 2.37.27.16.1 Profil

Wählen Sie hier aus, für welches WLAN-Profil die in diesem Eintrag spezifizierte Skript-Datei verwendet werden soll.

**SNMP-ID:** 2.37.27.16.1

**Pfad Telnet:** /Setup/WLAN-Management/Zentrales-Firmware-Management/Skriptverwaltung

**Mögliche Werte:**

- Auswahl aus der Liste der definierten WLAN-Profile, maximal 31 ASCII-Zeichen

**Default:** Leer

#### 2.37.27.16.2 Name

Name der zu verwendenen Skript-Datei.

**SNMP-ID:** 2.37.27.16.2

**Pfad Telnet:** /Setup/WLAN-Management/Zentrales-Firmware-Management/Skriptverwaltung

**Mögliche Werte:**

- Dateiname in der Form *.lcs, maximal 63 ASCII-Zeichen

**Default:** Leer

### 2.37.27.11 Firmware-Depot-URL

Verzeichnis, in dem die aktuellen Firmware-Dateien liegen

**SNMP-ID:** 2.37.27.11

**Pfad Telnet:** /Setup/WLAN-Management/Zentrales-Firmware-Management

**Mögliche Werte:**

- URL in der Form Server/Verzeichnis oder http://Server/Verzeichnis

**Default:** Leer

### 2.37.27.25 Firmware-Loopback-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

**SNMP-ID:** 2.37.27.25

**Pfad Telnet:** /Setup/WLAN-Management/Zentrales-Firmware-Management

**Mögliche Werte:**

- Name eines definierten IP-Netzwerks.
- 'INT' für die IP-Adresse im ersten Netzwerk mit der Einstellung 'Intranet'.
- 'DMZ' für die IP-Adresse im ersten Netzwerk mit der Einstellung 'DMZ'.
- Name einer Loopback-Adresse.
- Beliebige andere IP-Adresse.

**Default:** Leer

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, wird die zugehörige IP-Adresse verwendet.

### 2.37.27.14 Maximale-Anzahl-geladener-Firmwares

Maximale Anzahl der Firmwareversionen im Speicher.

**SNMP-ID:** 2.37.27.14

**Pfad Telnet:** /Setup/WLAN-Management/Zentrales-Firmware-Management

**Mögliche Werte:**

- 1 bis 10

**Default:** 5

### 2.37.27.12 Script-Depot-URL

Pfad zum Verzeichnis mit den Skript-Dateien.

**SNMP-ID:** 2.37.27.12

**Pfad Telnet:** /Setup/WLAN-Management/Zentrales-Firmware-Management

**Mögliche Werte:**

- URL in der Form Server/Verzeichnis oder http://Server/Verzeichnis

**Default:** Leer

### 2.37.27.26 Skript-Loopback-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

**SNMP-ID:** 2.37.27.26

**Pfad Telnet:** /Setup/WLAN-Management/Zentrales-Firmware-Management

**Mögliche Werte:**

- Name eines definierten IP-Netzwerks.
- 'INT' fur die IP-Adresse im ersten Netzwerk mit der Einstellung 'Intranet'.
- 'DMZ' für die IP-Adresse im ersten Netzwerk mit der Einstellung 'DMZ'.
- Name einer Loopback-Adresse.
- Beliebige andere IP-Adresse.

**Default:** Leer

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, wird die zugehörige IP-Adresse verwendet.

### 2.37.27.13 Aktualisiere-Firmware-und-Skript-Information

Startet einen Update-Prozess über die verfügbaren Firmware- und Script-Informationen

**SNMP-ID:** 2.37.27.13

**Pfad Telnet:** /Setup/WLAN-Management/Zentrales-Firmware-Management

**Mögliche Werte:**

- Syntax: do Aktualisiere-Firmware-und-Skript-Information

Do-Commando

### 2.37.27.18 Aktualisierte-APs-neustarten

Reboot bei upgedateten Aps durchführen.

**SNMP-ID:** 2.37.27.18

**Pfad Telnet:** /Setup/WLAN-Management/Zentrales-Firmware-Management

**Mögliche Werte:**

- Syntax: do Aktualisierte-APs-neustarten

Do-Commando

## 2.37.17 RADIUS-Server

Standardmäßig übernimmt Ihr WLAN-Controller die Weiterleitung von Anfragen für die Konto-, bzw." " Zugangsverwaltung zum RADIUS-Server. Damit die APs den entsprechenden RADIUS- Server direkt" " ansprechen können, müssen Sie hier weitere Angaben machen.

**SNMP-ID:** 2.37.17

**Pfad Telnet:** /Setup/WLAN-Management

### 2.37.17.1 Typ

Type der RADIUS Anwendung

**SNMP-ID:** 2.37.17.1

**Pfad Telnet:** /Setup/WLAN-Management/RADIUS-Server

**Mögliche Werte:**

- Account
- Access

**Default:** leer

**Besondere Werte:** Wert ist Fix

nicht per LANconfig konfigurierbar

### 2.37.17.2 IP-Adresse

IP-Adresse des Radius Servers, die den AP mitgeteilt wird, um den RADIUS Server zu erreichen. Wird hier kein Wert angegeben, wird automatisch die IP-Adresse des Kontrollers genommen.

**SNMP-ID:** 2.37.17.2

**Pfad Telnet:** /Setup/WLAN-Management/RADIUS-Server

**Mögliche Werte:**

- Gültige IP-Adresse.

**Default:** Leer

nicht per LANconfig konfigurierbar

### 2.37.17.3 Port

Port-Nummer, die den AP mitgeteilt wird, um den RADIUS Server zu erreichen. Dieser Wert wird ignoriert, wenn keine IP-Adresse konfiguriert ist, da dann der Kontroller selbst als RADIUS-Server benutzt wird.

**SNMP-ID:** 2.37.17.3

**Pfad Telnet:** /Setup/WLAN-Management/RADIUS-Server

**Mögliche Werte:**

- Port-Nummer

**Default:** Leer

nicht per LANconfig konfigurierbar

### 2.37.17.4 Secret

Passwort für den RADIUS Dienst, wird keine IP-Adresse konfiguriert, wird vom Kontroller ein Zufallspasswort erzeugt, welches dann der AP benutzt um sich beim RADIUS Server des Kontroller zu authentisieren.

**SNMP-ID:** 2.37.17.4

**Pfad Telnet:** /Setup/WLAN-Management/RADIUS-Server

**Mögliche Werte:**

- max. 31 ASCII-Zeichen

**Default:** Leer

nicht per LANconfig konfigurierbar

## 2.37.20 Zugangs-Liste

Um den Datenverkehr zwischen dem Wireless-LAN und Ihrem lokalen Netz einzuschränken, können Sie für einzelne logische WLAN-Netze die MAC-Adress-Prüfung einschalten und in der folgenden Tabelle alle Stationen eintragen, welche Zugang zu diesen eingeschränkten logischen WLAN-Netzen erhalten.

**SNMP-ID:** 2.37.20

**Pfad Telnet:** /Setup/WLAN-Management

### 2.37.20.1 MAC-Adresse

Geben Sie hier die MAC-Adresse einer Station ein.

**SNMP-ID:** 2.37.20.1

**Pfad Telnet:** /Setup/WLAN-Management/Zugangs-Liste

**Mögliche Werte:**

- Gültige MAC-Adresse

**Default:** Leer

Jede Netzwerkkarte hat eine eigene, weltweit eindeutige MAC-Adresse. Diese Adresse ist eine 12-stellige Hexadezimalzahl (zum Beispiel 00A057010203). Sie finden diese Adresse meistens als Aufdruck auf der Netzwerkkarte selbst.

### 2.37.20.2 Name

Sie können zu jeder Station einen beliebigen Namen und einen Kommentar eingeben.

Dies ermöglicht Ihnen eine einfachere Zuordnung der MAC-Adressen zu bestimmten Stationen oder Benutzern.

**SNMP-ID:** 2.37.20.2

**Pfad Telnet:** /Setup/WLAN-Management/Zugangs-Liste

**Mögliche Werte:**

- max. 32 Zeichen

**Default:** Leer

### 2.37.20.3 Kommentar

Kommentar zu diesem Eintrag

**SNMP-ID:** 2.37.20.3

**Pfad Telnet:** /Setup/WLAN-Management/Zugangs-Liste

**Mögliche Werte:**

- max. 30 Zeichen

**Default:** Leer

### 2.37.20.4 WPA-Passphrase

Hier können Sie optional für jede physikalische Adresse (MAC) eine separate Passphrase eintragen, die in den 802.11i/WPA/AES-PSK gesicherten Netzwerken benutzt wird. Ohne die Angabe einer gesonderten Passphrase für diese MAC-Adresse werden die im Bereich '802.11i/WEP' für jedes logische Wireless-LAN-Netzwerk hinterlegten Passphrases verwendet.

**SNMP-ID:** 2.37.20.4

**Pfad Telnet:** /Setup/WLAN-Management/Zugangs-Liste

**Mögliche Werte:**

- ASCII-Zeichenkette mit einer Lange von 8 bis 63 Zeichen

**Default:** Leer

**Besondere Werte:** 0

Bei WEP gesicherten Netzwerken hat dieses Feld keine Bedeutung.

### 2.37.20.5 Tx-Limit

Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients. Ein Client übermittelt seine eigene Einstellung bei der Anmeldung an die Basisstation. Diese bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

**SNMP-ID:** 2.37.20.5

**Pfad Telnet:** /Setup/WLAN-Management/Zugangs-Liste

**Mögliche Werte:**

- 0 bis 65535 kbit/s

**Default:** 0

**Besondere Werte:** 0: keine Begrenzung

Die Bedeutung der Werte Rx und Tx ist abhängig von der Betriebsart des Gerätes. In diesem Fall als Access Point steht Rx für „Daten senden“ und Tx für „Daten empfangen“.

### 2.37.20.6 Rx-Limit

Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients.

Ein Client übermittelt seine eigene Einstellung bei der Anmeldung an die Basisstation. Diese bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

**SNMP-ID:** 2.37.20.6

**Pfad Telnet:** /Setup/WLAN-Management/Zugangs-Liste

**Mögliche Werte:**

- 0 bis 65535 kbit/s

**Default:** 0

**Besondere Werte:** 0: keine Begrenzung

Die Bedeutung der Werte Rx und Tx ist abhängig von der Betriebsart des Gerätes. In diesem Fall als Access Point steht Rx für „Daten senden“ und Tx für „Daten empfangen“.

### 2.37.20.7 VLAN-Id

Diese VLAN-ID wird Paketen zugewiesen, die von dem Client mit der eingetragenen MAC-Adresse empfangen wurden.

**SNMP-ID:** 2.37.20.7

**Pfad Telnet:** /Setup/WLAN-Management/Zugangs-Liste

**Mögliche Werte:**

- 0 bis 4096

**Default:** 0

## 2.39 Zertifikate

Dieses Menü enthält die Konfiguration der Zertifikate.

**SNMP-ID:** 2.39

**Pfad Telnet:** /Setup

## 2.39.1 SCEP-Client

Dieses Menü enthält die Konfiguration des SCEP-Clients.

**SNMP-ID:** 2.39.1

**Pfad Telnet:** /Setup/Zertifikate

### 2.39.1.1 Aktiv

Schaltet die Nutzung von SCEP ein oder aus.

**SNMP-ID:** 2.39.1.1

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

**Besondere Werte:** No

### 2.39.1.9 Aktualisieren

Startet manuell die Anfrage nach einem neuen Systemzertifikat, unabhängig von der verbleibenden Gültigkeitsdauer. Dabei wird ein neues Schlüsselpaar erzeugt.

**SNMP-ID:** 2.39.1.9

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client

### 2.39.1.12 Ausstehende-Anfragen-Prüfen-Intervall

Intervall in Sekunden für das Prüfen von ausstehenden Zertifikatsanfragen.

**SNMP-ID:** 2.39.1.12

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 101

### 2.39.1.10 Bereinige-SCEP-Dateisystem

Startet die Bereinigung des SCEP-Dateisystems.

gelöscht werden: RA-Zertifikate, ausstehende Zertifikatsanfragen, neue und inaktive CA-Zertifikate, neue und inaktive private Schlüssel.

erhalten bleiben: aktuell im VPN-Betrieb genutzte Systemzertifikate, private Schlüssel dazu und die aktuell im VPN-Betrieb genutzten CA-Zertifikate.

**SNMP-ID:** 2.39.1.10

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client

### 2.39.1.3 CA-Zertifikate-Aktualisieren-Vor-Ablauf

Vorlaufzeit in Tagen zur rechtzeitigen Abholung neuer RA/CA-Zertifikate.

**SNMP-ID:** 2.39.1.3

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 3

### 2.39.1.8 Reinit

Startet die manuelle Re-Initialisierung der SCEP-Parameter. Dabei werden wie bei der gewöhnlichen SCEP-Initialisierung auch die notwendigen RA- und CA-Zertifikate von der CA abgerufen und so im Dateisystem des LANCOM Wireless abgelegt, dass Sie noch nicht für die Nutzung im VPN-Betrieb bereit stehen. Sofern das vorhandene Systemzertifikat zum abgerufenen CA-Zertifikat passt, können Systemzertifikat, CAZertifikat und privater Geräteschlüssel für den VPN-Betrieb genutzt werden. Sofern die vorhandenen Systemzertifikate nicht zum abgerufenen CA-Zertifikat passen, muss zunächst eine neue Zertifikatsanfrage beim SCEP-Server gestellt werden. Erst wenn so ein neues, zum CA-Zertifikat passendes Systemzertifikat ausgestellt und abgerufen wurde, können Systemzertifikat, CA-Zertifikat und privater Geräteschlüssel für den VPN-Betrieb genutzt werden.

**SNMP-ID:** 2.39.1.8

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client

### 2.39.1.2 CA-Zertifikate-Aktualisieren-Vor-Ablauf

Vorlaufzeit in Tagen zur rechtzeitigen Abholung neuer RA/CA-Zertifikate.

**SNMP-ID:** 2.39.1.2

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** leer

### 2.39.1.13 Trace-Stufe

Für den SCEP-Client-Trace kann die Ausgabe von Tracemeldungen auf einen bestimmten Inhalt beschränkt werden. Dazu wird ein Wert angegeben, bis zu welcher Stufe die Pakete im Trace ausgegeben werden sollen.

**SNMP-ID:** 2.39.1.13

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client

**Mögliche Werte:**

- alles: alle Tracemeldungen, auch reine Info- und Debug-Meldungen
- reduziert: nur Fehler- und Warnmeldungen
- nur-Fehler: nur Fehlermeldungen

**Default:**

alles

### 2.39.1.11 Wiederholen-Nach-Fehler-Intervall

Intervall in Sekunden für Wiederholungen nach jeglicher Art von Fehler.

**SNMP-ID:** 2.39.1.11

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 22

### 2.39.1.7 Zertifikate

Hier können Sie Zertifikate konfigurieren bzw. Neue hinzufügen.

**SNMP-ID:** 2.39.1.7

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client

#### 2.39.1.7.1 Name

Konfigurationsname des Zertifikats.

**SNMP-ID:** 2.39.1.7.1

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client/Zertifikate

**Mögliche Werte:**

- max. 16 Zeichen

**Default:** leer

#### 2.39.1.7.2 CADN

Distinguished Name der CA. Über diesen Parameter erfolgt einerseits die Zuordnung von CAs zu Systemzertifikaten (und umgekehrt). Andererseits spielt dieser Parameter auch eine Rolle bei der Bewertung, ob erhaltene bzw. vorhandene Zertifikate der Konfiguration entsprechen.

**SNMP-ID:** 2.39.1.7.2

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client/Zertifikate

**Mögliche Werte:**

- max. 251 Zeichen

**Default:** leer

#### 2.39.1.7.3 Subject

Distinguished Name des Subjects des Antragstellers.

**SNMP-ID:** 2.39.1.7.3

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client/Zertifikate

**Mögliche Werte:**

- max. 251 Zeichen

**Default:** leer

#### 2.39.1.7.4 ChallengePwd

Kennwort (für das automatische Ausstellen der Geräte-Zertifikate auf dem SCEP-Server).

**SNMP-ID:** 2.39.1.7.4

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client/Zertifikate

**Mögliche Werte:**

- max. 251 Zeichen

**Default:** leer

#### 2.39.1.7.5 SubjectAltName

Weitere Angaben zum Requester, z. B. Domain oder IP-Adresse.

**SNMP-ID:** 2.39.1.7.5

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client/Zertifikate

**Mögliche Werte:**

- max. 251 Zeichen

**Default:** leer

#### 2.39.1.7.6 KeyUsage

Beliebige kommaseparierte Kombination aus: digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign, cRLSign, encipherOnly, decipherOnly, critical (möglich aber nicht empfohlen)

**SNMP-ID:** 2.39.1.7.6

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client/Zertifikate

**Mögliche Werte:**

- max. 251 Zeichen

**Default:** leer

#### 2.39.1.7.7 Systemzertifikate-Schlüssellänge

Länge der Schlüssel, die für das Gerät selbst erzeugt werden.

**SNMP-ID:** 2.39.1.7.7

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client/Zertifikate

**Mögliche Werte:**

- 31 oder größer

**Default:** 0

#### 2.39.1.7.8 Verwendung

Gibt den Verwendungszweck der eingetragenen Zertifikate an. Die hier eingetragenen Zertifikate werden dann nur für den entsprechenden Verwendungszweck abgefragt.

**SNMP-ID:** 2.39.1.7.8

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client/Zertifikate

**Mögliche Werte:**

- VPN

**Default:** VPN

#### 2.39.1.7.9 Extended-KeyUsage

Beliebige kommaseparierte Kombination aus: critical, serverAuth, clientAuth, codeSigning, emailProtection, timeStamping, msCodeInd, msCodeCom, msCTLSign, msSGC, msEFS, nsSGC, 1.3.6.1.5.5.7.3.18 für WLAN-Controller, 1.3.6.1.5.5.7.3.19 für Access Points im Managed-Modus

**SNMP-ID:** 2.39.1.7.9

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client/Zertifikate

**Mögliche Werte:**

- max. 251 Zeichen

**Default:** leer

### 2.39.1.14 CAs

In dieser Tabelle definieren sie die verfügbaren CAs.

**SNMP-ID:** 2.39.1.14

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client/CAs

#### 2.39.1.14.1 Name

Geben Sie einen Namen ein, der diese Konfiguration kennzeichnet.

**SNMP-ID:** 2.39.1.14.1

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client/Zertifikate/Name

**Mögliche Werte:** max. 16 alphamnumerische Zeichen

**Default:** leer

#### 2.39.1.14.11 Loopback-Addr.

Geben Sie eine Loopback-Adresse an.

**SNMP-ID:** 2.39.1.14.11

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client/Zertifikate/Loopback-Addr.

**Mögliche Werte:** max. 16 Zeichen

**Default:** leer

#### 2.39.1.14.2 URL

Hier muss die sogenannte 'Enrollment-URL' eingegeben werden. Um ein Zertifikat zu beantragen, muss der Router die Zertifizierungsstelle (CA - Certificate Authority) kontaktieren. Dazu wird eine URL benötigt, die von Anbieter zu Anbieter unterschiedlich ist und meist anhand der Dokumentation zur CA herauszufinden ist. Beispiel: http:/ /postman/certsrv/mscep/mscep.dll

**SNMP-ID:** 2.39.1.14.2

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client/Zertifikate/URL

**Mögliche Werte:**

- max. 251 alphanumerische Zeichen

**Default:** leer

#### 2.39.1.14.3 DN

Hier muss der 'Distinguished Name' eingegeben werden. Hierüber erfolgt einerseits die Zuordnung von CAs zu Systemzertifikaten (und umgekehrt). Andererseits spielt dieser Parameter auch eine Rolle bei der Bewertung ob erhaltene bzw. vorhandene Zertifikate der Konfiguration entsprechen. Es handelt sich um eine durch Komma oder Schrägstrich separierte Auflistung, in der Name, Abteilung, Bundesland und Land des Gateways angegeben werden können. Die folgenden Beispiele zeigen, wie der Eintrag aussehen kann: CN=myCACN, DC=mscep, DC=ca, C=DE, ST=berlin, O=myOrg /CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE

**SNMP-ID:** 2.39.1.14.3

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client/Zertifikate/DN

**Mögliche Werte:**

- max. 251 alphanumerische Zeichen

**Default:** leer

#### 2.39.1.14.4 Enc-Alg

Wählen Sie hier den Verschlüsselungs-Algorithmus (Encryption-Algorithmus) zur Verschlüsselung innerhalb des SCEP-Protokolls (Simple Certificate Enrollment Protocol) aus. Sowohl bei der Zertifizierungsstelle (CA), als auch beim Zertifikatnehmer (Client) muss der Algorithmus unterstützt werden. Es stehen drei Verfahren zur Auswahl:

**SNMP-ID:** 2.39.1.14.4

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client/Zertifikate/Enc-Alg

**Mögliche Werte:**

- **DES** - Data-Encryption-Standard: Der DES-Algorithmus benutzt einen 64-Bit-Schlüssel. Dies ist die SCEP-Standard-Verschlüsselung. DES ist ein vom amerikanischen National Bureau of Standards (NBS) entwickelter Algorithmus. Der DES-Algorithmus benutzt einen 64-Bit-Schlüssel, der Kombinationen von Substitutionschiffre, Transpositionschiffre und Exklusiv-Oder-Funktionen (XOR) ermöglicht. Der 64-Bit-Datensatz besteht aus einer effektiven Schlüssellänge von 56 Bits und 8 Parity-Bits, das zugrunde liegende Verschlüsselungsverfahren heißt Lucifer. Das Verfahren, wurde 1974 veröffentlicht und in den USA als ANSI-Standard normiert (ANSI X3.92-1981), er ist außerdem von der ISO unter ISO 8227 spezifiziert. Er wird seit vielen Jahren insbesondere bei der Übertragung sensitiver Daten, wie sie in Kapitalmärkten und auf Smartcards vorkommen, eingesetzt und kann als internationaler Quasi-Standard bezeichnet werden.
- **3DES** - Dreifach-DES: Dies ist eine verbesserte DES-Verschlüsselung, die 2 64-Bit-Schlüssel verwendet.
- **BLOWFISH**: Der BLOWFISH-Algorithmus benutzt eine variable Schlüssellänge von 32 bis 448 Bit und zeichnet sich durch einen schnellen und sehr sicheren Algorithmus aus. Er hat wesentliche Vorteile gegenüber anderen symmetrischen Verfahren wie DES und 3DES. 1993 von Bruce Schneier entwickelt, ist Blowfish ein symmetrisches Verschlüsselungsverfahren, das sich durch einen schnellen und sehr sicheren Algorithmus auszeichnet, besonders in Verbindung mit 32-Bit-Rechnern. Das Verfahren arbeitet mit einer Blocklänge von 64 Bit und einer variablen Schlüssellänge von 32 Bit bis 448 Bit. Blowfish ist sehr effizient und arbeitet mit XOR-Verknüpfungen und Additionen 32-Bit-Wörtern. Er gilt als sicher und hat wesentliche Vorteile gegenüber anderen symmetrischen Verfahren wie DES und 3DES.
- **AES128:** Der Advanced Encryption Standard (AES) besitzt eine variable Blockgröße von 128, 192 oder 256 Bit und eine variable Schlüssellänge von 128, 192 oder 256 Bit und bietet ein sehr hohes Maß an Sicherheit.

**Default:** des

Sie sollten nach Möglichkeit eines der beiden letzteren Verfahren (3DES oder BLOWFISH) einsetzen, wenn dieses von CA und allen Clients unterstützt wird. Als Standard ist hier DES-Verschlüsselung voreingestellt, um die Interoperabilität zu wahren.

#### 2.39.1.14.5 Identifier

Hier kann ein zusätzlicher Identifier eingegeben werden. Dieser Wert wird von manchen Webservern benötigt um die CA zuordnen zu können.

**SNMP-ID:** 2.39.1.14.5

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client/Zertifikate/Identifier

**Mögliche Werte:**

- max. 251 alphanumerische Zeichen

**Default:** leer

#### 2.39.1.14.6 CA-Signaturalgorithmus

Wählen Sie hier den Signaturalgorithmus aus, den die Zertifizierungsstelle (CA) zur Signatur (Unterschrift) der Zertifikate verwenden soll. Sowohl bei der CA als auch beim Zertifikatnehmer (Client) muss das Verfahren unterstützt werden, da der Client die Integrität des Zertifikates anhand der Signatur prüft. Es stehen zwei weit verbreitete kryptographische Hash-Funktionen zur Auswahl:

**SNMP-ID:** 2.39.1.14.6

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client/Zertifikate/CA-Signaturalgorithmus

**Mögliche Werte:**

- **MD5** (Standard) - Message Digest Algorithm 5 erzeugt einen 128-Bit-Hashwert. MD5 wurde 1991 von Ronald L. Rivest entwickelt. Aus dem Ergebnis können keine Rückschlüsse auf den Schlüssel erfolgen. Dem Verfahren nach wird aus einer beliebig langen Nachricht eine 128 Bit lange Information, der Message Digest gebildet, der an die unverschlüsselte Nachricht angehangen wird. Der Empfänger vergleicht den Message Digest mit dem von ihm aus der Information ermittelten Wert.
- **SHA1** - Secure Hash Algorithm 1 erzeugt einen 160-Bit-Hashwert. Diese dienen zur Berechnung eines eindeutigen Prüfwerts für beliebige Daten. Meist handelt es sich dabei um Nachrichten. Es soll praktisch unmöglich sein, zwei verschiedene Nachrichten mit dem gleichen SHA-Wert zu finden. Die Länge des Hashwertes liegt beim SHA-Algorithmus bei 160 Bit.

**Default:** aus

#### 2.39.1.14.7 RA-Autoapprove

Bei Auswahl dieser Option werden Neuanträge, bei bereits vorliegendem Systemzertifikat, mit diesem unterschrieben. Die Option muss sowohl beim Zertifikatnehmer (Client), als auch bei der Zertifizierungsstelle (CA-Server) eingeschaltet werden. Die CA authentifiziert den Client in diesem Falle ohne Angabe eines Challenge-Passwortes, sondern nur anhand des Zertifikats.

**SNMP-ID:** 2.39.1.14.7

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client/Zertifikate/RA-Autoapprove

**Mögliche Werte:**

- ja
- nein

**Default:** nein

#### 2.39.1.14.8 CA-Fingerprintalgorithmus

Wählen Sie hier einen Fingerprint-Algorithmus aus, den die Zertifizierungsstelle (CA) zur Berechnung des Fingerprints (Fingerabdruck) der Signatur (Unterschrift) verwenden soll. Sowohl bei der CA als auch beim Zertifikatnehmer (Client) muss das Verfahren unterstützt werden.

Der Fingerprint ist eine Hash-Wert von Daten (Schlüssel, Zertifikat, etc.), d.h. eine kurze Zahlenfolge die zur Überprüfung der Integrität der Daten benutzt werden kann.

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client/Zertifikate/CA-Fingerprintalgorithmus

**Mögliche Werte:**

- aus
- **MD5** (Standard) - Message Digest Algorithm 5 erzeugt einen 128-Bit-Hashwert.
- **SHA1** - Secure Hash Algorithm 1 erzeugt einen 160-Bit-Hashwert.

**Default:** aus

#### 2.39.1.14.9 CA-Fingerprint

Hier kann der CA-Fingerprint eingetragen werden. Es handelt sich hierbei um den Hash-Wert, der sich bei Verwendung des Fingerprint-Algorithmus ergibt. Anhand dieses Hash-Wertes kann die Authentizität des erhaltenen CA-Zertifikats gesichert werden (wenn ein CA-Fingerprintalgorithmus gewählt ist). Mögliche Delimiter sind: ' :' ' -' ' ,' ' '

**SNMP-ID:** 2.39.1.14.9

**Pfad Telnet:** /Setup/Zertifikate/SCEP-Client/Zertifikate/CA-Fingerprint

**Mögliche Werte:**

- max. 59 alphanumerische Zeichen

**Default:** leer

## 2.39.2 SCEP-CA

Dieses Menü enthält die Einstellungen für die SCEP-CA.

**SNMP-ID:** 2.39.2

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA

### 2.39.2.1 Aktiv

Aktivieren oder deaktivieren Sie den SCEP-Client.

**SNMP-ID:** 2.39.2.1

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Aktiv

**Mögliche Werte:**

- ja
- nein

**Default:** nein

### 2.39.2.7 Fingerabdruck-Algorithmus

Wählen Sie hier einen Fingerprint-Algorithmus aus, den die Zertifizierungsstelle (CA) zur Berechnung des Fingerprints (Fingerabdruck) der Signatur (Unterschrift) verwenden soll. Sowohl bei der CA als auch beim Zertifikatnehmer (Client) muss das Verfahren unterstützt werden. Der Fingerprint ist eine Hash-Wert von Daten (Schlüssel, Zertifikat, etc.), d.h. eine kurze Zahlenfolge die zur überprüfung der Integrität der Daten benutzt werden kann.

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Fingerabdruck-Algorithmus

**Mögliche Werte:**

- MD5: Message Digest Algorithm 5 erzeugt einen 128-Bit-Hashwert
- SHA1: Secure Hash Algorithm 1 erzeugt einen 160-Bit-Hashwert

**Default:** MD5

### 2.39.2.4 RA-Automatische-Authentifikation

Bei Auswahl dieser Option werden Neuanträge, bei bereits vorliegendem Systemzertifikat, mit diesem unterschrieben. Die Option muss sowohl beim Zertifikatnehmer (Client), als auch bei der Zertifizierungsstelle (CA-Server) eingeschaltet werden. Die CA authentifiziert den Client in diesem Falle ohne Angabe eines Challenge-Passwortes, sondern nur anhand des Zertifikats.

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/RA-Automatische-Authentifikation

**Mögliche Werte:**

- ja
- nein

**Default:** ja

### 2.39.2.9 Reinitialisiere

Mit diesem Befehl reinitialisieren Sie die CA. Das Gerät prüft die Konfiguration und die Zertifikate, wenn nötig aktualisiert das Gerät die entsprechenden Werte bzw. Dateien.

Führen Sie diesen Befehl aus, wenn die CA wegen eines Konfigurationsfehlers nicht läuft, um die erneute Überprüfung nach einer Konfigurationsänderung auszulösen.

**SNMP-ID:** 2.39.2.9

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Reinitialisiere

### 2.39.2.6 Signatur-Algorithmus

Wählen Sie hier den Signaturalgorithmus aus, den die Zertifizierungsstelle (CA) zur Signatur (Unterschrift) der Zertifikate verwenden soll. Sowohl bei der CA als auch beim Zertifikatnehmer (Client) muss das Verfahren unterstützt werden, da der Client die Integrität des Zertifikates anhand der Signatur prüft. Es stehen zwei weit verbreitete kryptographische Hash-Funktionen zur Auswahl.

**SNMP-ID:** 2.39.2.6

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Signatur-Algorithmus

**Mögliche Werte:**

- aus
- **SHA1** - Secure Hash Algorithm 1 erzeugt einen 160-Bit-Hashwert. Diese dienen zur Berechnung eines eindeutigen Prüfwerts für beliebige Daten. Meist handelt es sich dabei um Nachrichten. Es soll praktisch unmöglich sein, zwei verschiedene Nachrichten mit dem gleichen SHA-Wert zu finden. Die Länge des Hashwertes liegt beim SHA-Algorithmus bei 160 Bit.
- **MD5** (Standard) - Message Digest Algorithm 5 erzeugt einen 128-Bit-Hashwert. MD5 wurde 1991 von Ronald L. Rivest entwickelt. Aus dem Ergebnis können keine Rückschlüsse auf den Schlüssel erfolgen. Dem Verfahren nach wird aus einer beliebig langen Nachricht eine 128 Bit lange Information, der Message Digest gebildet, der an die unverschlüsselte Nachricht angehangen wird. Der Empfänger vergleicht den Message Digest mit dem von ihm aus der Information ermittelten Wert.

**Default:** aus

### 2.39.2.3 Verschluesselungsalgorithmus

Wählen Sie hier den Verschlüsselungs-Algorithmus (Encryption-Algorithmus) zur Verschlüsselung innerhalb des SCEP-Protokolls (Simple Certificate Enrollment Protocol) aus. Sowohl bei der Zertifizierungsstelle (CA), als auch beim Zertifikatnehmer (Client) muss der Algorithmus unterstützt werden.

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Verschluesselungsalgorithmus

**Mögliche Werte:**

- DES: Data-Encryption-Standard: Der DES-Algorithmus benutzt einen 64-Bit-Schlüssel. Dies ist die SCEP-Standard-Verschlüsselung.
- 3DES: Dreifach-DES: Dies ist eine verbesserte DES-Verschlüsselung, die 2 64-Bit-Schlüssel verwendet.
- BLOWFISH: Der BLOWFISH-Algorithmus benutzt eine variable Schlüssellänge von 32 bis 448 Bit und zeichnet sich durch einen schnellen und sehr sicheren Algorithmus aus. Er hat wesentliche Vorteile gegenüber anderen symmetrischen Verfahren wie DES und 3DES.

- AES128: Der Advanced Encryption Standard (AES) besitzt eine variable Blockgröße von 128, 192 oder 256 Bit und eine variable Schlüssellänge von 128, 192 oder 256 Bit und bietet ein sehr hohes Maß an Sicherheit.

**Default:** DES

## 2.39.2.2 CA-Zertifikate

Dieses Menü enthält die Einstellungen für die CA-Zertifikate.

**SNMP-ID:** 2.39.2.2

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/CA-Zertifikate

#### 2.39.2.2.3 Alternativer-Name

Hier kann ein alternativer 'Subject-Name' eingegeben werden.

**Beispiele:** critical,DNS:host.company.de IP:10.10.10.10 DNS:host.company.de, IP:10.10.10.10 UFQDN:email:name@company.de

**SNMP-ID:** 2.39.2.2.3

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/CA-Zertifikate/Alternativer-Name

#### 2.39.2.2.1 CA-Distinguished-Name

Hier muss der 'Distinguished Name' eingegeben werden. Hierüber erfolgt einerseits die Zuordnung von CAs zu Systemzertifikaten (und umgekehrt). Andererseits spielt dieser Parameter auch eine Rolle bei der Bewertung ob erhaltene bzw. vorhandene Zertifikate der Konfiguration entsprechen. Es handelt sich um eine durch Komma oder Schrägstrich separierte Auflistung, in der Name, Abteilung, Bundesland und Land des Gateways angegeben werden können. Die folgenden Beispiele zeigen, wie der Eintrag aussehen kann: CN=myCACN, DC=mscep, DC=ca, C=DE, ST=berlin, O=myOrg /CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE

**SNMP-ID:** 2.39.2.2.1

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/CA-Zertifikate/CA-Distinguished-Name

**Mögliche Werte:**

- max. 251 Zeichen

**Default:** leer

#### 2.39.2.2.6 CA-Zertifikate-aktualisieren-vor-Ablauf

Tragen Sie hier den Zeitraum für die 'Erneuerung vor Ablauf' in Tagen ein.

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/CA-Zertifikate/CA-Zertifikate-aktualisieren-vor-Ablauf

**Mögliche Werte:**

- maximal 2 numerische Zeichen

**Default:** 4

#### 2.39.2.2.9 Erstelle-neue-CA-Zertifikate

Führen Sie diesen Befehl aus, wenn Sie die Konfiguration der CA geändert haben.

Die CA erstellt nur dann automatisch neue Zertifikate, wenn die alten abgelaufen oder gar keine vorhanden sind. WennSie nachträglich die Schlüssellänge, den Namen oder andere Werte der CA-Zertifikate ändern, erstellen Sie über diesen Befehl die entsprechenden Zertifikatsdateien neu.

**SNMP-ID:** 2.39.2.2.9

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/CA-Zertifikate/Erstelle-neue-CA-Zertifikate

#### 2.39.2.2.10 Erstelle-PKCS12-Backup-Dateien

Für die Wiederherstellung der CA bzw. der RA im Backup-Fall werden die jeweiligen Root-Zertifikate mit den privaten Schlüsseln benötigt, die beim Systemstart automatisch vom WLAN Controller erzeugt werden.

Damit diese vertraulichen Daten auch beim Export aus dem Gerät heraus geschützt bleiben, werden sie zunächst in einen PCKS12-Container gespeichert, der mit einer Passphrase geschützt ist.

Mit dem Befehl "Erstelle-PKCS12-Backup-Dateien" starten Sie den Export. Geben Sie als Parameter die gewünschte Passphrase an.

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/CA-Zertifikate/Erstelle-PKCS12-Backup-Dateien

#### 2.39.2.2.5 Gueltigkeitsdauer

Tragen Sie hier den Gültigkeitszeitraum für das ausgestellte Zertifikat in Tagen ein.

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/CA-Zertifikate/Gueltigkeitsdauer

**Mögliche Werte:**

- maximal 5 numerische Zeichen

**Default:** 1100

#### 2.39.2.2.8 RA-Distinguished-Name

Hier muss der 'Distinguished Name' eingegeben werden. Hierüber erfolgt einerseits die Zuordnung von CAs zu Systemzertifikaten (und umgekehrt). Andererseits spielt dieser Parameter auch eine Rolle bei der Bewertung ob erhaltene bzw. vorhandene Zertifikate der Konfiguration entsprechen. Es handelt sich um eine durch Komma oder Schrägstrich separierte Auflistung, in der Name, Abteilung, Bundesland und Land des Gateways angegeben werden können. Die folgenden Beispiele zeigen, wie der Eintrag aussehen kann: CN=myCACN, DC=mscep, DC=ca, C=DE, ST=berlin, O=myOrg /CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE

**SNMP-ID:** 2.39.2.2.8

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/CA-Zertifikate/RA-Distinguished-Name

**Mögliche Werte:**

- max. 251 Zeichen

**Default:** leer

#### 2.39.2.2.4 RSA-Schluessellaenge

Hier muss die Schlüssellänge eingegeben werden. Dieser Wert bestimmt für neue Schlüssel die Länge in Bits.

**SNMP-ID:** 2.39.2.2.4

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/CA-Zertifikate/RSA-Schluessellaenge

**Mögliche Werte:**

- 1024
- 2048
- 3072
- 4096
- 8192

**Default:** 2048

Je nach zur Verfügung stehender Systemleistung dauert die Berechnung unterschiedlich lange, je größer die Anzahl Bits umso länger.

#### 2.39.2.2.11 Zertifikate-aus-Backup-wiederherstellen

Mit diesem Befehl können Sie die beiden PKCS12-Dateien mit den jeweiligen Root-Zertifikaten und den privaten Schlüsseln der CA bzw. der RA im Backup-Fall wiederherstellen.

**SNMP-ID:** 2.39.2.2.11

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/CA-Zertifikate/Zertifikate-aus-Backup-wiederherstellen

### 2.39.2.5 Client-Zertifikate

Dieses Menü enthält die Einstellungen für die Client-Zertifikate.

**SNMP-ID:** 2.39.2.5

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Client-Zertifikate

#### 2.39.2.5.4 Allgemeines-Challenge-Passwort

Hier kann ein weiteres 'Passwort' eingetragen werden, das an die CA übertragen wird. Dieses kann standardmäßig zur Authentifizierung von Rücknahme-Anträgen benutzt werden. Auf CAs mit Microsoft-SCEP (mscep) können (falls dort aktiviert) die von der CA vergebenen Einmalpasswörter zur Antragsauthentifizierung eingetragen.

**SNMP-ID:** 2.39.2.5.4

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Client-Zertifikate/Allgemeines-Challenge-Passwort

**Mögliche Werte:**

- max. 16 Zeichen

**Default:** XuL[ksKcC3+'%PA2

#### 2.39.2.5.1 Gueltigkeitsdauer

Bestimmen Sie hier die Gültigkeitsdauer des Zertifikats in Tagen.

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Client-Zertifikate/Gueltigkeitsdauer

**Mögliche Werte:**

- maximal 5 numerische Zeichen

**Default:** 365

#### 2.39.2.5.3 Challenge-Passwoerter

In dieser Tabelle erhalten Sie einen Überblick über die Challenge-Passwörter.

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Client-Zertifikate/Challenge-Passwoerter

##### 2.39.2.5.3.1 Index

Geben Sie hier den Index für das Challenge-Passwort an.

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Client-Zertifikate/Gueltigkeitsdauer/Index

**Mögliche Werte:**

- maximal 10 numerische Zeichen

**Default:** leer

#### 2.39.2.5.3.2 Subject-Distinguished-Name

Hier muss der 'Distinguished Name' eingegeben werden. Hierüber erfolgt einerseits die Zuordnung von CAs zu Systemzertifikaten (und umgekehrt). Andererseits spielt dieser Parameter auch eine Rolle bei der Bewertung ob erhaltene bzw. vorhandene Zertifikate der Konfiguration entsprechen. Es handelt sich um eine durch Komma oder Schrägstrich separierte Auflistung, in der Name, Abteilung, Bundesland und Land des Gateways angegeben werden können. Die folgenden Beispiele zeigen, wie der Eintrag aussehen kann: CN=myCACN, DC=mscep, DC=ca, C=DE, ST=berlin, O=myOrg /CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE

**SNMP-ID:** 2.39.2.5.3.2

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Client-Zertifikate/Gueltigkeitsdauer/Subject-Distinguished-Name

**Mögliche Werte:**

- max. 251 Zeichen

**Default:** leer

#### 2.39.2.5.3.3 MAC-Adresse

Tragen Sie hier die MAC-Adresse des Clients ein, dessen Passwort in der Challange-Passwort-Tabelle verwaltet wird.

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Client-Zertifikate/Gueltigkeitsdauer/MAC-Adresse

**Mögliche Werte:**

- maximal 12 alphanumerische Zeichen

**Default:** leer

#### 2.39.2.5.3.4 Challenge

Geben Sie hier die Challenge (Passwort) für den Client an.

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Client-Zertifikate/Gueltigkeitsdauer/Challenge

**Mögliche Werte:**

- maximal 16 alphanumerische Zeichen

**Default:** leer

#### 2.39.2.5.3.5 Gueltigkeit

Geben Sie hier die Gültigkeit der Passwörter in Tagen an.

**SNMP-ID:** 2.39.2.5.3.5

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Client-Zertifikate/Gueltigkeitsdauer/Gueltigkeit

**Mögliche Werte:**

- max. 5 Zeichen

**Default:** 365 Tage

### 2.39.2.8 Zertifikatswiderruflisten

Hier finden Sie die Zertifikatswiderruflisten.

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Zertifikatswiderruflisten

#### 2.39.2.8.2 CRL-Verteilungspunkt-Rechnername

Tragen Sie hier das Aktualisierungs-Intervall in Sekunden für die Erstellung einer neuen CRL ein. Die untere Grenze hierfür liegt bei 600 Sekunden.

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Zertifikatswiderruflisten/CRL-Verteilungspunkt-Rechnername

**Mögliche Werte:**

- maximal 63 numerische Zeichen

**Default:** 600

#### 2.39.2.8.3 Erstelle-neue-Zertifikatswiderrufliste

Normalerweise erstellt die CA automatisch eine neue Zertifikatswiderrufliste (CRL) erstellt, wenn die alte CRL abgelaufen ist oder wenn sich der Inhalt der CRL ändert (durch SCEP-Operationen).

Führen Sie diesen Befehl aus, wenn Sie in der Zertifikatsstatusliste ein Zertifikat zurückgerufen haben.

**SNMP-ID:** 2.39.2.8.3

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Zertifikatswiderruflisten/Erstelle-neue-Zertifikatswiderrufliste

#### 2.39.2.8.1 Update-Intervall

Tragen Sie hier das Aktualisierungs-Intervall in Sekunden für die Erstellung einer neuen CRL ein. Die untere Grenze hierfür liegt bei 600 Sekunden. .

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Zertifikatswiderruflisten/Update-Intervall

**Mögliche Werte:**

- maximal 63 numerische Zeichen

**Default:** 86.400

### 2.39.2.10 Benachrichtigung

In diesem Menü finden Sie die Einstellungen zu Benachrichtigungen über Ereignisse im Zusammenhang mit den Zertifikaten.

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Benachrichtigung

#### 2.39.2.10.1 E-Mail

Aktivieren Sie hier, ob eine Benachrichtigung beim Eintreffen eines Ereignisses gesendet wird.

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Benachrichtigung/E-Mail

**Mögliche Werte:**

- nein
- ja

**Default:** nein

#### 2.39.2.10.3 E-Mail-Empfaenger

Geben Sie hier die Emailadresse an, an die eine Benachrichtigung beim Eintreffen eines Ereignisses gesendet wird.

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Benachrichtigung/E-Mail

**Mögliche Werte:**

- maximal 63 alphanumerische Zeichen

**Default:** leer

#### 2.39.2.10.4 Sende-Backup-Erinnerung

Aktivieren Sie hier die Funktion, dass das Gerät automatisch eine Erinnerung zur Erstellung eines Backups an die eingetragene Emailadresse schickt.

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Benachrichtigung/Sende-Backup-Erinnerung

**Mögliche Werte:**

- nein
- ja

**Default:** nein

#### 2.39.2.10.2 Syslog

Aktivieren Sie hier die Protokollfunktion der Benachrichtigungen via SYSLOG.

**Pfad Telnet:** /Setup/Zertifikate/SCEP-CA/Benachrichtigung/Syslog

**Mögliche Werte:**

- nein
- ja

**Default:** nein

Um die Protokollfunktion zu Nutzen, muss der SYSLOG-Client im Gerät entsprechend konfiguriert sein.

## 2.39.3 CRLs

Dieses Menü enthält die Konfiguration der CRLs.

**SNMP-ID:** 2.39.3

**Pfad Telnet:** /Setup/Zertifikate

### 2.39.3.1 Aktiv

Aktiviert: Bei Prüfung eines Zertifikats wird die CRL (falls vorhanden) ebenfalls herangezogen.

**SNMP-ID:** 2.39.3.1

**Pfad Telnet:** /Setup/Zertifikate/CRLs

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

Wenn diese Option aktiviert ist und keine gültige CRL gefunden werden kann, weil z. B. der Server nicht erreichbar ist, werden alle Verbindungen abgelehnt und bestehende Verbindungen unterbrochen.

### 2.39.3.5 Automatische-Auffrisch-Periode

Die Länge des Zeitraums, nach dessen Ablauf periodisch versucht wird, eine neue CRL zu erhalten. Hiermit können eventuell außer der Reihe veröffentlichte CRLs frühzeitig heruntergeladen werden. Mit einem Eintrag von '0' wird das regelmäßige Abruf ausgeschaltet.

**SNMP-ID:** 2.39.3.5

**Pfad Telnet:** /Setup/Zertifikate/CRLs

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

Wenn die CRL bei regelmäßigen Update nicht geladen werden kann, werden keine Versuche bis zum nächsten regelmäßigen Termin gestartet.

### 2.39.3.7 CRL-Jetzt-Abholen

Holt die aktuelle CRL von der im Root-Zertifikat angegebenen URL bzw. von der Alternativ-URL, sofern diese Funktion eingerichtet ist.

**SNMP-ID:** 2.39.3.7

**Pfad Telnet:** /Setup/Zertifikate/CRLs

### 2.39.3.6 Gueltigkeitszeitueberschreitung

Zertifikatsbasierte Verbindungen werden auch nach Ablauf der CRL-Gültigkeit noch innerhalb des hier eingetragenen Zeitraums zugelassen. Mit dieser Toleranz-Zeit kann verhindert werden, dass z. B. bei kurzfristig nicht erreichbarem CRL-Server die Verbindungen abgelehnt oder getrennt werden.

**SNMP-ID:** 2.39.3.6

**Pfad Telnet:** /Setup/Zertifikate/CRLs

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

**Besondere Werte:** Innerhalb des hier eingestellten Zeitraums kann mit Hilfe der in der CRL bereits gesperrten Zertifikate weiterhin eine Verbindung aufrecht erhalten bzw. eine neue Verbindung aufgebaut werden.

In der hier definierten Zeitspanne können auch abgelaufene Zertifikate genutzt werden, um einer Verbindung aufrecht zu erhalten oder neu aufzubauen.

### 2.39.3.4 Holen-Vor-Ablauf

Der Zeitpunkt vor dem Ablauf der CRL, ab dem versucht wird, eine neue CRL zu laden. Dieser Wert wird um einen Zufallskomponente erhöht, um gehäufte Anfragen an den Server zu vermeiden. Be Erreichen dieses Zeitpunkts wird ein evtl. aktiviertes regelmäßiges Update angehalten.

**SNMP-ID:** 2.39.3.4

**Pfad Telnet:** /Setup/Zertifikate/CRLs

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 300

Wenn die CRL im ersten Versuch nicht geladen werden kann, werden in kurzen Zeitabständen neue Versuche gestartet.

### 2.39.3.9 Loopback-Adresse

Definieren Sie hier optional eine Sender-Adresse, die dem Empfänger anstelle der automatisch erzeugten Adresse angezeigt wird.

**SNMP-ID:** 2.39.3.9

**Pfad Telnet:** /Setup/Zertifikate/CRLs/Loopback-Adresse

**Mögliche Werte:**

- Name des IP-Netzwerks, dessen Adresse benutzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse des ersten DMZ
- LB0 - LBF für die 16 Loopback-Adressen
- Jede gültige IP-Adresse

**Default:** leer

Wenn es eine Schnittstelle namens "DMZ" gibt, dann wird deren Adresse genommen, wenn Sie "DMZ" auswählen.

### 2.39.3.8 Alternative-URL-Tabelle

In dieser Tabelle finden Sie die Liste der alternativen URLs.

Die Adresse, von der eine Certificate Revocation List (CRL) abgeholt werden kann, wird normalerweise innerhalb der Zertifikate (als crlDistributionPoint) angegeben. Im LCOS können in einer Tabelle alternative URLs angegeben werden. Nach dem Systemstart werden die entsprechenden CRLs automatisch von diesen URLs abgeholt und zusätzlich zu den in den Zertifikaten angegebenen Listen verwendet.

**SNMP-ID:** 2.39.3.8

**Pfad Telnet:** /Setup/Zertifikate/CRLs/Alternative-URL-Tabelle

#### 2.39.3.8.1 Alternative-URL

Geben Sie hier die alternative URL an, von der eine CRL abgeholt werden kann.

**SNMP-ID:** 2.39.3.8.1

**Pfad Telnet:** /Setup/Zertifikate/CRLs/Alternative-URL-Tabelle/Alternative-URL

**Mögliche Werte:**

- Gültige URL, max. 251 Zeichen.

**Default:** leer

## 2.29.6 OCSP-Client

Dieses Menü enthält die Einstellungen für den OCSP-Client.

**SNMP-ID:** 2.39.6

**Pfad Telnet:** /Setup/Zertifikate

### 2.39.6.1 CA-Profiltabelle

Diese Tabelle enthält die Informationen über die Certificate Authorities (CAs), deren Zertifikate der OCSP-Client mit einer Anfrage an einen OCSP-Responder prüft.

**SNMP-ID:** 2.39.6.1

**Pfad Telnet:** /Setup/Zertifikate/OCSP-Client

### Profilname

Geben Sie hier den Namen eines CA-Profils ein, welches der OCSP-Client für eine bestimmte CA verwendet.

**SNMP-ID:** 2.39.6.1.1

**Pfad Telnet:** /Setup/Zertifikate/OCSP-Client/CA-Profiltabelle

**Mögliche Werte:**

- Maximal 32 alphanumerische Zeichen

**Default:** leer

### CA-DN

Geben Sie hier den Distinguished Name der CA ein, deren Zertifikate der OCSP-Client mit diesem Profil prüft.

**SNMP-ID:** 2.39.6.1.2

**Pfad Telnet:** /Setup/Zertifikate/OCSP-Client/CA-Profiltabelle

**Mögliche Werte:**

- maximal 251 alphanumerische Zeichen

**Default:** leer

### AIA-Bevorzugen

Die Zertifikate für den VPN-Verbindungsaufbau führen optional den URL des zuständigen OCSP-Responders im Feld Auhority Info Access (AIA) mit. Stellen Sie hier ein, ob der OCSP-Client vorrangig den URL aus diesem Eintrag der CA-Profiltabelle verwendet oder den URL aus dem AIA-Feld sofern vorhanden.

**SNMP-ID:** 2.39.6.1.3

**Pfad Telnet:** /Setup/Zertifikate/OCSP-Client/CA-Profiltabelle

**Mögliche Werte:**

- nein: Der OCSP-Client verwendet immer den URL aus diesem Eintrag der CA-Profiltabelle und lässt den URL im AIA-Feld unbeachtet.
- ja: Der OCSP-Client verwendet (sofern angegeben) den URL aus dem AIA-Feld und lässt den URL aus diesem Eintrag der CA-Profiltabelle unbeachtet.

**Default:** nein

### Responder-Profilname

Wählen Sie hier das Responder-Profil aus, mit dem der OCSP-Client die Zertifikate dieser CA prüft.

**SNMP-ID:** 2.39.6.1.4

**Pfad Telnet:** /Setup/Zertifikate/OCSP-Client/CA-Profiltabelle

**Mögliche Werte:**

- Auswahl aus der Liste der Profilnamen in der Tabelle *2.39.6.2 Responder-Profiltabelle*, maximal 32 alphanumerische Zeichen.

**Default:** leer

Wenn das Feld für den Responder-Profilnamen frei bleibt, prüft das Gerät die verwendeten Zertifikate für die in diesem Eintrag definierte CA nicht mit OCSP, sondern mit Hilfe einer CRL.

**Quellinterface**

Hier können Sie optional eine Absenderadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absenderadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absenderadresse angeben.

**SNMP-ID:** 2.39.6.1.5

**Pfad Telnet:** /Setup/Zertifikate/OCSP-Client/CA-Profiltabelle

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige, gültige IP-Adresse

**Default:** 0.0.0.0

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, wird die zugehörige IP-Adresse verwendet. Name einer Loopback- Adresse.

**Cert-Pruefung**

Stellen Sie hier ein, wie sich das Gerät bei einer nicht erfolgreichen Prüfung des Zertifikats verhält. Der OCSP-Client fragt zunächst beim Verbindungsaufbau die Gültigkeit des verwendeten Zertifikats beim OCSP-Responder an.Wenn das Zertifikat in Kürze abläuft, fragt der OCSP-Client rechtzeitig vor dem Ablaufdatum automatisch die Gültigkeit erneut ab.

**SNMP-ID:** 2.39.6.1.6

**Pfad Telnet:** /Setup/Zertifikate/OCSP-Client/CA-Profiltabelle

**Mögliche Werte:**

- Streng: Wenn der OCSP-Responder die Anfrage für das verwendete Zertifikat beim Verbindungsaufbau als nicht gültig meldet, baut das Gerät keine Verbindung zur Gegenstelle auf. Wenn der OCSP-Responder während einer bestehenden Verbindung auf eine erneute Anfrage vor dem Ende des Ablaufdatums die Gültigkeit des verwendeten Zertifikats nicht rechtzeitig bestätigt, baut das Gerät die Verbindung ab.
- Lose: Wenn der OCSP-Responder die Anfrage für das verwendete Zertifikat beim Verbindungsaufbau als nicht gültig meldet, baut das Gerät trotzdem eine Verbindung zur Gegenstelle auf. Wenn der OCSP-Responder während einer bestehenden Verbindung auf eine erneute Anfrage vor dem Ende des Ablaufdatums die Gültigkeit des verwendeten Zertifikats nicht rechtzeitig bestätigt, baut das Gerät die Verbindung dennoch nicht ab.

**Default:** Streng

Überprüfen und protokollieren Sie die Ergebnisse der Zertifikatsprüfung beim OCSP-Responder bei Bedarf mit SYSLOG, SNMP-Traps und entsprechenden Traces.

**Syslog-Events**

Der OCSP-Client kann optional SYSLOG-Nachrichten mit Informationen über die Ergebnisse der Zertifikatsprüfungen beim OCSP-Responder erzeugen.

**SNMP-ID:** 2.39.6.1.7

**Pfad Telnet:** /Setup/Zertifikate/OCSP-Client/CA-Profiltabelle

**Mögliche Werte:**

- ja: Der OCSP-Client erzeugt SYSLOG-Nachrichten.
- nein: Der OCSP-Client erzeugt keine SYSLOG-Nachrichten.

**Default:** ja

### Responder-Profiltabelle

Diese Tabelle enthält die Informationen über die Certificate Authorities (CAs), deren Zertifikate der OCSP-Client mit einer Anfrage an einen OCSP-Responder prüft.

**SNMP-ID:** 2.39.6.2

**Pfad Telnet:** /Setup/Zertifikate/OCSP-Client

#### Profilname

Geben Sie hier den Namen eines OCSP-Responder-Profils ein, das der OCSP-Client in der CA-Profiltabelle referenziert.

**SNMP-ID:** 2.39.6.2.1

**Pfad Telnet:** /Setup/Zertifikate/OCSP-Client/CA-Profiltabelle

**Mögliche Werte:**

- Maximal 32 alphanumerische Zeichen

**Default:** leer

#### URL

Geben Sie hier den URL an, über welchen der OCSP-Client den OCSP-Responder erreicht.

**SNMP-ID:** 2.39.6.2.2

**Pfad Telnet:** /Setup/Zertifikate/OCSP-Client/CA-Profiltabelle

**Mögliche Werte:**

- Gültige URL mit maximal 251 alphanumerische Zeichen

**Default:** leer

## 2.40 GPS

Hier finden Sie die Einstellungen für GPS.

**SNMP-ID:** 2.40

**Pfad Telnet:** /Setup/GPS

## 2.40.1 Aktiv

Aktivieren oder Deaktivieren Sie hier die GPS-Funktion. Sie können das GPS-Modul unabhängig von der gewählten Verifikations-Methode der Standort-Verifikation einschalten, um die aktuellen Standortkoordinaten beispielsweise mit LANmonitor zu überwachen.

**SNMP-ID:** 2.40.1

**Pfad Telnet:** /Setup/GPS/Aktiv

**Mögliche Werte:**

- nein

- ja

**Default:** nein

# 2.41 UTM

Hier finden Sie die Einstellung zu UTM.

**SNMP-ID:** 2.41

**Pfad Telnet:** /Setup/

## 2.41.2 Content-Filter

Hier finden Sie die Einstellungen für den Content-Filter.

**SNMP-ID:** 2.41.2

**Pfad Telnet:** /Setup/UTM/

### 2.41.2.1 Aktiv

Hier können Sie den Content Filter aktivieren.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Aktiv

**Mögliche Werte:**

- Ja: Aktiviert den Content Filter.
- Nein: Deaktiviert den Content Filter.

**Default:**

- Nein

### 2.41.2.2 Globale Einstellungen

NEW

Hier finden Sie die globalen Einstellungen für den Content-Filter.

**SNMP-ID:** 2.41.2.2

**Pfad Telnet:** /Setup/UTM/Content-Filter/

#### 2.41.2.2.1 Admin-Email

Um die E-Mail Benachrichtigungsfunktion zu nutzen, muss ein SMTP-Client entsprechend konfiguriert sein. Sie können den Client in diesem Gerät dazu verwenden oder einen anderen Ihrer Wahl.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen

Wenn kein E-Mail Empfänger angegeben wird, dann wird keine E-Mail verschickt.

#### 2.41.2.2.5 Aktion bei Fehler

Hier können Sie bestimmen, was bei einem Fehler passieren soll. Kann der Bewertungsserver beispielsweise nicht kontaktiert werden, kann der Benutzer in Folge dieser Einstellung entweder ungehindert surfen oder aber es wird der komplette Webzugriff verboten.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen

**Mögliche Werte:**

- Blockieren, Durchlassen

**Default:** Blockieren

#### 2.41.2.2.7 Aktion bei Lizenzablauf

Die Lizenz zur Nutzung des LANCOM Content Filters gilt für einen bestimmten Zeitraum. Sie werden 30 Tage, eine Woche und einen Tag vor Ablauf der Lizenz an die auslaufende Lizenz erinnert (an die E-Mailadresse, die konfiguriert ist unter LANconfig: Meldungen > Allgemein).

Hier können Sie bestimmen, was bei Ablauf der Lizenz passieren soll (blockieren oder ungeprüft durchlassen). Der Benutzer kann in Folge dieser Einstellung bei Ablauf der für ihn verwendeten Lizenz entweder ungehindert surfen oder aber es wird der komplette Webzugriff verboten.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen

**Mögliche Werte:**

- Blockieren, Durchlassen

**Default:** Blockieren

#### 2.41.2.2.6 Aktion bei Lizenzüberschreitung

Hier können Sie bestimmen, was bei Überschreitung der lizensierten Benutzeranzahl passieren soll. Die Benutzer werden über die IP-Adresse identifiziert. Das heißt, dass die IP-Adressen, die eine Verbindung durch den LANCOM Content Filter aufbauen, gezählt werden. Baut z. B. bei einer 10er Option ein elfter Benutzer eine Verbindung auf, findet keine Prüfung mehr durch den LANCOM Content Filter statt. Der Benutzer, für den keine Lizenz mehr zur Verfügung steht, kann in Folge dieser Einstellung entweder ungehindert surfen oder aber es wird der komplette Webzugriff verboten.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen

**Mögliche Werte:**

- Blockieren, Durchlassen

**Default:** Blockieren

Die Benutzer des Content-Filters werden automatisch aus der Benutzerliste entfernt, wenn von dieser IP-Adresse seit 24 Stunden keine Verbindung durch den Content-Filter mehr aufgebaut wurde.

#### 2.41.2.2.17 Im-Flashrom-speichern

Schalten Sie diese Option ein, damit die Kategoriestatistik im Flash-ROM abgelegt wird.

Dadurch gehen die Daten auch durch Ausschalten des Gerätes oder bei einem Stromausfall nicht verloren.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen/Im-Flashrom-speichern

**Mögliche Werte:**

- Ja: Aktiviert das Speichern im Flash-ROM.
- Nein: Deaktiviert das Speichern im Flash-ROM.

**Default:** Nein

#### 2.41.2.2.22 Loopback bei Override

Dieser Parameter wird ab LCOS 8.50 nicht mehr verwendet.

Hier können Sie optional eine Absende-Adresse für die Override-URL konfigurieren, die statt der ansonsten automatisch für die Ziel-Adresse gewählten Absende-Adresse verwendet wird. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absende-Adresse angeben.

**SNMP-ID:** 2.41.2.2.22

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen

**Englische Bezeichnung:** Loopback-To-Use-On-Override

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ (Achtung: wenn es eine Schnittstelle Namens "DMZ" gibt, dann wird deren Adresse genommen)
- LB0 ... LBF für die 16 Loopback-Adressen
- GUEST
- Beliebige IP-Adresse in der Form x.x.x.x

**Default:** leer

Die hier eingestellte Absende-Adresse wird für jede Gegenstelle unmaskiert verwendet.

#### 2.41.2.2.12 Loopback-wenn-blockiert

Hier können Sie optional eine Absende-Adresse für die Blockiert-URL konfigurieren, die statt der ansonsten automatisch für die Ziel-Adresse gewählten Absende-Adresse verwendet wird. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absende-Adresse angeben.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ (Achtung: wenn es eine Schnittstelle Namens "DMZ" gibt, dann wird deren Adresse genommen)
- LB0 ... LBF für die 16 Loopback-Adressen
- GUEST
- Beliebige IP-Adresse in der Form x.x.x.x

**Default:** leer

Die hier eingestellte Absende-Adresse wird für jede Gegenstelle unmaskiert verwendet.

#### 2.41.2.2.13 Override-aktiv

Hier können Sie die Override-Funktion aktivieren und weitere Einstellungen für diese Funktion vornehmen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen

**Mögliche Werte:**

- ja, nein

**Default:** nein

#### 2.41.2.2.14 Overridedauer

Der Override kann hier zeitlich begrenzt werden. Nach Ablauf der Zeitspanne wird jedes Betreten der gleichen Domain und/oder Kategorie wieder verboten. Mit einem erneuten Klick auf den Override-Button kann die Seite wieder für die Override-Dauer betreten werden, der Administrator erhält je nach Einstellung eine erneute Benachrichtigung.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen/

**Mögliche Werte:**

- 1-1440 (Minuten)
- max. 4 Zeichen

**Default:** 5 Minuten

#### 2.41.2.2.15 Overridetyp

Hier können Sie den Override-Typ einstellen, für den der Override gelten soll. Er kann für die Domain oder die Kategorie der zu blockierenden Seite oder für beides erlaubt werden.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen

**Mögliche Werte:**

- Kategorie: Während der Override-Dauer sind alle URLs erlaubt, die unter die angezeigten Kategorien fallen (zuzüglich derer, die auch ohne den Override schon erlaubt gewesen wären).
- Domain: Während der Override-Dauer sind alle URLs unter der besuchten Domain erlaubt, egal zu welchen Kategorien sie gehören.
- Kategorie und Domain: Während der Override-Dauer sind alle URLs erlaubt, die sowohl zu dieser Domain als auch zu den freigeschalteten Kategorien gehören. Dies ist die stärkste Einschränkung.

**Default:** Kategorie und Domain

#### 2.41.2.2.24 Proxyverbindungs-Limit

Stellen Sie hier die Anzahl der Proxy-Verbindungen ein, die maximal gleichzeitig aufgebaut werden dürfen. Die Last kann somit auf dem System eingeschränkt werden. Es wird eine Benachrichtigung ausgelöst, wenn diese Anzahl überschritten wird.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen/Proxyverbindungs-Limit

**Mögliche Werte:**

- 0 bis 999999 Verbindungen

**Default:** geräteabhängig

#### 2.41.2.2.21 URL bei Override

Dieser Parameter wird ab LCOS 8.50 nicht mehr verwendet.

Hier können Sie eine alternative URL-Adresse eintragen. Im Falle des Override wird dann statt der Standard-Webseite die hier eingetragene URL aufgerufen. In der externen HTML-Seite können Sie z. B. das Corporate Design Ihres Unternehmens abbilden oder weitere Funktionen wie JavaScript etc. nutzen. Außerdem können hier auch die gleichen Tags wie im Override-Text verwendet werden. Wenn Sie an dieser Stelle keinen Eintrag vornehmen, wird die im Gerät hinterlegte Standard-Webseite aufgerufen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen

**Mögliche Werte:**

- gültige URL-Adresse

**Default:** leer

#### 2.41.2.2.11 URL wenn blockiert

Hier können Sie eine alternative URL-Adresse eintragen. Im Falle des Blockierens wird dann statt der Standard-Webseite die hier eingetragene URL aufgerufen. In der externen HTML-Seite können Sie z. B. das Corporate Design Ihres Unternehmens abbilden oder weitere Funktionen wie JavaScript etc. nutzen. Außerdem können hier auch die gleichen HTML-Tags wie im Blocktext verwendet werden. Wenn Sie an dieser Stelle keinen Eintrag vornehmen, wird die im Gerät hinterlegte Standard-Webseite aufgerufen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen

**Mögliche Werte:**

- gültige URL-Adresse

**Default:** leer

#### 2.41.2.2.25 Verarbeitungs-Timeout-in-ms

Stellen Sie hier die Zeit in Millisekunden ein, die der Proxy maximal für die Bearbeitung benötigen darf. Wird diese Zeit überschritten, wird dies durch eine entsprechende Zeitüberschreitungs-Fehlerseite quittiert.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen/Verarbeitungs-Timeout-in-ms

**Mögliche Werte:**

- 0 bis 999999 Millisekunden

**Default:**

- 3000 Millisekunden

**Besondere Werte:**

- Der Wert 0 steht für keine Zeitbegrenzung. Werte kleiner als 100 Millisekunden sind nicht sinnvoll.

#### 2.41.2.2.9 Benachrichtigung

Hier definieren Sie, in welcher Form Sie über bestimmte Ereignisse informiert werden. Die Benachrichtigung kann erfolgen durch E-Mail, SNMP oder SYSLOG. Für verschiedene Ereignisse kann separat definiert werden, über welchen Weg Meldungen ausgegeben werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen/

**Fehler:**

- Bei SYSLOG: Quelle “System”, Priorität “Alarm”.
- Default: Benachrichtigung SYSLOG

**Lizenzüberschreitung:**

- Bei SYSLOG: Quelle “Verwaltung”, Priorität “Alarm”.
- Default: Benachrichtigung E-MAIL, SNMP und SYSLOG

**Lizenzablauf:**

- Bei SYSLOG: Quelle “Verwaltung”, Priorität “Alarm”.
- Default: Benachrichtigung E-MAIL, SNMP und SYSLOG

**Override:**

- Bei SYSLOG: Quelle “Router”, Priorität “Alarm”.
- Default: Keine Benachrichtigung

**Proxy-Limit:**

- Bei SYSLOG: Quelle "Router", Priorität "Info"
- Default: Benachrichtigung SYSLOG

#### 2.41.2.2.9.1 Grund

Wählen Sie hier einen der vordefinierten Werte für den Grund der Benachrichtigung aus.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen/Benachrichtigung

#### 2.41.2.2.9.2 Email

Hier können Sie einstellen, ob Sie eine Benachrichtigung per Email bekommen möchten.

**SNMP-ID:** 2.41.2.2.9.2

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen/Benachrichtigung

**Mögliche Werte:**

- ja
- nein

**Default:** je nach Grund unterschiedlich vorbelegt.

#### 2.41.2.2.9.3 SNMP

Hier können Sie einstellen, ob Sie eine Benachrichtigung per SNMP bekommen möchten.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen/Benachrichtigung

**Mögliche Werte:**

- ja, nein

**Default:** je nach Grund unterschiedlich vorbelegt.

#### 2.41.2.2.9.4 Syslog

Hier können Sie einstellen, ob Sie eine Benachrichtigung per SYSLOG bekommen möchten.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen/Benachrichtigung

**Mögliche Werte:**

- ja
- nein

**Default:** je nach Grund unterschiedlich vorbelegt.

### 2.41.2.2.10 Blocktext

Hier können Sie einen Text definieren, der bei Blockierung angezeigt wird. Für unterschiedliche Sprachen kann jeweils ein eigener Blocktext definiert wird. Die Auswahl des verwendeten Blocktextes wird anhand des übermittelten Spracheinstellung des Browsers (User Agents) vorgenommen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen

#### 2.41.2.2.10.1 Sprache

Damit der Anwender alle Meldungen in seiner voreingestellten Browser-Sprache erhält, kann hier der entsprechende Country-Code eingetragen werden. Wird der im Browser eingestellten Country-Code hier gefunden, kommt der dazu passende Text zur Anzeige.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen/Blocktext

Weitere Sprachen können nach Belieben hinzugefügt werden.

Der Country-Code sieht dafür z. B. folgendermaßen aus:

- de-DE: Deutschsprachig-Deutschland
- de-CH: Deutschsprachig-Schweiz
- de-AT: Deutschsprachig-Österreich
- en-GB: Englischsprachig-Großbritannien
- en-US: Englischsprachig-Vereinigte Staaten

Der Contentfilter verarbeitet nur den ersten Teil des Country-Codes bis zum '-', d.h. "en", "en-GB" und "en-US" sind für den Contentfilter identisch. Der Contentfilter unterscheidet nicht zwischen Groß- und Kleinschreibung. Wird der im Browser eingestellte Country-Code in dieser Tabelle nicht gefunden oder der dafür hinterlegte Text gelöscht, so wird der bereits vordefinierten Standardtext (Default) verwendet. Den Default-Text können Sie bearbeiten.

**Mögliche Werte:**

10 alphanumerische Zeichen

**Default:**

leer

#### 2.41.2.2.10.2 Text

Geben Sie hier den Text ein, der als Blocktext für diese Sprache verwendet werden soll.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen/Blocktext

**Mögliche Werte:**

- 254 alphanumerische Zeichen

**Default:**

leer

**Besondere Werte:**

Sie können für den Blocktext auch spezielle Tags verwenden, wenn Sie unterschiedliche Seiten anzeigen wollen, je nachdem aus welchem Grund (z. B. verbotene Kategorie oder Eintrag in der Blacklist) die Seite verboten wurde.

Für die einzusetzenden Werte können Sie folgende Tags verwenden:

- <CF-URL/> für den verbotenen URL
- <CF-HOST/> oder <CF-DOMAIN/> zeigen den Hostteil bzw. die Domain des freigeschalteten URL an. Die Tags sind gleichwertig und können wahlweise verwendet werden.
- <CF-CATEGORIES/> für die Liste der Kategorien aufgrund der die Webseite verboten wurde
- <CF-PROFILE/> für den Profilnamen
- <CF-DURATION/> zeigt die Override-Dauer in Minuten.
- <CF-OVERRIDEURL/> für den URL zum Freischalten des Overrides (dieser kann in ein einfaches <a>-Tag oder einen Button eingebaut werden)
- <CF-LINK/> fügt einen Link zum Freischalten des Overrides ein
- <CF-BUTTON/> für einen Button zum Freischalten des Overrides

Zum Ein- und Ausblenden von Teilen des HTML-Dokuments wird ein Tag mit Attributen verwendet: <CF-IF att1 att2> ... </CF-IF>.

**Attribute sind:**

- BLACKLIST: wenn die Seite verboten wurde, weil sie auf der Blacklist des Profils steht
- FORBIDDEN: wenn die Seite aufgrund einer ihrer Kategorien verboten wurde

- CATEGORY: wenn der Override-Typ "Kategorie" ist und der Override erfolgreich war
- ERR: wenn ein Fehler aufgetreten ist.

Da es getrennte Texttabellen für die Blockseite und die Fehlerseite gibt, ist das Tag nur sinnvoll, wenn Sie einen alternativen Block-URL konfiguriert haben.

- OVERRIDEOK: wenn dem Benutzer ein Override erlaubt wurde (in diesem Fall sollte die Seite eine entsprechende Schaltfläche anzeigen)

Werden in einem Tag mehrere Attribute angegeben, dann wird der Bereich eingeblendet, wenn mind. eine dieser Bedingungen erfüllt ist. Alle Tags und Attribute lassen sich mit den jeweils ersten zwei Buchstaben abkürzen (z. B. CF-CA oder CF-IF BL). Das ist notwendig, weil der Blocktext nur maximal 254 Zeichen lang sein darf.

Beispiel:

- <CF-URL/> wird wegen der Kategorien <CF-CA/> verboten.<br>Ihr Contentfilterprofil ist <CF-PR/>.<br><CF-IF OVERRIDEOK><br><CF-BU/></CF-IF>

Die hier beschriebenen Tags können auch in externen HTML-Seiten (alternativer Block-URL) verwendet werden.

#### 2.41.2.2.19 Fehlertext

Hier können Sie einen Text definieren, der bei einem Fehler zur Anzeige kommt.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen

#### 2.41.2.2.19.1 Sprache

Damit der Anwender alle Meldungen in seiner voreingestellten Browser-Sprache erhält, kann hier der entsprechende Country-Code eingetragen werden. Wird der im Browser eingestellten Country-Code hier gefunden, kommt der dazu passende Text zur Anzeige.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen/Fehlertext

Weitere Sprachen können nach Belieben hinzugefügt werden.

Der Country-Code sieht dafür z. B. folgendermaßen aus:

- de-DE: Deutschsprachig-Deutschland
- de-CH: Deutschsprachig-Schweiz
- de-AT: Deutschsprachig-Österreich
- en-GB: Englischsprachig-Großbritannien
- en-US: Englischsprachig-Vereinigte Staaten

Der Contentfilter verarbeitet nur den ersten Teil des Country-Codes bis zum '-', d.h. "en", "en-GB" und "en-US" sind für den Contentfilter identisch. Der Contentfilter unterscheidet nicht zwischen Groß- und Kleinschreibung. Wird der im Browser eingestellte Country-Code in dieser Tabelle nicht gefunden oder der dafür hinterlegte Text gelöscht, so wird der bereits vordefinierten Standardtext (Default) verwendet. Den Default-Text können Sie bearbeiten.

**Mögliche Werte:**

10 alphanumerische Zeichen

**Default:**

leer

#### 2.41.2.2.19.2 Text

Geben Sie hier den Text ein, der als Fehlertext für diese Sprache verwendet werden soll.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen/Fehlertext

**Mögliche Werte:**

254 alphanumerische Zeichen

**Default:**

leer

**Besondere Werte:**

Sie können für den Fehlertext auch HTML-Tags verwenden.

Für die einzusetzenden Werte können Sie folgende Empty-Element-Tags verwenden:

- <CF-URL/> für den verbotenen URL
- <CF-HOST/> oder <CF-DOMAIN/> zeigen den Hostteil bzw. die Domain des blockierten URL an. Die Tags sind gleichwertig und können wahlweise verwendet werden.
- <CF-DURATION/> zeigt die Override-Dauer in Minuten.
- <CF-PROFILE/> für den Profilnamen
- <CF-ERROR/> für die Fehlermeldung

Zum Ein- und Ausblenden von Teilen des HTML-Dokuments wird ein Tag mit Attributen verwendet: <CF-IF att1 att2> ... </CF-IF>.

**Attribute sind:**

- CHECKERROR: der Fehler ist beim Prüfen des URL aufgetreten
- OVERRIDEERROR: der Fehler ist beim Freischalten eines Override aufgetreten

**Beispiel:**

<CF-URL/> wird verboten, weil ein Fehler aufgetreten ist:<br><CF-ERROR/>

<CF-URL>: blockierter URL <CF-HOST> oder <CF-DOMAIN>: Hostteil des blockierten URL <CF-PROFILE>: Contentfilterprofil des Benutzers <CF-DURATION>: Overridedauer in Minuten <CF-ERROR>: Fehlermeldung <CF-IF> bis </CF-IF>: bedingte Auswertung mit logischem ODER der folgenden Parameter: CHECKERROR: der Fehler ist beim Prüfen des URL aufgetreten (wie früher) OVERRIDEERROR: der Fehler ist beim Freischalten eines Overrides aufgetreten

#### 2.41.2.2.20 Overridetext

Hier können Sie einen Text definieren, der als Bestätigung für den Benutzer bei einem Override angezeigt wird.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen

#### 2.41.2.2.20.1 Sprache

Damit der Anwender alle Meldungen in seiner voreingestellten Browser-Sprache erhält, kann hier der entsprechende Country-Code eingetragen werden. Wird der im Browser eingestellten Country-Code hier gefunden, kommt der dazu passende Text zur Anzeige.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen/Overridetext

Weitere Sprachen können nach Belieben hinzugefügt werden.

Der Country-Code sieht dafür z. B. folgendermaßen aus:

- de-DE: Deutschsprachig-Deutschland
- de-CH: Deutschsprachig-Schweiz
- de-AT: Deutschsprachig-Österreich
- en-GB: Englischsprachig-Großbritannien
- en-US: Englischsprachig-Vereinigte Staaten

Der Contentfilter verarbeitet nur den ersten Teil des Country-Codes bis zum '-', d.h. "en", "en-GB" und "en-US" sind für den Contentfilter identisch. Der Contentfilter unterscheidet nicht zwischen Groß- und Kleinschreibung. Wird der im Browser eingestellte Country-Code in dieser Tabelle nicht gefunden oder der dafür hinterlegte Text gelöscht, so wird der bereits vordefinierten Standardtext (Default) verwendet. Den Default-Text können Sie bearbeiten.

**Mögliche Werte:**

10 alphanumerische Zeichen

**Default:**

leer

#### 2.41.2.2.20.2 Text

Geben Sie hier den Text ein, der als Overridetext für diese Sprache verwendet werden soll.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen/Overridetext

**Mögliche Werte:**

- 254 alphanumerische Zeichen

**Default:**

leer

**Besondere Werte:**

Sie können für den Blocktext auch HTML-Tags verwenden, wenn Sie unterschiedliche Seiten anzeigen wollen, je nachdem aus welchem Grund (z. B. verbotene Kategorie oder Eintrag in der Blacklist) die Seite verboten wurde.

Für die einzusetzenden Werte können Sie folgende Tags verwenden:

- <CF-URL/> für den ursprünglich verbotenen URL, der jetzt aber freigeschaltet ist
- <CF-CATEGORIES/> für die Liste der Kategorien, die durch diesen Override freigeschaltet sind (außer bei Domain-Override).
- <CF-BUTTON/> zeigt einen Override-Button, der auf den ursprünglich aufgerufenen URL weiterleitet.
- <CF-LINK/> zeigt einen Override-Link an, der auf den ursprünglich aufgerufenen URL weiterleitet.
- <CF-HOST/> oder <CF-DOMAIN/> zeigen den Hostteil bzw. die Domain des freigeschalteten URL an. Die Tags sind gleichwertig und können wahlweise verwendet werden.
- <CF-ERROR/> erzeugt eine Fehlermeldung, falls der Override fehlschlägt.
- <CF-DURATION/> zeigt die Override-Dauer in Minuten.

Zum Ein- und Ausblenden von Teilen des HTML-Dokuments wird ein Tag mit Attributen verwendet: <CF-IF att1 att2> ... </CF-IF>.

**Attribute können sein:**

- BLACKLIST: wenn die Seite verboten wurde, weil sie auf der Blacklist des Profils steht
- FORBIDDEN: wenn die Seite aufgrund einer ihrer Kategorien verboten wurde
- CATEGORY: wenn der Override-Typ "Kategorie" ist und der Override erfolgreich war
- DOMAIN: wenn der Override-Typ "Domain" ist und der Override erfolgreich war
- BOTH: wenn der Override-Typ "Kategorie und Domain" ist und der Override erfolgreich war
- ERROR: falls der Override fehlgeschlagen ist
- OK: falls entweder CATEGORY oder DOMAIN oder BOTH zutreffend sind

Werden in einem Tag mehrere Attribute angegeben, dann sollte der Bereich eingeblendet werden, wenn mind. eine dieser Bedingungen erfüllt ist. Alle Tags und Attribute lassen sich mit den jeweils ersten zwei Buchstaben abkürzen (z. B. CF-CA oder CF-IF BL). Das ist notwendig, weil der Text nur maximal 254 Zeichen lang sein darf.

**Beispiel:**

<CF-IF CA BO>Die Kategorien <CF-CAT/> sind</CF-IF><CF-IF BO> in der Domain <CF-DO/></CF-IF><CF-IF DO>Die Domain <CF-DO/> ist</CF-IF><CF-IF OK> für <CF-DU/> Minuten freigeschaltet.<br><CF-LI/></CF-IF><CF-IF ERR>Override-Fehler:<br><CF-ERR/></CF-IF>

#### 2.41.2.2.23 Schnappschuss

Hier können Sie den Content-Filter-Schnappschuss aktivieren und bestimmen wann und wie häufig er stattfindet. Der Schnappschuss kopiert die Tabelle der Kategoriestatistik in die Letzter-Schnappschuss-Tabelle, dabei wird der alte Inhalt der Schnappschuss-Tabelle überschrieben. Die Werte der Kategoriestatistik werden dann auf 0 gesetzt.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen

#### 2.41.2.2.23.1 Aktiv

Hier können Sie den Content-Filter-Schnappschuss aktivieren und bestimmen wann und wie häufig er stattfindet. Der Schnappschuss kopiert die Tabelle der Kategoriestatistik in die Letzter-Schnappschuss-Tabelle, dabei wird der alte Inhalt der Schnappschuss-Tabelle überschrieben. Die Werte der Kategoriestatistik werden dann auf 0 gesetzt.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen/Schnappschuss/Aktiv

**Mögliche Werte:**

- Ja: Aktiviert den Schnappschuss.
- Nein: Deaktiviert den Schnappschuss.

**Default:**

- Ja

#### 2.41.2.2.23.4 Tag

Ist eine monatliche Ausführung des SnapShot gewünscht, wählen Sie hier den Tag an dem der SnapShot angefertigt werden soll.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen/Schnappschuss

**Mögliche Werte:**

max. 2 Zeichen

**Default:**

1

Wählen Sie als Monatstag sinnvollerweise eine Zahl zwischen 1 und 28, damit der Tag in jedem Monat vorkommt.

#### 2.41.2.2.23.2 Typ

Wählen Sie hier, ob der SnapShot monatlich, wöchentlich oder täglich angefertigt werden soll.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen/Schnappschuss

**Mögliche Werte**

Monatlich, Wöchentlich, Täglich

**Default:**

Monatlich

#### 2.41.2.2.23.5 Wochentag

Ist eine wöchentliche Ausführung des SnapShot gewünscht, selektieren Sie hier den Wochentag, an dem der SnapShot angefertigt werden soll.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen/Schnappschuss

**Mögliche Werte:**

Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag

**Default:** Sonntag

#### 2.41.2.2.23.3 Zeit

Ist eine tägliche Ausführung des SnapShot gewünscht, tragen Sie hier die Tageszeit in Stunden und Minuten ein.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen/Schnappschuss

**Mögliche Werte:**

- max. 5 Zeichen
- Format HH:MM

**Default:**

00:00

#### 2.41.2.2.21 URL bei Fehler

Hier können Sie einen alternativen URL eintragen. Im Falle eines Fehlers wird dann statt der Standard-Webseite der hier eingetragene URL aufgerufen. In der externen HTML-Seite können Sie z. B. das Corporate Design Ihres Unternehmens abbilden oder weitere Funktionen wie JavaScript etc. nutzen. Außerdem können hier auch die gleichen Tags wie im Override-Text verwendet werden. Wenn Sie an dieser Stelle keinen Eintrag vornehmen, wird die im Gerät hinterlegte Standard-Webseite aufgerufen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen

**Mögliche Werte:**

- gültige URL-Adresse

**Default:** leer

#### 2.41.2.2.22 Loopback bei Fehler

Hier können Sie optional eine Absenderadresse für den Fehler-URL konfigurieren, der statt der ansonsten automatisch für die Ziel-Adresse gewählten Absenderadresse verwendet wird. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absenderadresse angeben.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Globale-Einstellungen

**Englische Bezeichnung:** Loopback-To-Use-On-Override

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ (Achtung: wenn es eine Schnittstelle Namens "DMZ" gibt, dann wird deren Adresse genommen)
- LB0 ... LBF für die 16 Loopback-Adressen
- GUEST
- Beliebige IP-Adresse in der Form x.x.x.x

**Default:** leer

Die hier eingestellte Absenderadresse wird für jede Gegenstelle unmaskiert verwendet.

## 2.41.2.3 Profile

Hier finden Sie die Profil-Einstellungen für den Content-Filter.

### 2.41.2.3.1 Profile

Hier können Sie Content-Filter-Profile erstellen, die zur Überprüfung von Webseiten auf nicht zugelassene Inhalte genutzt werden. Ein Content-Filter-Profil hat immer einen Namen und ordnet verschiedenen Zeitabschnitten das jeweils gewünschte Kategorieprofil sowie optional eine Black- und eine Whitelist zu.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile

Um verschiedene Zeiträume unterschiedlich zu definieren, werden mehrere Content-Filter-Profileinträge mit dem gleichen Namen angelegt. Das Content-Filter-Profil besteht dann aus der Summe aller Einträge mit dem gleichen Namen.

Das Content-Filter-Profil wird über die Firewall angesprochen.

Bitte beachten Sie, dass Sie zur Nutzung der Profile im LANCOM Content Filters entsprechende Einstellungen in der Firewall vornehmen müssen.

#### 2.41.2.3.1.1 Name

Geben Sie hier den Namen des Content-Filter-Profils an, über das es in der Firewall referenziert wird.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile

**Mögliche Werte:**

- Name eines Profils
- maximal 31 Zeichen

**Default:**

leer

#### 2.41.2.3.1.2 Zeitschema

Wählen Sie den Zeitrahmen für das Content-Filter-Profil. Voreingestellt sind die Zeitrahmen “Always” und “Never”. Weitere Zeitrahmen können Sie konfigurieren unter: /Setup/Zeit/Zeitrahmen.

Zu einem Content-Filter-Profil kann es auch mehrere Zeilen mit unterschiedlichen Zeitrahmen geben.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile

**Mögliche Werte:**

- Always
- Never
- Name eines Zeitrahmenprofils
- maximal 31 Zeichen

**Default:** leer

Wenn sich bei der Verwendung von mehreren Einträgen für ein Content-Filter-Profil die Zeitrahmen überlappen, werden in diesem Zeitraum alle Seiten gesperrt, die durch einen der aktiven Einträge gesperrt werden. Bleibt bei der Verwendung von mehreren Einträgen für ein Content-Filter-Profil ein Zeitraum undefiniert, ist in diesem Zeitraum der ungeprüfte Zugriff auf alle Webseiten möglich.

#### 2.41.2.3.1.3 Whitelist

Wählen Sie hier die Whitelist, die für dieses Content-Filter-Profil gelten soll. Geben Sie einen neuen Namen ein oder wählen Sie einen vorhandenen Eintrag aus der Whitelist-Tabelle aus.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile

**Mögliche Werte:**

- Name einer vorhandenen Whitelist
- maximal 31 Zeichen

**Default:** leer

#### 2.41.2.3.1.4 Blacklist

Wählen Sie hier die Blacklist, die für dieses Content-Filter-Profil gelten soll. Geben Sie einen neuen Namen ein oder wählen Sie einen vorhandenen Eintrag aus der Blacklist-Tabelle aus.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile

**Mögliche Werte:**

- Name einer vorhandenen Blacklist
- maximal 31 Zeichen

**Default:** leer

#### 2.41.2.3.1.5 Kategorieprofil

Wählen Sie hier das Kategorie-Profil, welches für dieses Content-Filter-Profil gelten soll. Geben Sie einen neuen Namen ein oder wählen Sie einen vorhandenen Eintrag aus der Tabelle der Kategorie-Profile aus.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile

**Mögliche Werte:**

- Name eines Kategorie-Profils
- maximal 31 Zeichen

**Default:** leer

### 2.41.2.3.2 Whitelists

Hier können Sie Webseiten konfigurieren, die gezielt erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile

Die Einträge für die erlaubten Webseiten können maximal 252 Zeichen umfassen. Um längere Whitelist-Einträge zu definieren, können mehrere Einträge einen speziellen, gemeinsamen Namen verwenden. Geben Sie dazu den Namen der Whitelist ein gefolgt von einem #-Zeichen und einem beliebigen Suffix. Zum Beispiel legen Sie drei Whitelist-Einträge mit den Namen "MyWhitelist#1", "MyWhitelist#2" und "MyWhitelist#3" an. Im Content-Filter-Profil referenzieren Sie diese erweiterte Whitelist dann mit dem Namen "MyWhitelist".

#### 2.41.2.3.2.1 Name

Hier muss der Name der Whitelist angegeben werden, über den sie im Content-Filter-Profil referenziert wird.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Whitelists

**Mögliche Werte:**

- Name einer Whitelist
- maximal 31 Zeichen

**Default:**

leer

#### 2.41.2.3.2.2 Whitelist

Hier können Sie Webseiten konfigurieren, die lokal geprüft und anschließend akzeptiert werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Whitelists

**Mögliche Werte:**

- gültige URL-Adresse(n)
- maximal 252 Zeichen

Es können auch folgende Wildcards zum Einsatz kommen:

- * für mehrere beliebige Zeichen (z. B. findet www.lancom.* die Webseiten www.lancom.de, www.lancom.en, www.lancom.es etc.)
- ? für ein beliebiges Zeichen (z. B. findet www.lancom.e* die Webseiten www.lancom.en und www.lancom.es)

Bitte geben Sie die URL ohne führendes http:// ein. Beachten Sie, dass bei vielen URLs häufig automatisch ein Schrägstrich am Ende der URL angehängt wird, z. B. www.mycompany.de/ . Daher empfiehlt sich für die Eingabe an dieser Stelle die Form: www.mycompany.de*.

Einzelne URLs werden mit Leerzeichen getrennt.

**Default:**

leer

#### 2.41.2.3.3 Blacklists

Hier können Sie Webseiten konfigurieren, die anschließend verboten werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile

Die Einträge für die verbotenen Webseiten können maximal 252 Zeichen umfassen. Um längere Blacklist-Einträge zu definieren, können mehrere Einträge einen speziellen, gemeinsamen Namen verwenden. Geben Sie dazu den Namen der Blacklist ein gefolgt von einem #-Zeichen und einem beliebigen Suffix. Zum Beispiel legen Sie drei Blacklist-Einträge mit den Namen "MyBlacklist#1", "MyBlacklist#2" und "MyBlacklist#3" an. Im Content-Filter-Profil referenzieren Sie diese erweiterte Blacklist dann mit dem Namen "MyBlacklist".

#### 2.41.2.3.3.1 Name

Hier muss der Name der Blacklist angegeben werden, über den sie im Content-Filter-Profil referenziert wird.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Blacklists

**Mögliche Werte:**

- Name einer Blacklist
- maximal 31 Zeichen

**Default:**

leer

#### 2.41.2.3.3.2 Blacklist

Hier werden die URLs eingetragen, die über diese Blacklist verboten werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Blacklists

**Mögliche Werte:**

- gültige URL-Adresse(n)
- maximal 252 Zeichen

Es können auch folgende Wildcards zum Einsatz kommen:

- * für mehrere beliebige Zeichen (z. B. findet www.lancom.* die Webseiten www.lancom.de, www.lancom.en, www.lancom.es etc.)
- ? für ein beliebiges Zeichen (z. B. findet www.lancom.e* die Webseiten www.lancom.en und www.lancom.es)

Bitte geben Sie die URL ohne führendes http:// ein. Beachten Sie, dass bei vielen URLs häufig automatisch ein Schrägstrich am Ende der URL angehängt wird, z. B. www.mycompany.de/ . Daher empfiehlt sich für die Eingabe an dieser Stelle die Form: www.mycompany.de*.

Einzelne URLs werden mit Leerzeichen getrennt.

**Default:**

leer

#### 2.41.2.3.4 Kategorieprofile

Hier erstellen Sie ein Kategorieprofil und legen fest, welche Kategorien bzw. Gruppen bei der Bewertung der Webseiten berücksichtigt werden. Für jede Gruppe können Sie die einzelnen Kategorien erlauben, verbieten oder die Override-Funktion aktivieren.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/

#### 2.41.2.3.4.1 Name

Hier wird der Name der Kategorieprofils angegeben, über den sie im Content-Filter-Profil referenziert wird.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

**Mögliche Werte:**

- Name eines Kategorieprofils
- maximal 31 Zeichen

**Default:**

leer

#### 2.41.2.3.4.100 Unbekannt

Legen Sie hier fest, wie der Content-Filter URLs behandlen soll, die der Ratingserver noch nicht kennt und für die er deshalb keine Kategorien liefern kann.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:** Erlaubt

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

#### 2.41.2.3.4.101 Pornographie/Erotic/Sex

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.103 Swimwear/Lingerie

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelegt werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.104 Shopping

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.105 Auctions/Classified_Ads

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelegt werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.106 Governmental/Non-Profit_Organizations

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelegt werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.108 Cities/Regions/Countries

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelegt werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.109 Education

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.110 Political_Parties

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.111 Religion/Spirituality

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.113 Illegal_Activities

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.114 Computer_Crime/Warez/Hacking

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.115 Political_Extreme/Hate/Discrimination

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.117 Violence/Extreme

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.118 Gambling/Lottery

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.119 Computer_Games

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.120 Toys

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.121 Cinema/Television/Social_Media

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.122 Recreational_Facilities/Theme_Parks

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.123 Arts/Museums/Theaters

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.124 Music/Radio_Broadcast

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.125 Literature/Books

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.126 Humor/Cartoons

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.127 News/Magazines

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.128 Webmail/Unified_Messaging

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.129 Chat

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.130 Blogs/Bulletin_Boards

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.131 Mobile_Telephony

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.132 Digital_Postcards

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.133 Search_Engines/Web_Catalogs/Portals

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.134 Software/Hardware

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.135 Communication_Services

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.136 IT_Security/IT_Information

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.137 Web_Site_Translation

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.138 Anonymous_Proxies

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.139 Illegal_Drugs

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.140 Alcohol/Tobacco

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### 2.41.2.3.4.143 Dating/Networks

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### Restaurants/Entertainment_Venues

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**SNMP-ID:** 2.41.2.3.4.144

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

#### Travel

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**SNMP-ID:** 2.41.2.3.4.145

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

**Fashion/Cosmetics/Jewelry**

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**SNMP-ID:** 2.41.2.3.4.146

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

**Sports**

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**SNMP-ID:** 2.41.2.3.4.147

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

**Architecture/Construction/Furniture**

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**SNMP-ID:** 2.41.2.3.4.148

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

**Environment/Climate/Pets**

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**SNMP-ID:** 2.41.2.3.4.149

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

**Personal_Web_Sites**

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**SNMP-ID:** 2.41.2.3.4.150

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

**Job_Search**

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**SNMP-ID:** 2.41.2.3.4.151

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

**Finance/Investment**

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**SNMP-ID:** 2.41.2.3.4.152

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

**Banking**

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**SNMP-ID:** 2.41.2.3.4.154

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

**Vehicles**

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**SNMP-ID:** 2.41.2.3.4.155

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

**Weapons/Military**

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**SNMP-ID:** 2.41.2.3.4.156

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

**Medicine/Health/Self-Help**

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**SNMP-ID:** 2.41.2.3.4.157

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

**Abortion**

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**SNMP-ID:** 2.41.2.3.4.158

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

**Spam_URLs**

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**SNMP-ID:** 2.41.2.3.4.160

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

**Malware**

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**SNMP-ID:** 2.41.2.3.4.161

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

**Phishing_URLs**

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**SNMP-ID:** 2.41.2.3.4.162

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

**Instant_Messaging**

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**SNMP-ID:** 2.41.2.3.4.163

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

**General_Business**

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**SNMP-ID:** 2.41.2.3.4.167

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

**Banner_Advertisements**

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**SNMP-ID:** 2.41.2.3.4.174

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

**Web_Storage**

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

**SNMP-ID:** 2.41.2.3.4.180

**Pfad Telnet:** /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

**Mögliche Werte:**

Erlaubt, Verboten, Override

**Default:**

Erlaubt

# 2.42 ADSL

Asymmetrical Digital Subscriber Line - Übertragungsverfahren für die Hochgeschwindigkeitsdatenübertragung über normale Telefonverkabelungen. Mit ADSL sind Übertragungen (Downstream) bis zu 6 Mbit/s über normale Telefonkabel realisierbar, für die bidirektionale Übertragung steht ein zweites Frequenzband mit Übertragungsgeschwindigkeiten bis zu 640 kbit/s (Upstream) zur Verfügung - daher auch die Bezeichnung asymmetrisch.

**SNMP-ID:** 2.42

**Pfad Telnet:** /Setup

## 2.42.1 Trace-Modus

Der Trace-Modus legt fest, ob im ADSL-Trace auch interne Statuswerte ausgegeben werden (Erweitert), oder nur der Leitungsstatus (Einfach).

**SNMP-ID:** 2.42.1

**Pfad Telnet:** /Setup/ADSL/Trace-Modus

**Mögliche Werte Telnet:**

- Einfach
- Erweitert

**Default:** Erweitert

Ab der Firmware-Version 8.20 gilt 'Einfach' als Default.

## 2.42.4 Ueberwachungszeit(Std)

Dieser Parameter gibt dieUeberwachungszeit in Stunden an.

Verbindungsabbrueche (*2.42.3 Verbindungsabbrueche*) und Ueberwachungszeit gehören zum ADSL-Automodus. Sie geben zusammen an, wieviele Leitungsfehler in welcher Zeit erlaubt sind, um einen Linecode als funktionierend und stabil zu akzeptieren.

Bei den Leitungsfehlern wird der erste Syncverlust nicht gezählt, wenn er innerhalb der ersten Minute auftritt. Wird die zulässige Anzahl der Leitungsfehler in der Überwachungszeit überschritten, wählt das Gerät einen anderen Linecode.

**Pfad Telnet:** /Setup/ADSL/Ueberwachungszeit(Std)

**Mögliche Werte:**

- maximal 5 numerische Zeichen

**Default:** 24

Wenn Sie den Linecode fest in die Konfiguration eingetragen beachtet das Gerät diese Einstellung nicht.

## 2.42.3 Verbindungsabbrueche

Dieser Parameter gibt die maximal erlaubte Zahl von Verbindungsabbrüchen an.

Verbindungsabbrueche und Ueberwachungszeit (*2.42.4 Ueberwachungszeit(Std)*) gehören zum ADSL-Automodus. Sie geben zusammen an, wieviele Leitungsfehler in welcher Zeit erlaubt sind, um einen Linecode als funktionierend und stabil zu akzeptieren.

Bei den Leitungsfehlern wird der erste Syncverlust nicht gezählt, wenn er innerhalb der ersten Minute auftritt. Wird die zulässige Anzahl der Leitungsfehler in der Überwachungszeit überschritten, wählt das Gerät einen anderen Linecode.

**SNMP-ID:** 2.42.3

**Pfad Telnet:** /Setup/ADSL/Verbindungsabbrueche

**Mögliche Werte Telnet:**

- maximal 2 numerische Zeichen

**Default:** 1

Wenn Sie den Linecode fest in die Konfiguration eingetragen beachtet das Gerät diese Einstellung nicht.

# 2.52 COM-Ports

Dieses Menü enthält die Konfiguration der COM-Ports.

**SNMP-ID:** 2.52

**Pfad Telnet:** /Setup

## 2.52.1 Geraete

Die seriellen Schnittstellen können im LANCOM für verschiedene Anwendungen genutzt werden, z. B. für den COM-Port-Server oder als WAN-Schnittstelle. In der Geräte-Tabelle können den einzelnen seriellen Geräten bestimmte Anwendungen zugewiesen werden.

**SNMP-ID:** 2.52.1

**Pfad Telnet:** /Setup/COM-Ports

### 2.52.1.1 Device-Type

Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

**SNMP-ID:** 2.52.1.1

**Pfad Telnet:** /Setup/COM-Ports/Geraete

**Mögliche Werte:**

- Alle verfügbaren seriellen Schnittstellen.

**Default:** Outband

### 2.52.1.4 Dienst

Aktivierung des Ports für den COM-Port-Server.

**SNMP-ID:** 2.52.1.4

**Pfad Telnet:** /Setup/COM-Ports/Geraete

**Mögliche Werte:**

- WAN
- COM-Port server

**Default:** WAN

## 2.52.2 COM-Port-Server

Dieses Menü enthält die Konfiguration des COM-Port-Servers.

**SNMP-ID:** 2.52.2

**Pfad Telnet:** /Setup/COM-Ports

### 2.52.2.1 Betrieb

Diese Tabelle aktiviert den COM-Port-Server auf einem Port einer bestimmten seriellen Schnittstelle. Fügen Sie dieser Tabelle eine Zeile hinzu, um eine neue Instanz des COM-Port-Servers zu starten. Löschen Sie eine Zeile, um die entsprechende Server-Instanz abzubrechen.

**SNMP-ID:** 2.52.2.1

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server

#### 2.52.2.1.1 Device-Type

Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

**SNMP-ID:** 2.52.2.1.1

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/Device-Type

**Mögliche Werte:**

- Alle verfügbaren seriellen Schnittstellen.

**Default:** Outband

#### 2.52.2.1.2 Port-Nummer

Manche seriellen Geräte wie z. B. die CardBus haben mehr als einen seriellen Port. Tragen Sie hier die Nummer des Ports ein, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt werden soll.

**SNMP-ID:** 2.52.2.1.2

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/Device-Type

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

**Besondere Werte:** 0 für serielle Schnittstellen mit nur einem Port wie z. B. Outband.

#### 2.52.2.1.4 Operating

Aktiviert den COM-Port-Server auf dem gewählten Port der gewählten Schnittstelle.

**SNMP-ID:** 2.52.2.1.4

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/Device-Type

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

### 2.52.2.2 COM-Port-Einstellungen

Diese Tabelle enthält die Einstellungen für die Datenübertragung auf der seriellen Schnittstelle.

Bitte beachten Sie, dass alle diese Parameter durch die Gegenstelle überschrieben werden können, wenn die RFC2217-Verhandlung aktiviert ist; die aktuellen Einstellungen können im Status-Menü eingesehen werden.

**SNMP-ID:** 2.52.2.2

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server

#### 2.52.2.2.1 Device-Type

Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

**SNMP-ID:** 2.52.2.2.1

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/COM-Port-Einstellungen

**Mögliche Werte:**

- Alle verfügbaren seriellen Schnittstellen.

**Default:** Outband

#### 2.52.2.2.10 Bereit-Daten-Timeout

Der Timeout schaltet den Port wieder in den Zustand Nicht-Bereit, wenn keine Daten empfangen werden. Mit einem Timeout von Null wird diese Funktion ausgeschaltet. In diesem Fall ist der Port immer bereit, wenn der Daten-Modus gewählt ist.

**SNMP-ID:** 2.52.2.2.10

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/COM-Port-Einstellungen

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

**Besondere Werte:** 0 schaltet den Bereit-Daten-Timeout aus.

#### 2.52.2.2.2 Port-Nummer

Manche seriellen Geräte wie z. B. die CardBus haben mehr als einen seriellen Port. Tragen Sie hier die Nummer des Ports ein, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt werden soll.

**SNMP-ID:** 2.52.2.2.2

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/COM-Port-Einstellungen

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

**Besondere Werte:** 0 für serielle Schnittstellen mit nur einem Port wie z. B. Outband.

#### 2.52.2.2.4 Bitrate

Verwendete Bitrate auf dem COM-Port.

**SNMP-ID:** 2.52.2.2.4

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/COM-Port-Einstellungen

**Mögliche Werte:**

- 110 bis 230400

**Default:** 9600

#### 2.52.2.2.5 Daten-Bits

Anzahl der Daten-Bits.

**SNMP-ID:** 2.52.2.2.5

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/COM-Port-Einstellungen

**Mögliche Werte:**

- 7
- 8

**Default:** 8

#### 2.52.2.2.6 Paritaet

Auf dem COM-Port verwendetes Prüfverfahren.

**SNMP-ID:** 2.52.2.2.6

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/COM-Port-Einstellungen

**Mögliche Werte:**

- keine
- gerade
- ungerade

**Default:** keine

#### 2.52.2.2.7 Stop-Bits

Anzahl der Stop-Bits.

**SNMP-ID:** 2.52.2.2.7

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/COM-Port-Einstellungen

**Mögliche Werte:**

- 1
- 2

**Default:** 1

#### 2.52.2.2.8 Handshake

Auf dem COM-Port verwendete Datenflusskontrolle.

**SNMP-ID:** 2.52.2.2.8

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/COM-Port-Einstellungen

**Mögliche Werte:**

- keiner
- RTS/CTS

**Default:** RTS/CTS

#### 2.52.2.2.9 Bereit-Bedingung

Eine wichtige Eigenschaft eines seriellen Ports ist die Bereit-Bedingung. Der COM-Port-Server überträgt keine Daten zwischen dem seriellen Port und dem Netzwerk, solange er sich nicht im Zustand “Bereit” befindet. Außerdem wird der Wechsel zwischen den Zuständen “Bereit” und “Nicht-Bereit” verwendet, um im Client-Modus TCP-Verbindungen aufzubauen bzw. abzubrechen. Die Bereitschaft des Ports kann auf zwei verschiedene Arten ermittelt werden. Im DTR-Modus (Default) wird nur der DTR-Handshake überwacht. Die serielle Schnittstelle wird solange als bereit angesehen, wie die DTR-Leitung aktiv ist. Im Daten-Modus wird die serielle Schnittstelle als bereit betrachtet, sobald sie Daten empfängt. Wenn für die eingestellte Timeout-Zeit keine Daten empfangen werden, fällt der Port zurück in den Zustand “Nicht-Bereit”.

**SNMP-ID:** 2.52.2.2.9

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/COM-Port-Einstellungen

**Mögliche Werte:**

- DTR
- Daten

**Default:** DTR

### 2.52.2.3 Netzwerk-Einstellungen

Diese Tabelle enthält alle Einstellungen, die das Verhalten des COM-Ports im Netzwerk definieren.

Bitte beachten Sie, dass alle diese Parameter durch die Gegenstelle überschrieben werden können, wenn die RFC2217-Verhandlung aktiviert ist; die aktuellen Einstellungen können im Status-Menü eingesehen werden.

**SNMP-ID:** 2.52.2.3

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server

#### 2.52.2.3.1 Device-Type

Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

**SNMP-ID:** 2.52.2.3.1

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

**Mögliche Werte:**

- Alle verfügbaren seriellen Schnittstellen.

**Default:** Outband

#### 2.52.2.3.10 Newline-Konversion

Wählen Sie hier aus, welches Zeichen auf dem seriellen Port ausgegeben wird, wenn der Binär-Modus aktiviert ist.

Die Einstellung ist abhängig von der Anwendung, die über den seriellen Port kommunizieren wird. Wenn an den Port ein weiteres LANCOM-Gerät angeschlossen ist, können Sie hier entweder CRLF oder nur CR wählen, da die Outband-Schnittstelle dieser Geräte ein "Carriage Return" zur automatischen Bestimmung der Datenübertragungsgeschwindigkeit erwartet. Manche Unix-Anwendungen würden CRLF allerdings als unerlaubte doppelte Zeilenschaltung interpretieren, in diesem Fall wählen Sie CR oder LF.

**SNMP-ID:** 2.52.2.3.10

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

**Mögliche Werte:**

- CRLF
- CR
- LF

**Default:**

CRLF

Diese Einstellung wird nur ausgewertet, wenn für diesen seriellen Port der Binär-Modus deaktiviert ist.

#### 2.52.2.3.11 Nehme-Binaermodus-an

Manche Netzwerkgeräte, die an einem seriellen COM-Port angeschlossen sind, versenden Datenstrukturen, die als Steuerzeichen (CR/LF – Carriage Return / Line Feed) interpretiert werden können. In der Standardeinstellung werten die COM-Ports in den LANCOM-Geräten diese Informationen aus, um den Datenfluss zu steuern. Mit dem "Binärmodus" kann ein COM-Port angewiesen werden, alle Daten binär weiterzuleiten und keine Anpassungen dieser Steuerzeichen vorzunehmen.

**SNMP-ID:** 2.52.2.3.11

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

**Mögliche Werte:**

- Ja
- Nein

**Default:** Nein

#### 2.52.2.3.12 TCP-Wdh.-Timeout

Maximale Zeit für den Retransmission-Timeout. Dieser Timeout gibt an, in welchen Intervallen der Zustand einer TCP-Verbindung geprüft und das Ergebnis an die Applikation gemeldet wird, welche die entsprechende TCP-Verbindung nutzt.

**SNMP-ID:** 2.52.2.3.12

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

**Mögliche Werte:**

- 0 bis 99 Sekunden
- maximal 2 Zeichen

**Besondere Werte:**

- 0 verwendet den Standardwert nach RFC 1122 (60 Sekunden).

**Default:**

- 0

Die maximale Dauer der TCP-Verbindungsprüfung wird aus dem Produkt von TCP-Wdh.-Timeout und TCP-Wdh.-Zahl gebildet. Erst wenn der Timeout für alle Versuche abgelaufen ist, wird die entsprechende TCP-Anwendung informiert. Mit den Standardwerten von 60 Sekunden Timeout und maximal 5 Versuchen kann es bis zu 300 Sekunden dauern, bis eine nicht aktive TCP-Verbindung von der Applikation erkannt wird.

#### 2.52.2.3.13 TCP-Wdh.-Zahl

Maximale Anzahl der Versuche, mit denen der Zustand einer TCP-Verbindung geprüft und das Ergebnis an die Applikation gemeldet wird, welche die entsprechende TCP-Verbindung nutzt.

**SNMP-ID:** 2.52.2.3.13

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

**Mögliche Werte:**

- 0 bis 9
- maximal 1 Zeichen

**Besondere Werte:**

- 0 verwendet den Standardwert nach RFC 1122 (5 Versuche).

**Default:**

- 0

Die maximale Dauer der TCP-Verbindungsprüfung wird aus dem Produkt von TCP-Wdh.-Timeout und TCP-Wdh.-Zahl gebildet. Erst wenn der Timeout für alle Versuche abgelaufen ist, wird die entsprechende TCP-Anwendung informiert. Mit den Standardwerten von 60 Sekunden Timeout und maximal 5 Versuchen kann es bis zu 300 Sekunden dauern, bis eine nicht aktive TCP-Verbindung von der Applikation erkannt wird.

#### 2.52.2.3.14 TCP-Keepalive

Der RFC 1122 definiert ein Verfahren, mit dem die Verfügbarkeit von TCP-Verbindungen geprüft werden kann (TCP-Keepalive). Ein inaktiver Transmitter sendet nach diesem Verfahren Anfragen nach dem Empfängerstatus an die Gegenstelle. Wenn die TCP-Sitzung zur Gegenstelle verfügbar ist, antwortet diese mit ihrem Empfängerstatus. Wenn die TCP-Sitzung zur Gegenstelle nicht verfügbar ist, wird die Anfrage in einem kürzeren Intervall solange wiederholt, bis die Gegenstelle mit ihrem Empfängerstatus antwortet (danach wird wieder ein längeres Intervall verwendet). Sofern die zugrunde liegende Verbindung funktioniert, die TCP-Sitzung zur Gegenstelle allerdings nicht verfügbar ist, sendet die Gegenstelle ein RST-Paket und löst so den Abbau der TCP-Sitzung bei der anfragenden Applikation aus.

**SNMP-ID:** 2.52.2.3.14

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

**Mögliche Werte:**

- inaktiv: Der TCP-Keepalive wird nicht verwendet.
- aktiv: Der TCP-Keepalive ist aktiv, nur RST-Pakete führen zum Abbau von TCP-Sitzungen.
- proaktiv: Der TCP-Keepalive ist aktiv, wiederholt die Anfrage nach dem Empfängerstatus der Gegenstelle aber nur für den als "TCP-Wdh.-Zahl" eingestellten Wert. Sofern nach dieser Anzahl von Anfragen keine Antwort mit dem Empfängerstatus vorliegt, wird die TCP-Sitzung als "nicht verfügbar" eingestuft und an die Applikation gemeldet. Wird während der Wartezeit ein RST-Paket empfangen, so löst dieses vorzeitig den Abbau der TCP-Sitzung aus.

**Default:**

- inaktiv

Für Serverapplikationen wird die Einstellung "aktiv" empfohlen.

#### 2.52.2.3.15 TCP-Keepalive-Intervall

Dieser Wert gibt an, in welchen Intervallen die Anfragen nach dem Empfängerstatus versendet werden, wenn die erste Anfrage nicht erfolgreich beantwortet wurde. Der dazu gehörende Timeout wird gebildet als Intervall / 3 (maximal 75 Sekunden).

**SNMP-ID:** 2.52.2.3.15

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

**Mögliche Werte:**

- maximal 10 Ziffern

**Default:**

- 0

**Besondere Werte:**

- 0 verwendet den Standardwert nach RFC 1122 (Intervall 7200 Sekunden, Timeout 75 Sekunden).

#### 2.52.2.3.2 Port-Nummer

Manche seriellen Geräte wie z. B. die CardBus haben mehr als einen seriellen Port. Tragen Sie hier die Nummer des Ports ein, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt werden soll.

**SNMP-ID:** 2.52.2.3.2

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

**Besondere Werte:** 0 für serielle Schnittstellen mit nur einem Port wie z. B. Outband.

#### 2.52.2.3.4 TCP-Modus

Jede Instanz des COM-Port-Servers überwacht im Server-Modus den definierten Listen-Port auf eingehende TCP-Verbindungen. Pro Instanz ist nur eine aktive Verbindung erlaubt, alle anderen Verbindungsanfragen werden abgelehnt. Im Client-Modus versucht die Instanz eine TCP-Verbindung über einen definierten Port zur angegebenen Gegenstelle aufzubauen, sobald der Port bereit ist. Die TCP-Verbindung wird wieder geschlossen, sobald der Port nicht mehr bereit ist. In beiden Fällen schließt ein LANCOM die offenen Verbindungen bei einem Neustart des Gerätes.

**SNMP-ID:** 2.52.2.3.4

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

**Mögliche Werte:**

- Server
- Client

**Default:** Server

#### 2.52.2.3.5 Listen-Port

Auf diesem TCP-Port erwartet der COM-Port im TCP-Server-Modus eingehende Verbindungen.

**SNMP-ID:** 2.52.2.3.5

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

#### 2.52.2.3.6 Aufbau-Host-Name

Zu diesem Host baut der COM-Port im TCP-Client-Modus eine Verbindung auf, sobald sich der Port im Zustand “Bereit” befindet.

**SNMP-ID:** 2.52.2.3.6

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

**Mögliche Werte:**

- DNS-Name
- IP-Adresse

**Default:** leer

#### 2.52.2.3.7 Aufbau-Port

Über diesen TCP-Port baut der COM-Port im TCP-Client-Modus eine Verbindung auf, sobald sich der Port im Zustand “Bereit” befindet.

**SNMP-ID:** 2.52.2.3.7

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

**Mögliche Werte:**

- max. 10 Zeichen

**Default:** 0

#### 2.52.2.3.8 Loopback-Addr.

Über diese Adresse kann der COM-Port angesprochen werden. Dies ist die eigene IP-Adresse, die als Quelladresse beim Verbindungsaufbau benutzt wird. Sie wird z. B. verwendet, um die IP-Route festzulegen, über die die Verbindung aufgebaut wird.

**SNMP-ID:** 2.52.2.3.8

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

**Mögliche Werte:**

- max. 16 Zeichen

**Default:** leer

#### 2.52.2.3.9 RFC2217-Erweiterungen

Die RFC2217-Erweiterungen können für beide TCP-Modi aktiviert werden. Wenn diese Erweiterungen eingeschaltet sind, signalisiert ein LANCOM seine Bereitschaft, Telnet Steuerungssequenzen zu akzeptieren, mit der Sequenz IAC DO COM-PORT-OPTION. In der Folge werden auf dem COM-Port die entsprechenden Optionen verwendet, die konfigurierten Default-Werte werden überschrieben. Außerdem versucht der Port, für Telnet das lokale Echo und den Line Mode zu verhandeln. Die Verwendung der RFC2217-Erweiterungen ist auch bei nicht kompatibler Gegenstelle unkritisch, möglicherweise werden dann unerwartete Zeichen bei der Gegenstelle angezeigt. Als Nebeneffekt führt die Verwendung der RFC2217-Erweiterungen dazu, dass der Port einen regelmäßigen Alive-Check durchführt, indem Telnet-NOPs zur Gegenstelle gesendet werden.

**SNMP-ID:** 2.52.2.3.9

**Pfad Telnet:** /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

**Mögliche Werte:**

- Ja
- Nein

**Default:** Ja

## 2.52.3 WAN

Dieses Menü enthält die Konfiguration des Wide-Area-Networks (WAN).

**SNMP-ID:** 2.52.3

**Pfad Telnet:** /Setup/COM-Ports

### 2.52.3.1 Geraete

Die Tabelle mit den WAN-Geräten dient nur als Status-Tabelle. Alle Hotplug-Geräte (über USB oder CardBus angeschlossen) tragen sich selbst in diese Tabelle ein.

**SNMP-ID:** 2.52.3.1

**Pfad Telnet:** /Setup/COM-Ports/WAN

#### 2.52.3.1.1 Device-Type

Liste der im Gerät verfügbaren seriellen Schnittstellen.

**SNMP-ID:** 2.52.3.1.1

**Pfad Telnet:** /Setup/COM-Ports/WAN/Geraete

**Mögliche Werte:**

- Alle verfügbaren seriellen Schnittstellen.

#### 2.52.3.1.3 Aktiv

Status des angeschlossenen Gerätes.

**SNMP-ID:** 2.52.3.1.3

**Pfad Telnet:** /Setup/COM-Ports/WAN/Geraete

**Mögliche Werte:**

- Ja
- Nein

## 2.52.4 Serielle-Konfig

Dieses Menü enthält die Konfiguration für die Autokonfiguration von WLAN-Strecken über eine serielle Verbindung.

**SNMP-ID:** 2.52.4

**Pfad Telnet:** /Setup/COM-Ports

### 2.52.4.1 Bit-Rate

Stellen Sie hier die Bitrate ein, mit der die Geräte bei der automatischen Konfiguration von WLAN-Strecken über serielle Verbindungen kommunizieren.

**SNMP-ID:** 2.52.4.1

**Pfad Telnet:** /Setup/COM-Ports

**Mögliche Werte:**

- 1200
- 2400
- 4800
- 9600
- 19200
- 38400
- 57600
- 115200

**Default:** 9600

Die identische Einstellung der Bit-Rate bei allen Geräten, die über serielle Verbindungen kommunizieren, ist eine zwingende Voraussetzung für die automatische Konfiguration der WLAN-Strecken.

# 2.53 Temperatur-Monitor

Hier finden Sie die Einstellungen für den Temperatur-Monitor.

**SNMP-ID:** 2.53

**Pfad Telnet:** /Setup/Temperatur-Monitor

## 2.53.1 Obergrenze-Grad

Bei Überschreiten der hier eingestellten Temperatur sendet das Gerät einen SNMP-Trap vom Typ "trpTempMonOverTemp" aus.

**Pfad Telnet:** /Setup/Temperatur-Monitor/Obergrenze-Grad

**Mögliche Werte**:

- 0 bis 127 ° Celsius

**Default**: 70

### 2.53.2 Untergrenze-Grad

Bei Unterschreiten der hier eingestellten Temperatur sendet das Gerät einen SNMP-Trap vom Typ "trpTempMonUnderTemp" aus.

**Pfad Telnet:** /Setup/Temperatur-Monitor/Untergrenze-Grad

**Mögliche Werte**:

- 0 bis 127 ° Celsius

**Default**: 0

## 2.54 TACACS

### 2.54.3 Accounting

**WEBconfig:** /Setup/TACACS+

Aktiviert das Accounting über einen TACACS+-Server. Wenn das TACACS+-Accounting aktiviert ist, werden alle Accounting-Daten über das TACACS+-Protokoll an den konfigurierten TACACS+-Server übertragen.

Mögliche Werte: aktiviert, deaktiviert

Default: deaktiviert

Das TACACS+-Accounting wird nur dann aktiviert, wenn ein erreichbarer TACACS+-Server definiert ist.

### 2.54.1 Autentifizierung

**WEBconfig:** /Setup/TACACS+

**WEBconfig englisch:** LCOS menu tree/Setup/TACACS+

Aktiviert die Authentifizierung über einen TACACS+-Server. Wenn die TACACS+-Authentifizierung aktiviert ist, werden alle Authentifizierung-Anfragen über das TACACS+-Protokoll an den konfigurierten TACACS+-Server übertragen.

**Mögliche Werte:** aktiviert, deaktiviert

**Default:** deaktiviert

Die TACACS+-Authentifizierung wird nur dann aktiviert, wenn ein erreichbarer TACACS+-Server definiert ist. Der Rückgriff auf lokale Benutzer kann dabei nur genutzt werden, wenn für das LANCOM ein Root-Kennwort gesetzt ist. Bei Geräten ohne Root-Kennwort muss der Rückgriff auf lokale Benutzer deaktiviert werden, da sonst bei Ausfall der Netzwerkverbindung (TACACS+-Server nicht erreichbar) ein Zugriff ohne Kennwort auf das LANCOM möglich wäre.

### 2.54.2 Authorisierung

**WEBconfig:** /Setup/TACACS+

**WEBconfig englisch:** LCOS menu tree/Setup/TACACS+

Aktiviert die Authorisierung über einen TACACS+-Server. Wenn die TACACS+-Authorisierung aktiviert ist, werden alle Authorisierungs-Anfragen über das TACACS+-Protokoll an den konfigurierten TACACS+-Server übertragen.

**Mögliche Werte:** aktiviert, deaktiviert

**Default:** deaktiviert

Die TACACS+-Authorisierung wird nur dann aktiviert, wenn ein erreichbarer TACACS+-Server definiert ist. Wenn die TACACS+-Authorisierung aktiviert ist, wird für jedes Kommando beim TACACS+-Server eine Anfrage gestellt, ob der Benutzer diese Aktion ausführen darf. Dementsprechend erhöht sich der Datenverkehr bei der Konfiguration, außerdem müssen die Rechte für die Benutzer im TACACS+-Server definiert sein.

## 2.54.10 Rückgriff auf lokale Benutzer

**WEBconfig:** /Setup/TACACS+

**WEBconfig englisch:** LCOS menu tree/Setup/TACACS+

Für den Fall, dass die definierten TACACS+-Server nicht erreichbar sind, kann ein Rückgriff auf die lokalen Benutzerkonten im LANCOM erlaubt werden. So ist der Zugriff auf die Geräte auch bei Ausfall der TACACS+-Verbindung möglich, z. B. um die TACACS+-Nutzung zu deaktivieren oder die Konfiguration zu korrigieren.

**Mögliche Werte:** erlaubt, verboten

**Default:** erlaubt

Der Rückgriff auf lokale Benutzerkonten stellt ein Sicherheitsrisiko dar, wenn kein Root-Kennwort im LANCOM gesetzt ist. Daher kann die TACACS+-Authentifizierung mit Rückgriff auf lokale Benutzerkonten nur aktiviert werden, wenn ein Root-Kennwort definiert ist. Wenn kein Root-Kennwort gesetzt ist, kann der Konfigurationszugang zu den Geräten aus Sicherheitsgründen gesperrt werden, wenn die Verbindung zu den TACACS+-Servern nicht verfügbar ist! In diesem Fall muss das Gerät möglicherweise in den Auslieferungszustand zurückgesetzt werden, um wieder Zugang zur Konfiguration zu erhalten.

## 2.54.6 Shared-Secret

**WEBconfig:** /Setup/TACACS+

Das Kennwort für die Verschlüsselung der Kommunikation zwischen NAS und TACACS+-Server.

**Mögliche Werte:** 31 alphanumerische Zeichen

**Default:** Leer

Das Kennwort muss im LANCOM und im TACACS+-Server übereinstimmend eingetragen werden. Eine Nutzung von TACACS+ ohne Verschlüsselung ist nicht zu empfehlen.

## 2.54.12 SNMP-GET-Anfragen-Accounting

**WEBconfig:** /Setup/TACACS+

**WEBconfig englisch:** LCOS menu tree/Setup/TACACS+

Zahlreiche Netzwerkmanagementtools nutzen SNMP, um Informationen aus den Netzwerkgeräten abzufragen. Auch der LANmonitor greift über SNMP auf die LANCOM-Geräte zu, um Informationen über aktuelle Verbindungen etc. darzustellen oder Aktionen wie das Trennen einer Verbindung auszuführen. Da über SNMP ein Gerät auch konfiguriert werden kann, wertet TACACS+ diese Zugriffe als Vorgänge, die eine Authorisierung voraussetzen. Da LANmonitor diese Werte regelmäßig abfragt, würde so eine große Zahl von eigentlich unnötigen TACACS+-Verbindungen aufgebaut. Wenn Authentifizierung, Authorisierung und Accounting für TACACS+ aktiviert sind, werden für jede Anfrage drei Sitzungen auf dem TACACS+-Server gestartet.

Mit diesem Parameter kann das Verhalten der LANCOM-Geräte bei SNMP-Zugriffen geregelt werden, um TACACS+-Sitzungen für das Accounting zu reduzieren. Eine Authentifizierung über den TACACS+-Server bleibt dennoch erforderlich, sofern die Authentifizierung für TACACS+ generell aktiviert ist.

Mit dem Eintrag einer Read-Only-Community unter /Setup/SNMP kann auch die Authentifizierung über TACACS+ für den LANmonitor deaktiviert werden. Die dort definierte Read-Only-Community wird dazu im LANmonitor als Benutzername eingetragen.

**Mögliche Werte:**

- nur_für_SETUP_Baum: In dieser Einstellung ist nur bei SNMP-Zugriff auf den Setup-Zweig von LCOS ein Accounting über den TACACS+-Server erforderlich.
- alle: In dieser Einstellung wird für alle SNMP-Zugriffe ein Accounting über den TACACS+-Server durchgeführt. Werden z. B. Status-Informationen regelmäßig abgefragt, erhöht diese Einstellung deutlich die Last auf dem TACACS+-Server.
- keine: In dieser Einstellung ist für die SNMP-Zugriffe kein Accounting über den TACACS+-Server erforderlich.

**Default:** nur_für_SETUP_Baum

## 2.54.11 SNMP-GET-Anfragen-Authorisierung

**WEBconfig:** /Setup/TACACS+

**WEBconfig englisch:** LCOS menu tree/Setup/TACACS+

Mit diesem Parameter kann das Verhalten der LANCOM-Geräte bei SNMP-Zugriffen geregelt werden, um TACACS+-Sitzungen für die Authorisierung zu reduzieren. Eine Authentifizierung über den TACACS+-Server bleibt dennoch erforderlich, sofern die Authentifizierung für TACACS+ generell aktiviert ist.

**Mögliche Werte:**

- nur_für_SETUP_Baum: In dieser Einstellung ist nur bei SNMP-Zugriff auf den Setup-Zweig von LCOS eine Authorisierung über den TACACS+-Server erforderlich.
- alle: In dieser Einstellung wird für alle SNMP-Zugriffe eine Authorisierung über den TACACS+-Server durchgeführt. Werden z. B. Status-Informationen regelmäßig abgefragt, erhöht diese Einstellung deutlich die Last auf dem TACACS+-Server.
- keine: In dieser Einstellung ist für die SNMP-Zugriffe keine Authorisierung über den TACACS+-Server erforderlich.

**Default:** nur_für_SETUP_Baum

## 2.54.13 Umgehe-Tacacs-fuer-CRON/Skripte/Aktions-Tabelle

Hier können Sie die Umgehung der TACACS-Autorisierung und des TACACS+-Accounting für verschiedene Aktionen aktivieren bzw. deaktivieren.

**SNMP-ID:** 2.54.13

**Pfad Telnet:** /Setup/Tacacs+

**Mögliche Werte:**

- aktiviert
- deaktiviert

**Default:** deaktiviert

Bitte beachten Sie, dass die Funktion von TACACS+ für das gesamte System über diese Optionen beeinflusst wird. Beschränken Sie die Nutzung von CRON, der Aktionstabelle und von Scripten auf jeden Fall auf einen absolut vertrauenswürdigen Kreis von Administratoren!

## 2.54.7 Verschlüsselung

**WEBconfig:** /Setup/TACACS+

**WEBconfig englisch:** LCOS menu tree/Setup/TACACS+

Aktiviert oder deaktiviert die Verschlüsselung der Kommunikation zwischen NAS und TACACS+-Server.

**Mögliche Werte:**

- aktiviert
- deaktiviert

**Default:** aktiviert

Eine Nutzung von TACACS+ ohne Verschlüsselung ist nicht zu empfehlen. Wenn die Verschlüsselung hier aktiviert wird, muss außerdem das Kennwort für die Verschlüsselung passend zum Kennwort auf dem TACACS+-Server eingetragen werden.

## 2.54.14 Wert-zu-Authorisierungsanfrage-hinzufuegen

Wenn Sie diese Funktion deaktivieren, dann prüft TACACS+ nur beim Login die Benutzerrechte des Nutzers. Bei der Eingabe von Werten prüft das Gerät dann nicht erneut, ob der Benutzer die Berechtigung hat bestimmte Werte zu ändern.

**Pfad Telnet:** /Setup/Tacacs+/Wert-zu-Authorisierungsanfrage-hinzufuegen

**Mögliche Werte:**

- aktiviert: TACACS+ prüft bei der Übergabe von Werten, ob der Benutzer die Rechte hat diese zu ändern
- deaktiviert: TACACS+ prüft die Identität des Nutzers lediglich beim Login

**Default:** aktiviert

## 2.54.9 Server

Zur Nutzung der TACACS+-Funktionen können zwei Server definiert werden. Dabei dient ein Server als Backup, falls der andere Server ausfällt. Beim Login über Telnet oder WEBconfig kann der Anwender den zu benutzenden Server auswählen.

Dieses Menü enthält die Einstellungen für die TACACS-Server.

**SNMP-ID:** 2.54.9

**Pfad Telnet:** /Setup/TACACS+

### 2.54.9.1 Server-Adresse

Adresse des TACACS+-Server, an den die Anfragen für Authentifizierung, Authorisierung und Accounting weitergeleitet werden sollen.

**SNMP-ID:** 2.54.9.1

**Pfad Telnet:** /Setup/Tacacs+/Server-Adresse

**Mögliche Werte Telnet:**

- Gültiger DNS-auflösbarer Name oder gültige IP-Adresse.

**Default:** Leer

### 2.54.9.2 Loopback-Adresse

Hier können Sie optional eine Loopback-Adresse konfigurieren.

**SNMP-ID:** 2.54.9.2

**Pfad Telnet:** /Setup/Tacacs+/Loopback-Adresse

**Mögliche Werte Telnet:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll

- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

**Default:** Leer

### 2.54.9.3 Kompatibilitätsmodus

TACACS+-Server werden in einer freien und in einer kommerziellen Version angeboten, die jeweils unterschiedliche Nachrichten verwenden. Der Kompatibilitätsmodus ermöglicht die Verarbeitung der Nachrichten von den freien TACACS+-Servern.

**SNMP-ID:** 2.54.9.3

**Pfad Telnet:** /Setup/Tacacs+/Kompatibilitätsmodus

**Mögliche Werte Telnet:**

- aktiviert
- deaktiviert

**Default:** deaktiviert

## 2.56 Automatisches-Laden

In diesem Menü finden Sie die Konfiguration für das automatische Laden von Firmware oder Konfiguration von externen Datenträgern.

**SNMP-ID:** 2.56

**Pfad Telnet:** /Setup/Automatisches-Laden

## 2.56.1 Firmware-und-Loader

Mit dieser Option aktivieren Sie das automatische Laden von Loader- und/oder Firmware-Dateien von einem angeschlossenen USB-Medium.

**Pfad Telnet:** /Setup/Automatisches-Laden/Firmware-und-Loader

**Mögliche Werte:**

- Inaktiv: Das automatische Laden von Loader- und/oder Firmware-Dateien für das Gerät ist deaktiviert.
- Aktiv: Das automatische Laden von Loader- und/oder Firmware-Dateien für das Gerät ist aktiviert. Beim Mounten eines USB-Mediums wird versucht, eine passende Loader- und/oder Firmware-Datei in das Gerät zu laden. Das USB-Medium wird beim Einstecken in den USB-Anschluss am Gerät oder beim Neustart gemountet.
- Wenn-unkonfiguriert: Das automatische Laden von Loader- und/oder Firmware-Dateien für das Gerät wird nur dann aktiviert, wenn sich das Gerät im Auslieferungszustand befindet. Durch einen Konfigurations-Reset kann ein Gerät jederzeit wieder auf den Auslieferungszustand zurückgesetzt werden.

**Default:**

- Wenn-unkonfiguriert

Durch den Assistenten für Sicherheitseinstellungen bzw. für Grundeinstellungen wird diese Option auf "inaktiv" gesetzt.

## 2.56.2 Konfiguration-und-Skript

Mit dieser Option aktivieren Sie das automatische Laden von Konfigurations- und/oder Skript-Dateien von einem angeschlossenen USB-Medium.

**Pfad Telnet:** /Setup/Automatisches-Laden/Konfiguration-und-Skript

**Mögliche Werte:**

- Inaktiv: Das automatische Laden von Konfigurations- und/oder Skript-Dateien für das Gerät ist deaktiviert.
- Aktiv: Das automatische Laden von Konfigurations- und/oder Skript-Dateien für das Gerät ist aktiviert. Beim Mounten eines USB-Mediums wird versucht, eine passende Konfigurations- und/oder Skript-Dateien in das Gerät zu laden. Das USB-Medium wird beim Einstecken in den USB-Anschluss am Gerät oder beim Neustart gemountet.
- Wenn-unkonfiguriert: Das automatische Laden von Konfigurations- und/oder Skript-Dateien für das Gerät wird nur dann aktiviert, wenn sich das Gerät im Auslieferungszustand befindet. Durch einen Konfigurations-Reset kann ein Gerät jederzeit wieder auf den Auslieferungszustand zurückgesetzt werden.

**Default:**

- Wenn-unkonfiguriert

Durch den Assistenten für Sicherheitseinstellungen bzw. für Grundeinstellungen wird diese Option auf “inaktiv” gesetzt.

Wenn Sie verhindern wollen, dass ein Gerät durch manuellen Reset auf Werkseinstellungen und Einstecken eines USB-Datenträgers mit einer unerwünschten Konfiguration versehen werden kann, müssen Sie den Reset-Schalter deaktivieren.

# 2.59 WLAN-Management

Dieses Menü enthält die Konfiguration des WLAN-Managements für Access Points.

## 2.59.120 Log-Eintraege

Diese Parameter definiert die maximale Anzahl der Log-Einträge des Geräts.

**Pfad Telnet:** /Setup/WLAN-Management/Log-Eintraege

**Mögliche Werte:**

- 0 bis 9999

**Default:** 200

## 2.59.1 Statische-WLC-Konfiguration

In dieser Tabelle können Sie die WLAN-Controller (WLCs) angeben, mit denen ein gemanagter Access Point vornehmlich Verbindung aufnehmen soll. Befinden sich Access Point und WLC im gleichen IP-Netzwerk ist hier keine Einstellung erforderlich.

Diese Einstellung ist nur dann von Bedeutung, wenn sich mindestens ein WLAN-Interface des Geräts in der Betriebsart "Managed" befindet.

**SNMP-ID:** 2.59.1

**Pfad Telnet:** /Setup/WLAN-Management/Statische-WLC-Konfiguration

### 2.59.1.1 IP-Adresse

Hier wird der Name des CAPWAP-Services angegeben, über den der DNS-Server die WLAN-Controller auflöst.

Der Name ist so voreingestellt, dass Sie hier nichts ändern müssen. Der Parameter bietet jedoch grundsätzlich die Möglichkeit auch CAPWAP-Services anderer Hersteller hier zu verwenden.

**SNMP-ID:** 2.59.1.1

**Pfad Telnet:** /Setup/WLAN-Management/Statische-WLC-Konfiguration/IP-Adresse

**Mögliche Werte:**

- Gültige IP-Adresse oder auflösbarer Name eines WLC-Controllers

**Default:** WLC-Address

### 2.59.1.2 Port

Hier können Sie den Port angeben, der für die Kommunikation mit dem WLAN-Controller verwendet werden soll.

**SNMP-ID:** 2.59.1.2

**Pfad Telnet:** /Setup/WLAN-Management/Statische-WLC-Konfiguration/Port

**Mögliche Werte:**

- Gültige Port-Bezeichnung

**Default:** 1027

### 2.59.1.3 Loopback-Addr.

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

**SNMP-ID:** 2.59.1.3

**Pfad Telnet:** /Setup/WLAN-Management/Statische-WLC-Konfiguration/Loopback-Addr.

**Mögliche Werte:**

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll.
- "INT" für die Adresse des ersten Intranets.
- "DMZ" für die Adresse der ersten DMZ (Achtung: wenn es eine Schnittstelle Namens "DMZ" gibt, dann wird deren Adresse genommen).
- LB0 ... LBF für die 16 Loopback-Adressen.
- Desweiteren kann eine beliebige IP-Adresse in der Form x.x.x.x angegeben werden.

**Default:** leer

Die hier eingestellte Absendeadresse wird für jede Gegenstelle **unmaskiert** verwendet.

## 2.60 Automatisches-Laden

In diesem Menü finden Sie die Einstellungen für das automatische Laden von Firmware, Konfiguration oder Skript von externen Datenträgern oder von einer URL.

**SNMP-ID:** 2.60

**Pfad Telnet:** /Setup/Automatisches-Laden

## 2.60.1 Netzwerk

In diesem Menü finden Sie die Einstellungen für das Laden von Firmware, Konfiguration oder Skripten über das Netzwerk.

Die in diesem Bereich definierten Einstellungen werden verwendet, wenn auf der Kommandozeile die Befehle LoadFirmware, LoadConfig oder LoadScript aufgerufen werden. Diese Befehle laden Firmware, Konfiguration oder Skript mit Hilfe des TFTP- oder HTTP(S)-Clients in das Gerät.

**SNMP-ID:** 2.60.1

**Pfad Telnet:** /Setup/Automatisches-Laden/Netzwerk

Das Laden von Firmware, Konfiguration oder Skript mit Hilfe des TFTP- oder HTTP(S)-Clients ist nur erfolgreich, wenn die URL zum Laden der jeweiligen Datei vollständig konfiguriert ist und diese URL beim Ausführen des Befehls erreichbar ist. Alternativ kann die URL beim Aufruf des Befehls als Parameter übergeben werden.

Die im Bereich /Setup/Automatisches-Laden/Netzwerk eingestellten Werte für Bedingung, URL und Minimal-Version stellen Default-Werte dar. Diese Werte werden ausschließlich dann verwendet, wenn beim Aufruf der Befehle LoadFirmware, LoadConfig oder LoadScript auf der Kommandozeilekeine anderen entsprechenden Parameter übergeben werden.

### 2.60.1.1 Firmware

In diesem Menü finden Sie die Einstellungen für das Laden einer Firmware über das Netzwerk.

**SNMP-ID:** 2.60.1.1

**Pfad Telnet:** /Setup/Automatisches-Laden/Netzwerk/Firmware

#### 2.60.1.1.1 Bedingung

Wählen Sie hier die Bedingung aus, nach der die unter /Setup/Automatisches-Laden/Netzwerk/Firmware/URL angegebene Firmware geladen wird, wenn der Befehl LoadFirmware ausgeführt wird.

**SNMP-ID:** 2.60.1.1.1

**Pfad Telnet:** /Setup/Automatisches-Laden/Netzwerk/Firmware

**Mögliche Werte:**

- unbedingt: Die Firmware wird auf jeden Fall auf den Speicherplatz der inaktiven Firmware geladen und ausgeführt. Diese Einstellung deaktiviert die Versionsprüfung, die angegebene Firmware wird auf jeden Fall geladen.
- wenn-unterschiedlich: Die Firmware wird dann auf den Speicherplatz der inaktiven Firmware geladen und ausgeführt, wenn sie eine andere Version enthält als die im Gerät aktive und die inaktive Firmware. Wenn die Version der angegebenen Firmware einer der beiden vorhandenen Firmware-Versionen entspricht, wird die angegebene Firmware nicht geladen. Der Befehl LoadFirmware verwendet für den Vergleich die Firmware-Version (z. B. "8.10"), den Releasecode (z. B. "RU1") und das Dateidatum.
- wenn-neuer: Die Firmware wird nur dann geladen und ausgeführt, wenn sie neuer ist als die aktuell im Gerät aktive Firmware. Die Firmware wird dann auf den Speicherplatz der inaktiven Firmware geladen, wenn sie neuer ist als die im Gerät aktive und die inaktive Firmware. Wenn die Version der angegebenen Firmware älter ist als eine der beiden vorhandenen Firmware-Versionen, wird die angegebene Firmware nicht geladen.

**Default:** unbedingt

Wenn der Befehl LoadFirmware zweimal nacheinander mit der Einstellung "unbedingt" ausgeführt wird enthalten beide Speicherplätze für die Firmware die gleiche Version.

#### 2.60.1.1.2 Minimal-Version

Stellen Sie hier die Minimal-Version der Firmware für das Laden über das Netzwerk ein.

**SNMP-ID:** 2.60.1.1.2

**Pfad Telnet:** /Setup/Automatisches-Laden/Netzwerk/Minimal-Version

**Mögliche Werte:**

- max. 14 Zeichen

**Default:** leer

Firmware-Versionen mir einer niedrigeren Versionsbezeichnung werden ignoriert.

#### 2.60.1.1.3 URL

Geben Sie hier die URL der Firmware an, die mit dem Befehl LoadFirmware über das Netzwerk geladen wird.

**SNMP-ID:** 2.60.1.1.3

**Pfad Telnet:** /Setup/Automatisches-Laden/Firmware/URL

**Mögliche Werte:**

- max. 127 Zeichen, beginnend mit "tftp://", "http://" oder "https://"

**Default:** leer

Der TFTP- bzw. HTTP(S)-Client lädt die hier eingetragene Datei nur, wenn dem Befehl LoadFirmware keine URL als Parameter übergeben wurde. Wird eine URL als Parameter angegeben, kann gezielt eine andere Datei geladen werden.

### 2.60.1.2 Konfiguration

In diesem Menü finden Sie die Einstellungen für das Laden einer Konfiguration über das Netzwerk.

**SNMP-ID:** 2.60.1.2

**Pfad Telnet:** /Setup/Automatisches-Laden/Netzwerk/Konfiguration

#### 2.60.1.2.1 Bedingung

Wählen Sie hier die Bedingung aus, nach der die unter /Setup/Automatisches-Laden/Netzwerk/Konfiguration/URL angegebene Konfiguration beim Start des Gerätesgeladen wird.

**SNMP-ID:** 2.60.1.2.1

**Pfad Telnet:** /Setup/Automatisches-Laden/Netzwerk/Konfiguration

**Mögliche Werte:**

- unbedingt: Die Konfiguration wird auf jeden Fall geladen.
- wenn-unterschiedlich: Die Konfiguration wird nur dann geladen, wenn sie eine andere Versionsnummer enthält als die aktuell im Gerät aktive Konfiguration.

**Default:** unbedingt

#### 2.60.1.2.3 URL

Geben Sie hier die URL der Konfiguration an, die mit dem Befehl LoadConfig über das Netzwerk geladen wird.

**SNMP-ID:** 2.60.1.2.3

**Pfad Telnet:** /Setup/Automatisches-Laden/Konfiguration/URL

**Mögliche Werte:**

- max. 127 Zeichen, beginnend mit "tftp://", "http://" oder "https://"

**Default:** leer

Der TFTP- bzw. HTTP(S)-Client lädt die hier eingetragene Datei nur, wenn der Befehl LoadConfig ohne zusätzliche Parameter ausgeführt wird. Mit entsprechenden Parametern beim Befehlsaufruf kann gezielt eine andere Datei geladen werden.

### 2.60.1.3 Skript

In diesem Menü finden Sie die Einstellungen für das Laden eines Skriptes über das Netzwerk.

**SNMP-ID:** 2.60.1.3

**Pfad Telnet:** /Setup/Automatisches-Laden/Netzwerk/Skript

#### 2.60.1.3.1 Bedingung

Wählen Sie hier die Bedingung aus, nach der das unter /Setup/Automatisches-Laden/Netzwerk/Konfiguration/URL angegebene Skript ausgeführt wird, wenn der Befehl LoadScript ausgeführt wird.

**SNMP-ID:** 2.60.1.3.1

**Pfad Telnet:** /Setup/Automatisches-Laden/Netzwerk/Skript

**Mögliche Werte:**

- unbedingt: Das Skript wird auf jeden Fall ausgeführt. Diese Einstellung deaktiviert den Vergleich der Prüfsumme, das angegebene Skript wird auf jeden Fall ausgeführt.Dabei belässt der Befehl LoadScript die im Gerät gespeicherte Prüfsumme des zuletzt ausgeführten Skriptes unverändert.
- wenn-unterschiedlich: Das Skript wird nur dann ausgeführt, wenn es sich vom zuletzt ausgeführten Skript unterscheidet.Der Unterschied zum zuletzt ausgeführten Skript wird über eine Prüfsumme festgestellt. Das Skript wird dazu grundsätzlich vollständig heruntergeladen. Dann vergleicht der Befehl LoadScript die Prüfsumme des geladenen Skriptes mit der im Gerät gespeicherten Prüfsumme des zuletzt ausgeführten Skriptes. Wenn das Skript ausgeführt wird aktualisiert der Befehl LoadScript die im Gerät gespeicherte Prüfsumme.

**Default:** unbedingt

#### 2.60.1.3.3 URL

Geben Sie hier die URL des Skriptes an, das mit dem Befehl LoadScript über das Netzwerk geladen wird.

**SNMP-ID:** 2.60.1.3.3

**Pfad Telnet:** /Setup/Automatisches-Laden/Skript/URL

**Mögliche Werte:**

- max. 127 Zeichen, beginnend mit "tftp://", "http://" oder "https://"

**Default:** leer

Der TFTP- bzw. HTTP(S)-Client lädt die hier eingetragene Datei nur dann, wenn der Befehl LoadScript ohne zusätzliche Parameter ausgeführt wird. Mit entsprechenden Parametern beim Befehlsaufruf kann gezielt eine andere Datei geladen werden.

### 2.60.1.4 TFTP-Client

In diesem Menü finden Sie die Konfiguration für den TFTP-Client.

**SNMP-ID:** 2.60.1.4

**Pfad Telnet:** /Setup/Automatisches-Laden/Netzwerk/TFTP-Client

#### 2.60.1.4.1 Bytes-pro-Hashmark

Stellen Sie hier ein, nach welcher Anzahl von erfolgreich geladenen Bytes der TFTP-Client bei der Ausführung von LoadFirmware, LoadConfig oder LoadScript ein Hash-Zeichen (#) auf der Kommandozeile ausgibt. Mit diesen Hash-Zeichen erzeugt der TFTP-Client einen Fortschrittsbalken beim Download von Firmware, Konfiguration oder Skript.

**SNMP-ID:** 2.60.1.4.1

**Pfad Telnet:** /Setup/Automatisches-Laden/Netzwerk/TFTP-Client

**Mögliche Werte:**

- 4 Zeichen

**Default:** 8192

Dieser Wert wird nur beim Laden über TFTP verwendet, nicht bei HTTP oder HTTPS. Bei HTTP oder HTTPS wird das Hash-Zeichen max. alle 100ms ausgeben, wenn ein Fortschritt stattgefunden hat.

## 2.60.56 USB

In diesem Menü finden Sie die Konfiguration für das automatische Laden von Firmware oder Konfiguration von externen Datenträgern.

**SNMP-ID:** 2.60.56

**Pfad Telnet:** /Setup/Automatisches-Laden/USB

### 2.60.56.1 Firmware-und-Loader

Mit dieser Option aktivieren Sie das automatische Laden von Loader- und/oder Firmware-Dateien von einem angeschlossenen USB-Medium. Speichern Sie die benötigten Loader- und/oder Firmware-Dateien im Verzeichnis "Firmware" in der obersten Ebene des angeschlossenen USB-Mediums.

**SNMP-ID:** 2.60.56.1

**Pfad Telnet:** /Setup/Automatisches-Laden/USB

**Mögliche Werte:**

- Inaktiv: Das automatische Laden von Loader- und/oder Firmware-Dateien für das Gerät ist deaktiviert.
- Aktiv: Das automatische Laden von Loader- und/oder Firmware-Dateien für das Gerät ist aktiviert. Beim Mounten eines USB-Mediums wird versucht, eine passende Loader- und/oder Firmware-Datei in das Gerät zu laden. Das USB-Medium wird beim Einstecken in den USB-Anschluss am Gerät oder beim Neustart gemountet.
- Wenn-unkonfiguriert: Das automatische Laden von Loader- und/oder Firmware-Dateien für das Gerät wird nur dann aktiviert, wenn sich das Gerät im Auslieferungszustand befindet. Durch einen Konfigurations-Reset kann ein Gerät jederzeit wieder auf den Auslieferungszustand zurückgesetzt werden.

**Default:**

- Wenn-unkonfiguriert

Durch den Assistenten für Sicherheitseinstellungen bzw. für Grundeinstellungen wird diese Option auf “inaktiv” gesetzt.

### 2.60.56.2 Konfiguration-und-Skript

Mit dieser Option aktivieren Sie das automatische Laden von Konfigurations- und/oder Skript-Dateien von einem angeschlossenen USB-Medium. Speichern Sie die benötigten Konfigurations- und/oder Skript-Dateien im Verzeichnis "Config" in der obersten Ebene des angeschlossenen USB-Mediums.

**SNMP-ID:** 2.60.56.2

**Pfad Telnet:** /Setup/Automatisches-Laden/USB

**Mögliche Werte:**

- Inaktiv: Das automatische Laden von Konfigurations- und/oder Skript-Dateien für das Gerät ist deaktiviert.
- Aktiv: Das automatische Laden von Konfigurations- und/oder Skript-Dateien für das Gerät ist aktiviert. Beim Mounten eines USB-Mediums wird versucht, eine passende Konfigurations- und/oder Skript-Dateien in das Gerät zu laden. Das USB-Medium wird beim Einstecken in den USB-Anschluss am Gerät oder beim Neustart gemountet.
- Wenn-unkonfiguriert: Das automatische Laden von Konfigurations- und/oder Skript-Dateien für das Gerät wird nur dann aktiviert, wenn sich das Gerät im Auslieferungszustand befindet. Durch einen Konfigurations-Reset kann ein Gerät jederzeit wieder auf den Auslieferungszustand zurückgesetzt werden.

**Default:**

- Wenn-unkonfiguriert

Durch den Assistenten für Sicherheitseinstellungen bzw. für Grundeinstellungen wird diese Option auf "inaktiv" gesetzt.

Wenn Sie verhindern wollen, dass ein Gerät durch manuellen Reset auf Werkseinstellungen und Einstecken eines USB-Datenträgers mit einer unerwünschten Konfiguration versehen werden kann, müssen Sie den Reset-Schalter deaktivieren.

# 2.63 Paket-Capture

Mit dieser Einstellung verwalten Sie die Verwendung von LCOSCAP zur Aufzeichnung des Netzwerk-Datenverkehrs.

**SNMP-ID:**

2.63

**Pfad Telnet:**

**Setup** > **Paket-Capture**

## 2.63.1 LCOSCap-In-Betrieb

Mit dieser Einstellung aktivieren Sie die LCOSCAP-Funktionalität.

**SNMP-ID:**

2.63.1

**Pfad Telnet:**

**Setup** > **Paket-Capture** > **LCOSCap-In-Betrieb**

**Mögliche Werte:**

ja

nein

**Default:**

ja

### 2.63.2 LCOSCap-Port

Mit dieser Einstellung bestimmen Sie den Port, den LCOSCAP nutzt.

**SNMP-ID:**

2.63.2

**Pfad Telnet:**

**Setup** > **Paket-Capture** > **LCOSCap-Port**

**Mögliche Werte:**

5 Zeichen aus '0123456789'

**Default:**

41047

## 2.200 SIP-ALG

Konfigurieren Sie hier die Einstellungen für den SIP-ALG.

**SNMP-ID:**

2.200

**Pfad Telnet:**

**Setup**

### 2.200.1 Operating

Diese Einstellung legt fest, ob der SIP-ALG aktiviert ist.

**SNMP-ID:**

2.200.1

**Pfad Telnet:**

**Setup** > **SIP-ALG**

**Mögliche Werte:**

ja

nein

**Default:**

nein

# 3 Firmware

In diesem Menü finden Sie die Aktionen und Einstellmöglichkeiten zur Verwaltung der Geräte-Firmware.

**Pfad Telnet:** /Firmware

## 3.7 Feature-Word

Anzeige der Feature-Bits, die Aufschluß gibt über die im Gerät freigeschalteten Optionen.

**Pfad Telnet:** /Firmware/Feature-Word

## 3.3 Modus-Firmsafe

Von den beiden im Gerät gespeicherten Firmware-Versionen kann immer nur eine aktiv sein. Beim Laden einer neuen Firmware wird die nicht aktive Firmware überschrieben. Mit dem Firmwafe-Modus können selbst entscheiden, welche Firmware nach dem Upload aktiviert werden soll.

Mögliche Werte:

- Unmittelbar: Als erste Möglichkeit können Sie die neue Firmware laden und sofort aktivieren. Folgende Situationen können dann entstehen:

  Die neue Firmware wird erfolgreich geladen und arbeitet anschließend wie gewünscht. Dann ist alles in Ordnung.

  Das Gerät ist nach dem Ladevorgang der neuen Firmware nicht mehr ansprechbar. Falls schon während des Uploads ein Fehler auftritt, aktiviert das Gerät automatisch wieder die bisherige Firmware und startet damit neu.

- Login: Um den Problemen eines fehlerhaften Uploads zu begegnen, gibt es die zweite Möglichkeit, bei der die Firmware geladen und ebenfalls sofort gestartet wird.

  Im Unterschied zur ersten Variante wartet das Gerät anschließend für den eingestellten Firmsafe-Timeout auf einen erfolgreichen Login über Telnet, ein Terminalprogramm oder WEBconfig. Nur wenn dieser Login erfolgt, wird die neue Firmware auch dauerhaft aktiviert.

  Wenn das Gerät nicht mehr ansprechbar ist oder ein Login aus anderen Gründen unmöglich ist, aktiviert es automatisch wieder die bisherige Firmware und startet damit neu.

- Manuell: Bei der dritten Möglichkeit können Sie ebenfalls selbst eine Zeit bestimmen, in der Sie die neue Firmware testen wollen. Das Gerät startet mit der neuen Firmware und wartet in der eingestellten Zeit darauf, dass die geladene Firmware von Hand aktiviert und damit dauerhaft wirksam gemacht wird. Unter LANconfig aktivieren Sie die neue Firmware mit Gerät > Firmware-Verwaltung > Im Test laufende Firmware freischalten, unter Telnet unter 'Firmware/Firmsafe-Tabelle' mit dem Befehl 'set # active' (dabei ist # die Position der Firmware in der Firmsafe-Tabelle). Unter WEBconfig finden Sie die Firmsafe-Tabelle unter Expertenkonfiguration Firmware.

Default:

- unmittelbar

Das Laden einer zweiten Firmware ist nur dann möglich, wenn das Gerät über ausreichenden Speicherplatz für zwei vollständige Firmwareversionen verfügt. Aktuelle Firmwareversionen (ggf. mit zusätzlichen Software-Optionen) können bei älteren Hardwaremodellen manchmal mehr als die Hälfte des verfügbaren Speicherplatzes benötigen. In diesem Fall wird das asymmetrische Firmsafe verwendet.

**Pfad Telnet:** /Firmware/Modus-Firmsafe

## 3.4 Timeout-Firmsafe

Die Zeit in Sekunden für den Test einer neuen Firmware.

Mögliche Werte:

- 0 bis 99999 Sekunden.

Default:

- 300 Sekunden

**Pfad Telnet:** /Firmware/Timeout-Firmsafe

## 3.1 Versions-Tabelle

In dieser Tabelle finden Sie die Informationen über die Firmware-Version und Seriennummer des Gerätes.

**Pfad Telnet:** /Firmware/Versions-Tabelle

### 3.1.1 Ifc

Das Interface, auf das sich dieser Eintrag bezieht.

**Pfad Telnet:** /Firmware/Versions-Tabelle/Ifc

### 3.1.2 Modul

Vollständige Bezeichnung des Gerätetyps.

**Pfad Telnet:** /Firmware/Versions-Tabelle/Modul

### 3.1.3 Version

Aktuell im Gerät aktive Firmware-Version mit Angabe des Release-Datums.

**Pfad Telnet:** /Firmware/Versions-Tabelle/Version

### 3.1.4 Seriennummer

Seriennummer des Gerätes.

**Pfad Telnet:** /Firmware/Versions-Tabelle/Seriennummer

## 3.2 Tabelle-Firmsafe

In dieser Tabelle finden Sie für jede der beiden im Gerät gespeicherten Firmware-Versionen die Angaben über die Position im Speicherbereich (1 oder 2), die Angabe des Zustandes (aktiv oder inaktiv), die Versionsnummer, das Datum, die Größe und den Index (fortlaufende Nummer).

**Pfad Telnet:** /Firmware/Tabelle-Firmsafe

## 3.2.1 Position

Position im Speicherbereich für den aktuellen Eintrag.

**Pfad Telnet:** /Firmware/Tabelle-Firmsafe/Position

## 3.2.2 Status

Status des aktuellen Eintrags.

Mögliche Werte:

- Inaktiv: Diese Firmware befindet sich im Wartezustand und kann aktiviert werden.
- Aktiv: Diese Firmware wird derzeit vom Gerät verwendet.
- Lader: Bei diesem Eintrag handelt es sich nicht um eine Firmware, sonder um einen Lader mit unterstützenden Funktionen.

**Pfad Telnet:** /Firmware/Tabelle-Firmsafe/Status

## 3.2.3 Version

Versionsbezeichnung der Firmware für den aktuellen Eintrag.

**Pfad Telnet:** /Firmware/Tabelle-Firmsafe/Version

## 3.2.4 Datum

Release-Datum der Firmware für den aktuellen Eintrag.

**Pfad Telnet:** /Firmware/Tabelle-Firmsafe/Datum

## 3.2.5 Groesse

Größe der Firmware für den aktuellen Eintrag.

**Pfad Telnet:** /Firmware/Tabelle-Firmsafe/Groesse

## 3.2.6 Index

Index für den aktuellen Eintrag.

**Pfad Telnet:** /Firmware/Tabelle-Firmsafe/Index

# 4 Sonstiges

In diesem Menü finden Sie zusätzliche Funktionen aus dem LCOS-Menübaum.

**Pfad Telnet:** /Sonstiges

## 4.5 Kaltstart

Mit dieser Aktion können Sie das Gerät neu booten.

**Pfad Telnet:** /Sonstiges/Kaltstart

## 4.2 System-Boot

Mit dieser Aktion können Sie manuell das Gerät neu booten.

**Pfad Telnet:** /Sonstiges/System-Boot

## 4.1 Manuelle-Wahl

In diesem Menü finden Sie die Aktionen für den manuellen Verbindungsaufbau.

**Pfad Telnet:** /Sonstiges/Manuelle-Wahl

### 4.1.2 Abbau

Mit dieser Aktion können Sie manuell die Verbindung zu einer Gegenstelle beenden.

Geben Sie als Parameter der Aktion den Namen der entsprechenden Gegenstelle an.

**Pfad Telnet:** /Sonstiges/Manuelle-Wahl/Abbau

### 4.1.1 Aufbau

Mit dieser Aktion können Sie manuell den Verbindungsaufbau zu einer Gegenstelle starten.

Geben Sie als Parameter der Aktion den Namen der entsprechenden Gegenstelle an.

**Pfad Telnet:** /Sonstiges/Manuelle-Wahl/Aufbau

### 4.1.4 Testruf

Mit dieser Aktion können Sie manuell den Verbindungsaufbau zu einer Gegenstelle testen.

Geben Sie als Parameter der Aktion den Namen der entsprechenden Gegenstelle an.

**Pfad Telnet:** /Sonstiges/Manuelle-Wahl/Testruf

# 4.6 Voice-Call-Manager

In diesem Menü finden Sie die Aktionen für den Voice-Call-Manager.

**Pfad Telnet:** /Sonstiges/Voice-Call-Manager

## 4.6.1 Line

In diesem Menü finden Sie die Aktionen für die Leitungen des Voice-Call-Managers.

**Pfad Telnet:** /Sonstiges/Voice-Call-Manager/Line

### 4.6.1.2 Register

Mit dieser Aktion können Sie gezielt eine Leitung des Voice-Call-Managers registrieren.

Geben Sie als Parameter der Aktion den Namen der entsprechenden Leitung an.

**Pfad Telnet:** /Sonstiges/Voice-Call-Manager/Line/Register

### 4.6.1.1 Unregister

Mit dieser Aktion können Sie gezielt eine Leitung des Voice-Call-Managers de-registrieren.

Geben Sie als Parameter der Aktion den Namen der entsprechenden Leitung an.

**Pfad Telnet:** /Sonstiges/Voice-Call-Manager/Line/Unregister

## 4.6.2 Groups

In diesem Menü finden Sie die Aktionen für die Gruppen des Voice-Call-Managers.

**Pfad Telnet:** /Sonstiges/Voice-Call-Manager/Groups

### 4.6.2.1 show

Mit dieser Aktion können Sie gezielt eine Gruppe des Voice-Call-Managers anzeigen.

Geben Sie als Parameter der Aktion den Namen der entsprechenden Gruppe an.

**Pfad Telnet:** /Sonstiges/Voice-Call-Manager/Groups/show

# Index


## A

Access Point
481, 500
Übertragung Nutzdaten 481
AIA (Authority Info Access) 531

## B

Bandbreitenlimit
348
Empfangsrichtung 348
Bandbreitenrichtung
348
Senderichtung 348
Bridge-Schnittstelle 501

## C

CA-Profiltabelle 530, 533
CAPWAP
500
Übertragung Multicast-Pakete 500
Certificate Authorities (CAs) 533

## D

Datenpakete
500
DSCP 500
Download 15
DSCP
499–500
Datenpakete 500
Kontrollpakete 499

## F

Firmware 15

## G

Grenzwert Sendewiederholungen SSID 344

## I

IGMP Snooping 501
Inband
15
mit Telnet 15
Interpoint-Alarm-Grenzen-Tabelle 345

## K

Kontrollpakete
499
DSCP 499

## L

LAN-Schnittstellen
346
Einstellungen 346
LCOS 15
Loopback-Adressen 502, 506

## M

Multicast-Adresse 502
Multicast-Netzwerke 500
Multicast-Port 502

## N

Netzwerk-Alarm-Grenzen
344
Einstellungen 344

## O

OCSP-Client 530, 532
OSCP-Responder 532
OSCP-Responder-Profil 533

## P

Phy-Signal 344

## R

Responder-Profiltabelle 533

## S

SSID 481, 500
Support 15
Syslog-Events 532
SYSLOG-Nachrichten
532
Zertifikatsprüfungsergebnisse 532

## T

Tx-Fehler 345
Tx-Limit 348

## V

VLAN-Id 482
VLAN-Modus 472, 481

## W

WEBconfig 22
WLAN
482
Datenaustausch Clients 482
WLAN-Controller 500
WLAN-Netzwerk
481
WLAN-Netzwerk *(Fortsetzung)*
Nutzdaten 481
WLAN-Netzwerke
471
definieren 471
WLC-Cluster 504
WLC-Daten-Tunnel
506
aktivieren 506
WLC-Discovery (Tabelle) 505
WLC Liste (Tabelle) 505

## Z

Zertifikatsprüfungsergebnisse als SYSLOG-Nachrichten 532
Zertifikatsüberprüfung
532
Ergebnisse prüfen/protokollieren 532