

LANCOM menu reference LCOS version 8.50

Revision 1 (April 2011)

© 2011 LANCOM Systems GmbH, Wuerselen (Germany). All rights reserved.

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. LANCOM Systems shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software included with this product is subject to written permission by LANCOM Systems. We reserve the right to make any alterations that arise as the result of technical development.

All explanations and documents for registration of the products you find in the appendix of this documentation, if they were present at the time of printing.

Trademarks

Windows®, Windows XP® and Microsoft® are registered trademarks of Microsoft, Corp.

The LANCOM Systems logo, LCOS and the name LANCOM are registered trademarks of LANCOM Systems GmbH. All other names mentioned may be trademarks or registered trademarks of their respective owners.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit <http://www.openssl.org/>.

This product includes cryptographic software written by Eric Young (eyay@cryptsoft.com).

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

LANCOM Systems GmbH
Sonnenweg 11
Adenauerstr. 20/B2
Germany

www.lancom.de

Würselen, April 2011

Contents

1 Introduction	28
1.1 About this documentation	28
1.2 Configuration with Telnet	29
1.3 Configuration with WEBconfig	33
2 Setup	36
2.1 Name	36
2.2 WAN	36
2.2.18 Backup delay seconds	36
2.2.10 Callback attempts	36
2.2.9 Protect	36
2.2.2 Dialup peers	36
2.2.2.1 Peer	37
2.2.2.2 Dialup remote	37
2.2.2.3 B1 DT	37
2.2.2.4 B2 DT	37
2.2.2.5 WAN layer	37
2.2.2.6 Callback	38
2.2.3 RoundRobin	38
2.2.3.1 Peer	38
2.2.3.2 Round robin	38
2.2.3.3 Head	39
2.2.4 Layer	39
2.2.4.1 WAN layer	39
2.2.4.2 Encapsulation	39
2.2.4.3 Layer 3	39
2.2.4.4 Layer 2	40
2.2.4.5 Layer 2 options	40
2.2.4.6 Layer 1	40
2.2.5 PPP	40
2.2.5.1 Peer	41
2.2.5.10 Rights	41
2.2.5.11 Authent. response	41
2.2.5.2 Authent. request	41
2.2.5.3 Password	42
2.2.5.4 Time	42
2.2.5.5 Try	42
2.2.5.6 Username	42
2.2.5.7 Conf	42
2.2.5.8 Fail	43
2.2.5.9 Term	43
2.2.6 Incoming calling numbers	43
2.2.6.1 Dialup remote	43
2.2.6.2 Peer	43
2.2.8 Scripts	44
2.2.8.1 Peer	44
2.2.8.2 Scripts	44
2.2.11 Router interface	44
2.2.11.1 Ifc	44
2.2.11.2 MSN/EAZ	44
2.2.11.3 CLIP	45
2.2.11.8 Y Connection	45
2.2.11.9 Accept calls	45
2.2.13 Manual dialing	45
2.2.13.2 Disconnect	45
2.2.13.1 Connect	46
2.2.17 Channel list	46
2.2.30.1 Peer	46
2.2.17.2 Min	46
2.2.17.3 Max	46

2.2.17.4 Head	46
2.2.19 DSL broadband peers	47
2.2.19.1 Peer	47
2.2.19.10 Service name	47
2.2.19.11 ATM-VPI	47
2.2.19.12 ATM-VCI	47
2.2.19.13 User def. MAC	48
2.2.19.14 DSL interface(s)	48
2.2.19.15 MAC type	48
2.2.19.16 VLAN-ID	48
2.2.19.2 Short holding time	48
2.2.19.3 AC name	49
2.2.19.10 Service name	49
2.2.19.5 WAN layer	49
2.2.19.9 AC name	49
2.2.20 IP list	49
2.2.20.1 Peer	50
2.2.20.2 IP address	50
2.2.20.3 IP netmask	50
2.2.20.4 Gateway	50
2.2.20.5 DNS default	50
2.2.20.6 DNS backup	50
2.2.20.7 NBNS default	51
2.2.20.8 NBNS backup	51
2.2.20.9 Masquerading IP address	51
2.2.21 PPTP peers	51
2.2.21.1 Peer	51
2.2.21.3 Port	52
2.2.21.4 SH time	52
2.2.21.5 Routing tag	52
2.2.21.6 IP address	52
2.2.22 RADIUS	52
2.2.22.1 Operating	52
2.2.22.3 Authentication port	53
2.2.22.10 Authentication protocols	53
2.2.22.6 CLIP operation	53
2.2.22.7 CLIP password	53
2.2.22.8 Loopback addr.	54
2.2.22.5 PPP operation	54
2.2.22.9 Protocol	54
2.2.22.4 Secret	55
2.2.22.2 Server address	55
2.2.23 Polling table	55
2.2.23.1 Peer	55
2.2.23.2 IP address-1	55
2.2.23.3 Time	55
2.2.23.4 Try	55
2.2.23.5 IP address-2	56
2.2.23.6 IP address-3	56
2.2.23.7 IP address-4	56
2.2.23.8 Loopback addr.	56
2.2.24 Backup peers	57
2.2.24.1 Peer	57
2.2.24.2 Alternative peers	57
2.2.24.3 Head	57
2.2.25 Action table	57
2.2.25.1 Index	57
2.2.25.2 Host name	58
2.2.25.3 Peer	58
2.2.25.4 Lock time	58
2.2.25.5 Condition	58

2.2.25.6 Action	58
2.2.25.7 Check for	59
2.2.25.8 Operating	59
2.2.25.9 Owner	60
2.2.26 MTU list	60
2.2.26.1 Peer	60
2.2.26.2 MTU	60
2.2.30 Additional PPTP gateways	60
2.2.30.1 Peer	60
2.2.30.3 Gateway-1	61
2.2.30.4 Rtg-Tag-1	61
2.2.30.5 Gateway-2	61
2.2.30.6 Rtg-Tag-2	61
2.2.30.7 Gateway-3	61
2.2.30.8 Rtg-Tag-3	62
2.2.30.9 Gateway-4	62
2.2.30.10 Rtg tag 4	62
2.2.30.11 Gateway 5	62
2.2.30.12 Rtg-Tag-5	62
2.2.30.13 Gateway 6	63
2.2.30.14 Rtg-Tag-6	63
2.2.30.15 Gateway-7	63
2.2.30.16 Rtg-Tag-7	63
2.2.30.17 Gateway-8	64
2.2.30.18 Rtg-Tag-8	64
2.2.30.19 Gateway-9	64
2.2.30.20 Rtg-Tag-9	64
2.2.30.21 Gateway-10	64
2.2.30.22 Rtg-Tag-10	65
2.2.30.23 Gateway-11	65
2.2.30.24 Rtg-Tag-11	65
2.2.30.25 Gateway-12	65
2.2.30.26 Rtg-Tag-12	65
2.2.30.27 Gateway-13	66
2.2.30.28 Rtg-Tag-13	66
2.2.30.29 Gateway-14	66
2.2.30.30 Rtg-Tag-14	66
2.2.30.31 Gateway-15	66
2.2.30.32 Rtg-Tag-15	67
2.2.30.33 Gateway-16	67
2.2.30.34 Rtg-Tag-16	67
2.2.30.35 Gateway-17	67
2.2.30.36 Rtg-Tag-17	67
2.2.30.37 Gateway-18	68
2.2.30.38 Rtg-Tag-18	68
2.2.30.39 Gateway-19	68
2.2.30.40 Rtg-Tag-19	68
2.2.30.41 Gateway-20	68
2.2.30.42 Rtg-Tag-20	69
2.2.30.43 Gateway-21	69
2.2.30.44 Rtg-Tag-21	69
2.2.30.45 Gateway-22	69
2.2.30.46 Rtg-Tag.22	69
2.2.30.47 Gateway-23	70
2.2.30.48 Rtg-Tag-23	70
2.2.30.49 Gateway-24	70
2.2.30.50 Rtg-Tag-24	70
2.2.30.51 Gateway-25	70
2.2.30.52 Rtg-Tag-25	71
2.2.30.53 Gateway-26	71
2.2.30.54 Rtg-Tag-26	71

2.2.30.55 Gateway-27	71
2.2.30.56 Rtg-Tag-27	71
2.2.30.57 Gateway-28	72
2.2.30.58 Rtg-Tag-28	72
2.2.30.59 Gateway-29	72
2.2.30.60 Rtg-Tag-29	72
2.2.30.61 Gateway-30	72
2.2.30.62 Rtg-Tag-30	73
2.2.30.63 Gateway-31	73
2.2.30.64 Rtg-Tag-31	73
2.2.30.65 Gateway-32	73
2.2.30.66 Rtg-Tag-32	73
2.2.30.2 Begin with	74
2.3 Charges	74
2.3.12 Reset budgets	74
2.3.1 Budget units	74
2.3.16 Activate additional budget	74
2.3.8 DSL broadband minutes budget	74
2.3.13 Dialup minutes budget	74
2.3.6 Total units	75
2.3.11 Additional DSL broadband budget	75
2.3.3 Spare units	75
2.3.9 Spare DSL broadband minutes	75
2.3.14 Spare dialup minutes	75
2.3.10 Router DSL broadband budget	75
2.3.4 Router units	75
2.3.15 Router ISDN serial minutes active	75
2.3.2 Days per period	75
2.3.5 Table budget	76
2.3.5.1 Ifc.	76
2.3.5.2 Budget units	76
2.3.5.3 Spare units	76
2.3.5.4 Units	76
2.3.7 Time table	76
2.3.7.1 Ifc.	76
2.3.7.2 Budget minutes	76
2.3.7.3 Spare minutes	76
2.3.7.4 Minutes active	76
2.3.7.5 Minutes passive	77
2.4 LAN	77
2.4.3 Spare heap	77
2.4.2 MAC-Address	77
2.4.9 Trace level	77
2.4.8 Trace MAC	77
2.4.10 IEEE802.1x	78
2.4.10.1 Supplicant Ifc setup	78
2.5 Bridge	78
2.5.4 Aging minutes	79
2.5.1 Operating	79
2.5.2 Peer	79
2.5.7 LAN interface	79
2.5.8 VLAN-ID	79
2.5.3 Bridge table	80
2.5.5 LAN configuration	80
2.5.5.1 Broadcast	80
2.5.5.2 Multicast	80
2.5.5.3 Destination address	81
2.5.5.4 Source address	81
2.5.6 WAN configuration	82
2.5.6.1 Broadcast	82
2.5.6.2 Multicast	82

2.5.6.3 Destination address	82
2.5.6.4 Source address	83
2.7 TCP-IP	83
2.7.1 Operating	83
2.7.11 ARP aging minutes	84
2.7.8 DNS backup	84
2.7.7 DNS default	84
2.7.22 ICMP on ARP timeout	84
2.7.10 NBNS backup	84
2.7.9 NBNS default	84
2.7.20 Non-local ARP replies	85
2.7.6 Access list	85
2.7.6.1 IP address	85
2.7.6.2 IP netmask	85
2.7.6.3 Routing tag	85
2.7.16 ARP table	85
2.7.16.1 IP address	85
2.7.16.2 MAC address	85
2.7.16.3 Last access	86
2.7.16.5 Ethernet port	86
2.7.16.6 Peer	86
2.7.16.7 VLAN-ID	86
2.7.16.8 Connect	86
2.7.17 Loopback list	86
2.7.17.1 Loopback address	86
2.7.17.2 Name	87
2.7.17.3 Routing tag	87
2.7.21 Alive test	87
2.7.21.6 Boot type	87
2.7.21.5 Fail limit	87
2.7.21.2 Test interval	87
2.7.21.4 Retry interval	87
2.7.21.3 Retry count	87
2.7.21.1 Target address	88
2.7.30 Network list	88
2.7.30.1 Network name	88
2.7.30.2 IP address	88
2.7.30.3 IP netmask	88
2.7.30.4 VLAN-ID	88
2.7.30.5 Interface	89
2.7.30.6 Source check	89
2.7.30.7 Type	90
2.7.30.8 Routing tag	90
2.7.30.9 Comment	90
2.8 IP router	90
2.8.1 Operating	90
2.8.12 End WAN pool	90
2.8.6 Send-ICMP-Redirect	91
2.8.14 Usage default timetable	91
2.8.5 Proxy-ARP	91
2.8.11 Start-WAN-Pool	91
2.8.22 WAN-Tag-Creation	91
2.8.2 IP routing table	92
2.8.2.1 IP address	92
2.8.2.2 IP netmask	92
2.8.2.3 Peer or IP	92
2.8.2.4 Distance	92
2.8.2.6 Operating	93
2.8.2.7 Comment	93
2.8.2.8 Routing tag	93
2.8.7 Routing method	93

2.8.7.2 ICMP-Routing-Method	93
2.8.7.6 Route internal services	94
2.8.7.4 L2-L3 tagging	94
2.8.7.5 L3-L2 tagging	94
2.8.7.1 Routing method	94
2.8.7.3 SYN/ACK speedup	95
2.8.8 RIP	95
2.8.8.2 R1 mask	95
2.8.8.4 WAN sites	95
2.8.8.5 LAN sites	98
2.8.8.6 Parameter	100
2.8.8.7 Filter	101
2.8.8.8 Best routes	102
2.8.8.9 All routes	102
2.8.9 1-N-NAT	102
2.8.9.7 Fragment aging seconds	102
2.8.9.6 Fragments	103
2.8.9.3 ICMP aging seconds	103
2.8.9.10 ID spoofing	103
2.8.9.8 IPSec aging seconds	103
2.8.9.1 TCP aging seconds	104
2.8.9.2 UDP aging seconds	104
2.8.9.4 Service table	104
2.8.9.5 Table- 1-N-NAT	105
2.8.9.9 IPSec table	106
2.8.10 Firewall	107
2.8.10.10 Admin e-mail	107
2.8.10.11 Operating	108
2.8.10.16 Authentication port	108
2.8.10.9 DoS action	108
2.8.10.13 IDS action	109
2.8.10.8 Max. half-open connections	109
2.8.10.14 Ping block	109
2.8.10.12 Port scan threshold	109
2.8.10.17 Deny session recover	110
2.8.10.15 Stealth mode	110
2.8.10.1 Objects	110
2.8.10.2 Rules	111
2.8.10.3 Filter list	113
2.8.10.4 Actions	115
2.8.10.5 Connection list	115
2.8.10.6 Host block list	117
2.8.10.7 Port-Block-List	117
2.8.10.19 Open port list	118
2.8.10.20 Applications	118
2.8.13 Default time list	121
2.8.13.1 Index	121
2.8.13.2 Days	121
2.8.13.3 Start	121
2.8.13.4 Stop	121
2.8.13.5 Peer	121
2.8.19 N-N-NAT	122
2.8.19.1 Index	122
2.8.19.2 Source address	122
2.8.19.3 Src-Mask	122
2.8.19.4 Destination station	122
2.8.19.5 New network address	122
2.8.20 Load balancer	123
2.8.20.1 Operating	123
2.8.20.2 Bundle peers	123
2.8.21 VRRP	124

2.8.21.1 Operating	124
2.8.21.4 Advert.-Interval	124
2.8.21.5 Internal-Services	125
2.8.21.3 Reconnect-Delay	125
2.8.21.2 VRRP-List	125
2.8.23 Tag-Table	126
2.8.23.1 Peer	126
2.8.23.2 Rtg-tag	126
2.8.23.3 Start-WAN-Pool	127
2.8.23.4 End-WAN-Pool	127
2.9 SNMP	127
2.9.3 Administrator	127
2.9.11 Comment-1	127
2.9.12 Comment-2	127
2.9.13 Comment-3	128
2.9.14 Comment-4	128
2.9.16 Comment-5	128
2.9.17 Comment-6	128
2.9.17 Comment-7	128
2.9.17 Comment-8	128
2.9.6 Delete monitor	128
2.9.10 Password required for SNMP read-access	129
2.9.15 Read-only community	129
2.9.5 Register monitor	129
2.9.4 Location	129
2.9.1 Send traps	129
2.9.20 Full host MIB	130
2.9.2 IP-Traps	130
2.9.2.1 Trap-IP	130
2.9.2.3 Loopback address	130
2.9.2.4 Version	130
2.9.7 Monitor table	131
2.9.7.1 IP address	131
2.9.7.2 Port	131
2.9.7.3 Timeout	131
2.9.7.4 MAC address	131
2.9.7.5 Peer	131
2.9.7.6 Loopback address	131
2.9.7.7 VLAN-ID	131
2.9.7.8 LAN-Ifc	132
2.9.7.9 Ethernet port	132
2.10 DHCP	132
2.10.7 Default-Lease-Time-Minutes	132
2.10.6 Max.-Lease-Time-Minutes	132
2.10.19 User class identifier	132
2.10.8 DHCP table	132
2.10.8.1 IP address	133
2.10.8.10 LAN-Ifc	133
2.10.8.2 MAC-Address	133
2.10.8.3 Timeout	133
2.10.8.4 Hostname	133
2.10.8.5 Type	133
2.10.8.7 Ethernet port	133
2.10.8.8 VLAN-ID	133
2.10.8.9 Network name	134
2.10.9 Hosts	134
2.10.9.1 MAC-Address	134
2.10.9.2 IP address	134
2.10.9.3 Hostname	134
2.10.9.4 Image alias	134
2.10.9.5 Network name	135

2.10.10 Alias list	135
2.10.10.1 Image alias	135
2.10.10.2 Image file	135
2.10.10.3 Image server	135
2.10.18 Ports	135
2.10.18.2 Port	136
2.10.18.3 Enable-DHCP	136
2.10.20 Network list	136
2.10.21.2 Network-name	136
2.10.20.10 NBNS backup	136
2.10.20.11 Operating	136
2.10.20.12 Broadcast bit	137
2.10.20.13 Master server	137
2.10.20.14 Cache	137
2.10.20.15 Adaption	138
2.10.20.16 Cluster	138
2.10.20.17 2nd master server	138
2.10.20.18 3rd master server	139
2.10.20.19 4th master server	139
2.10.20.2 Start address pool	139
2.10.20.3 End address pool	139
2.10.20.4 Netmask	139
2.10.20.5 Broadcast address	140
2.10.20.6 Gateway address	140
2.10.20.7 DNS default	140
2.10.20.8 DNS backup	140
2.10.20.9 NBNS default	140
2.10.21 Additional options	141
2.10.21.1 Option number	141
2.10.21.2 Network name	141
2.10.21.3 Option Value	141
2.10.21.4 Option-Type	141
2.11 Config	142
2.11.9 Administrator EAZ-MSN	142
2.11.41 Admin gender	142
2.11.42 Assert action	142
2.11.16 Screen height	143
2.11.5 Config aging minutes	143
2.11.60 CPU-load interval	143
2.11.40 Crash message	143
2.11.10 Display contrast	143
2.11.18 LED test	144
2.11.39 License expiry e-mail	144
2.11.7 Login errors	144
2.11.4 Maximum connections	144
2.11.33 Outband aging minutes	144
2.11.3 Password required for SNMP read access	145
2.11.17 Prompt	145
2.11.32 Reset button	145
2.11.8 Lock minutes	146
2.11.6 Language	146
2.11.25 SSH port	146
2.11.23 Telnet port	146
2.11.24 Telnet SSL port	147
2.11.13 TFTP client	147
2.11.13.5 Bytes per hashmark	147
2.11.13.1 Configuration address	147
2.11.13.2 Configuration filename	147
2.11.13.3 Firmware address	147
2.11.13.4 Firmware filename	148
2.11.13.6 Script address	148

2.11.13.7 Script filename	148
2.11.15 Access table	148
2.11.15.1 Interface	148
2.11.15.2 Telnet	148
2.11.15.3 TFTP	149
2.11.15.4 HTTP	149
2.11.15.5 SNMP	149
2.11.15.6 HTTPS	149
2.11.15.7 Telnet-SSL	150
2.11.15.8 SSH	150
2.11.20 Cron table	150
2.11.20.1 Index	150
2.11.20.10 Owner	150
2.11.20.11 Variation	151
2.11.20.2 Minute	151
2.11.20.3 Hour	151
2.11.20.4 DayOfWeek	151
2.11.20.5 Day	152
2.11.20.6 Month	152
2.11.20.7 Command	152
2.11.20.8 Base	152
2.11.20.9 Active	152
2.11.21 Admins	153
2.11.21.1 Administrator	153
2.11.21.2 Password	153
2.11.21.3 Function rights	153
2.11.21.4 Active	154
2.11.21.5 Access rights	154
2.11.26 SSH authentication methods	154
2.11.26.1 Interface	155
2.11.26.2 Methods	155
2.11.27 Predefined Admins	155
2.11.27.1 Name	155
2.11.30 Update client	155
2.11.30.1 Operating	155
2.11.30.4 Response-Timeout	156
2.11.30.7 Last firmware update	156
2.11.30.8 Last config update	156
2.11.30.2 Server name	156
2.11.30.3 Server port	157
2.11.30.5 Retry failure	157
2.11.30.6 Retry OK	157
2.11.31 Anti-Theft-Protection	157
2.11.31.3 Outgoing calling number	158
2.11.31.8 Deviation	158
2.11.31.10 Latitude	158
2.11.31.4 Checked calling number	158
2.11.31.12 Get GPS position	158
2.11.31.1 Enabled	159
2.11.31.7 ISDN interface	159
2.11.31.9 Longitude	159
2.11.31.6 Method	159
2.11.31.2 Called number	159
2.11.35 Monitor trace	160
2.11.35.1 Tracemask1	160
2.11.35.2 Tracemask2	160
2.11.43 Function keys	160
2.11.43.1 Key	160
2.11.43.2 Mapping	160
2.11.50 LL2M	161
2.11.50.1 Operating	161

2.11.50.2 Time limit	161
2.12 WLAN	161
2.12.114 Aggregate retry limit	161
2.12.38 ARP handling	161
2.12.48 Use full channel set	162
2.12.44 Allow illegal association without authentication	162
2.12.115 Omit global crypto sequence check	162
2.12.3 Spare heap	162
2.12.13 IAPP announce interval	162
2.12.14 IAPP handover timeout	163
2.12.60 IAPP-IP network	163
2.12.12 IAPP protocol	163
2.12.47 Idle timeout	163
2.12.26 Inter-SSID traffic	163
2.12.100 Card reinitialize cycle	164
2.12.36 Country	164
2.12.41 Mail address	164
2.12.46 Indoor only operation	164
2.12.108 Radar load threshold	165
2.12.101 Noise calibration cycle	165
2.12.105 Thermal recalibration cycle	165
2.12.103 Trace MAC	165
2.12.116 Trace packets	165
2.12.110 Trace level	166
2.12.27 Supervise stations	166
2.12.8 Access mode	166
2.12.7 Access list	166
2.12.7.1 MAC address	166
2.12.7.2 Name	167
2.12.7.3 Comment	167
2.12.7.4 WPA passphrase	167
2.12.7.5 Tx limit	167
2.12.7.6 Rx limit	168
2.12.7.7 VLAN-ID	168
2.12.29 RADIUS access check	168
2.12.29.7 Response lifetime	168
2.12.29.2 Authentication port	168
2.12.29.5 Backup authentication port	169
2.12.29.12 Backup loopback address	169
2.12.29.14 Backup protocol	169
2.12.29.6 Backup secret	169
2.12.29.4 Backup server IP address	169
2.12.29.11 Loopback address	170
2.12.29.8 Password source	170
2.12.29.13 Protocol	170
2.12.29.9 Recheck cycle	170
2.12.29.3 Secret	170
2.12.29.1 Server address	171
2.12.29.10 Provide server database	171
2.12.45 RADIUS accounting	171
2.12.45.2 Accounting port	171
2.12.45.9 Excluded VLAN	171
2.12.45.5 Backup authentication port	172
2.12.45.11 Backup loopback address	172
2.12.45.13 Backup protocol	172
2.12.45.6 Backup secret	172
2.12.45.4 Backup server IP address	172
2.12.45.7 Client bridge handling	173
2.12.45.8 Interim update period	173
2.12.45.10 Loopback address	173
2.12.45.14 Restart accounting	173

2.12.45.12 Protocol	174
2.12.45.3 Secret	174
2.12.45.1 Server address	174
2.12.50 Signal averaging	174
2.12.50.1 Method	174
2.12.50.2 Standard parameters	175
2.12.50.3 Filtered parameters	175
2.12.107 Radar pattern thresholds	176
2.12.107.1 Pattern pps	176
2.12.107.2 Threshold	177
2.12.109 Noise offsets	177
2.12.109.1 Band	177
2.12.109.2 Channel	177
2.12.109.3 Interface	178
2.12.109.4 Value	178
2.12.111 Noise immunity level	178
2.12.111.3 CCK weak signal detection threshold	178
2.12.111.4 Fir step level	178
2.12.111.2 OFDM weak signal detection	179
2.12.111.1 Noise immunity level	179
2.12.111.5 Spurious immunity level	179
2.13 LANCAPI	179
2.13.3 UDP port	179
2.13.1 Access list	180
2.13.1.1 IP address	180
2.13.1.2 IP netmask	180
2.13.1.3 Routing tag	180
2.13.6 Interface list	180
2.13.6.1 Ifc	180
2.13.6.2 Operating	181
2.13.6.3 EAZ MSN(s)	181
2.13.6.5 Force out MSN	181
2.13.6.6 Max connections	181
2.13.7 Priority list	181
2.13.7.1 Interface	181
2.13.7.2 Priority out	181
2.14 Time	182
2.14.2 Current time	182
2.14.5 Call attempts	182
2.14.1 Fetch method	182
2.14.11 Daylight saving time	182
2.14.13 Get time	182
2.14.3 Time call number	183
2.14.10 Timezone	183
2.14.12 DST clock changes	183
2.14.12.1 Event	184
2.14.12.2 Index	184
2.14.12.3 Day	184
2.14.12.4 Month	184
2.14.12.5 Hour	184
2.14.12.6 Minute	184
2.14.12.7 Time type	184
2.14.15 Holidays	184
2.14.15.1 Index	184
2.14.15.2 Date	185
2.14.16 Timeframe	185
2.14.16.1 Name	185
2.14.16.2 Start	185
2.14.16.3 Stop	185
2.14.16.4 Weekdays	185
2.15 LCR	186

2.15.2 Lancapi usage	186
2.15.1 Router usage	186
2.15.4 Time list	186
2.15.4.1 Index	186
2.15.4.2 Prefix	186
2.15.4.3 Days	187
2.15.4.4 Start	187
2.15.4.5 Stop	187
2.15.4.6 Number list	187
2.15.4.7 Fallback	188
2.16 NetBIOS	188
2.16.9 Update	188
2.16.1 Operating	188
2.16.11 Lease time	188
2.16.2 Scope ID	188
2.16.14 Support browsing	189
2.16.10 WAN update minutes	189
2.16.8 Watchdogs	189
2.16.4 Peers	189
2.16.4.1 Name	189
2.16.4.3 Type	190
2.16.5 Group list	190
2.16.5.1 Group/Domain	190
2.16.5.2 Type	190
2.16.5.3 IP address	190
2.16.5.4 Peer	190
2.16.5.5 Timeout	191
2.16.5.6 Flags	191
2.16.5.7 Network name	191
2.16.5.8 Routing tag	191
2.16.6 Host List	191
2.16.6.1 Name	191
2.16.6.2 Type	191
2.16.6.3 IP address	191
2.16.6.4 Peer	192
2.16.6.5 Timeout	192
2.16.6.6 Flags	192
2.16.6.7 Network name	192
2.16.6.8 Routing tag	192
2.16.7 Server list	192
2.16.7.1 Host	192
2.16.7.10 Flags	192
2.16.7.11 Network name	192
2.16.7.12 Routing tag	193
2.16.7.2 Group/Domain	193
2.16.7.4 IP address	193
2.16.7.5 OS ver.	193
2.16.7.6 SMB version	193
2.16.7.7 Server type	193
2.16.7.8 Peer	193
2.16.7.9 Timeout	193
2.16.12 Networks	193
2.16.12.1 Network name	194
2.16.12.2 Operating	194
2.16.12.3 NT domain	194
2.17 DNS	194
2.17.1 Operating	194
2.17.3 DHCP usage	194
2.17.2 Domain	195
2.17.12 Resolve domain	195
2.17.7 Lease time	195

2.17.4 NetBIOS usage	195
2.17.5 DNS list	195
2.17.5.1 Hostname	195
2.17.5.2 IP address	196
2.17.6 Filter list	196
2.17.6.1 Index	196
2.17.6.2 Domain	196
2.17.6.3 IP address	196
2.17.6.4 Netmask	196
2.17.8 Dynamic DNS list	197
2.17.8.1 Hostname	197
2.17.8.2 IP address	197
2.17.8.3 Timeout	197
2.17.9 DNS destinations	197
2.17.9.1 Domain name	197
2.17.9.2 Peer	197
2.17.10 Service location list	198
2.17.10.1 Service name	198
2.17.10.2 Hostname	198
2.17.10.3 Port	198
2.17.11 Dynamic SRV list	198
2.17.11.1 Service name	198
2.17.11.2 Hostname	199
2.17.11.3 Port	199
2.17.13 Sub domains	199
2.17.13.1 Network name	199
2.17.13.2 Sub-domain	199
2.18 Accounting	199
2.18.1 Operating	199
2.18.10 Discriminator	199
2.18.6 Delete accounting list	200
2.18.3 Sort by	200
2.18.2 Save to flashrom	200
2.18.4 Current user	200
2.18.4.1 Username	200
2.18.4.3 Peer	200
2.18.4.4 Connection type	200
2.18.4.5 Rx kbytes	200
2.18.4.6 Tx kbytes	201
2.18.4.8 Total time	201
2.18.4.9 Connection	201
2.18.5 Accounting list	201
2.18.5.1 Username	201
2.18.5.3 Peer	201
2.18.5.4 Connection type	201
2.18.5.5 Rx kbytes	201
2.18.5.6 Tx kbytes	201
2.18.5.8 Total time	202
2.18.5.9 Connection	202
2.18.8 Time snapshot	202
2.18.8.1 Index	202
2.18.8.2 Operating	202
2.18.8.3 Type	202
2.18.8.4 Day	202
2.18.8.5 DayOfWeek	203
2.18.8.6 Hour	203
2.18.8.7 Minute	203
2.18.9 Last snapshot	203
2.18.9.1 Username	203
2.18.9.3 Peer	203
2.18.9.4 Connection type	203

2.18.9.5 Rx kbytes	203
2.18.9.6 Tx kbytes	204
2.18.9.8 Total time	204
2.18.9.9 Connection	204
2.19 VPN	204
2.19.11 Aggressive mode IKE group default	204
2.19.10 Aggressive mode proposal list default	204
2.19.8 Operating	204
2.19.22 Allow remote network selection	204
2.19.25 Flexible ID comparison	205
2.19.15 Legacy dyn. VPN (LCOS5.0x) support	205
2.19.14 main mode IKE group default	205
2.19.13 Main mode proposal list default	205
2.19.24 Max concurrent connections	206
2.19.16 NAT-T operating	206
2.19.26 NAT-T port for rekeying	206
2.19.20 Quick mode PFS group default	206
2.19.19 Quick mode proposal list default	206
2.19.21 Quick mode shorthold time default	207
2.19.23 Establish SAs collectively	207
2.19.27 SSL encapsulation allowed	207
2.19.17 Simple cert. RAS operating	207
2.19.3 Isakmp	208
2.19.3.4 Timer	208
2.19.4 Proposals	209
2.19.4.9 IKE proposal lists	209
2.19.4.10 IPSEC proposal lists	210
2.19.4.11 IKE	211
2.19.4.12 IPSEC	213
2.19.5 Certificate keys	214
2.19.5.3 IKE keys	215
2.19.7 Layer	216
2.19.7.1 Name	216
2.19.7.3 PFS group	216
2.19.7.4 IKE group	216
2.19.7.5 IKE proposal list	216
2.19.7.6 IPSEC proposal list	217
2.19.7.7 IKE key	217
2.19.9 VPN peers	217
2.19.9.1 Peer	217
2.19.9.10 DPD-inactivity timeout	217
2.19.9.11 IKE configuration	218
2.19.9.12 XAUTH	218
2.19.9.13 SSL-Encaps.	218
2.19.9.15 Routing tag	219
2.19.9.2 Extranet address	219
2.19.9.4 Layer	219
2.19.9.5 Dynamic	219
2.19.9.6 Short-hold time	219
2.19.9.7 IKE exchange	220
2.19.9.8 Remote gateway	220
2.19.9.9 Rule creation	220
2.19.12 Additional gateways	220
2.19.12.1 Peer	220
2.19.12.10 Begin with	221
2.19.12.2 Remote gateway 1	221
2.19.12.11 Routing tag 1	221
2.19.12.3 Remote gateway 2	221
2.19.12.12 Routing tag 2	221
2.19.12.4 Remote gateway 3	221
2.19.12.13 Routing tag 3	222

2.19.12.5 Remote gateway 4	222
2.19.12.14 Routing tag 4	222
2.19.12.6 Remote gateway 5	222
2.19.12.15 Routing tag 5	222
2.19.12.7 Remote gateway 6	222
2.19.12.16 Routing tag 6	223
2.19.12.8 Remote gateway 7	223
2.19.12.17 Routing tag 7	223
2.19.12.9 Remote gateway 8	223
2.19.12.18 Routing tag 8	223
2.19.12.19 Remote gateway 9	223
2.19.12.27 Routing tag 9	224
2.19.12.20 Remote gateway 10	224
2.19.12.28 Routing tag 10	224
2.19.12.21 Remote gateway 11	224
2.19.12.29 Routing tag 11	224
2.19.12.22 Remote gateway 12	224
2.19.12.30 Routing tag 12	225
2.19.12.23 Remote gateway 13	225
2.19.12.31 Routing tag 13	225
2.19.12.24 Remote gateway 14	225
2.19.12.32 Routing tag 14	225
2.19.12.25 Remote gateway 15	225
2.19.12.33 Routing tag 15	226
2.19.12.26 Remote gateway 16	226
2.19.12.34 Routing tag 16	226
2.19.12.35 Gateway-17	226
2.19.12.36 Rtg-Tag-17	226
2.19.12.37 Gateway-18	226
2.19.12.38 Rtg-Tag-18	227
2.19.12.39 Gateway-19	227
2.19.12.40 Rtg-Tag-19	227
2.19.12.41 Gateway-20	227
2.19.12.42 Rtg-Tag-20	227
2.19.12.43 Gateway-21	227
2.19.12.44 Rtg-Tag-21	228
2.19.12.45 Gateway-22	228
2.19.12.46 Rtg-Tag-22	228
2.19.12.47 Gateway-23	228
2.19.12.48 Rtg-Tag-23	228
2.19.12.49 Gateway-24	228
2.19.12.50 Rtg-Tag-24	229
2.19.12.51 Gateway-25	229
2.19.12.52 Rtg-Tag-25	229
2.19.12.53 Gateway-26	229
2.19.12.54 Rtg-Tag-26	229
2.19.12.55 Gateway-27	229
2.19.12.56 Rtg-Tag-27	230
2.19.12.57 Gateway-28	230
2.19.12.58 Rtg-Tag-28	230
2.19.12.59 Gateway-29	230
2.19.12.60 Routing tag 29	230
2.19.12.61 Gateway-30	230
2.19.12.62 Rtg-Tag-30	231
2.19.12.63 Gateway-31	231
2.19.12.64 Rtg-Tag-31	231
2.19.12.65 Gateway-32	231
2.19.12.66 Rtg-Tag-32	231
2.20 LAN bridge	231
2.20.12 Aging time	231
2.20.2 Bridge priority	232

2.20.7 Forward delay	232
2.20.6 Hello time:	232
2.20.8 Isolated mode	232
2.20.5 Maximum age	233
2.20.1 Protocol version	233
2.20.4 Encapsulation table	233
2.20.4.1 Protocol	233
2.20.4.2 Encapsulation	233
2.20.10 Protocol table	233
2.20.10.1 Name	233
2.20.10.10 IP network	234
2.20.10.11 IP netmask	234
2.20.10.12 DHCP source MAC	234
2.20.10.2 Protocol	234
2.20.10.3 Sub-protocol	235
2.20.10.4 Port	235
2.20.10.5 Port end	235
2.20.10.6 Interface list	236
2.20.10.7 Action	236
2.20.10.8 Redirect IP address	236
2.20.10.9 Destination MAC address	236
2.20.11 Port	237
2.20.11.2 Port	237
2.20.11.3 Active	237
2.20.11.5 Bridge group	237
2.20.11.6 DHCP limit	237
2.20.11.7 Point-to-point port	238
2.20.13 Priority mapping	238
2.20.13.1 Name	238
2.20.13.2 DSCP value	238
2.20.13.3 Priority	238
2.20.20 Spanning tree	239
2.20.20.1 Operating	239
2.20.20.2 Bridge priority	239
2.20.20.7 Forward delay	239
2.20.20.6 Hello time	240
2.20.20.5 Maximum age	240
2.20.20.14 Path cost computation	240
2.20.20.12 Protocol version	240
2.20.20.13 Transmit hold count	240
2.20.20.11 Port	241
2.20.30 IGMP snooping	241
2.20.30.6 Query response interval	241
2.20.30.5 Query interval	242
2.20.30.1 Operating	242
2.20.30.7 Robustness	242
2.20.30.3 Unregistered data packet handling	243
2.20.30.9 Advertise interval	243
2.20.30.2 Port settings	243
2.20.30.4 Simulated queriers	244
2.20.30.8 Static members	245
2.21 HTTP	246
2.21.2 Page headers	246
2.21.1 Document root	246
2.21.6 Error-page style	247
2.21.15 HTTP compression	247
2.21.9 Maximum tunnel connections	247
2.21.7 Port	247
2.21.3 Font family	247
2.21.5 Page headers	248
2.21.11 Session timeout	248

2.21.8 SSL port	248
2.21.13 Standard design	248
2.21.10 Tunnel idle timeout	248
2.21.14 Show device information	248
2.21.14.1 Device information	248
2.21.14.2 Position	249
2.21.16 Keep server ports open	249
2.21.16.1 Interface	249
2.21.16.2 Keep server ports open	249
2.21.20 Rollout Wizard	250
2.21.20.6 Renumber actions	250
2.21.20.1 Operating	250
2.21.20.2 Title	250
2.21.20.5 Renumber variables	250
2.21.20.7 Display connection status	251
2.21.20.8 Use extra checks	251
2.21.20.3 Variables	251
2.21.20.4 Actions	252
2.21.30 File server	253
2.21.30.2 Operating	253
2.21.30.1 Public subdirectory	253
2.22 SYSLOG	254
2.22.1 Operating	254
2.22.5 Messages table order	254
2.22.4 Port	254
2.22.2 SYSLOG table	254
2.22.2.1 Index	254
2.22.2.2 IP address	254
2.22.2.3 Source	255
2.22.2.4 Level	255
2.22.2.6 Loopback address	255
2.22.3 Facility mapper	255
2.22.3.1 Source	255
2.22.3.2 Facility	256
2.23 Interfaces	256
2.23.19 PCM-SYNC-SOURCE	256
2.23.18 Permanent L1 activation	256
2.23.1 S0	257
2.23.1.1 Interface	257
2.23.1.13 Max in calls	257
2.23.1.13 Max out calls	257
2.23.1.2 Protocol	257
2.23.1.7 LL-B channel	258
2.23.1.9 Dial prefix	258
2.23.4 DSL	258
2.23.4.1 Interface	258
2.23.4.16 Upstream rate	258
2.23.4.17 External overhead	259
2.23.4.18 Downstream rate	259
2.23.4.2 Operating	259
2.23.4.23 LAN-Ifc	259
2.23.4.6 Mode	260
2.23.6 ADSL interface	260
2.23.6.1 Interface	260
2.23.6.2 Protocol	260
2.23.6.25 Power management	261
2.23.6.26 Linecode	261
2.23.7 Modem mobile	262
2.23.7.1 Interface	262
2.23.7.2 Operating	262
2.23.7.21 Data rate	262

2.23.7.22 Profile	262
2.23.8 VDSL	263
2.23.8.1 Interface	263
2.23.8.2 Protocol	263
2.23.20 WLAN	263
2.23.20.1 Network	263
2.23.20.2 Transmission	265
2.23.20.3 Encryption	270
2.23.20.4 Group encryption keys	273
2.23.20.5 Interpoint settings	275
2.23.20.6 Client modes	276
2.23.20.7 Operational settings	278
2.23.20.8 Radio settings	280
2.23.20.9 Performance	284
2.23.20.10 Beaconsing	285
2.23.20.11 Roaming	286
2.23.20.12 Interpoint peers	288
2.23.20.13 Network alarm limits	289
2.23.20.14 Interpoint alarm limits	290
2.23.21 LAN interfaces	291
2.23.21.1 Interface	291
2.23.21.2 Connector	291
2.23.21.3 MDI mode	291
2.23.21.5 Clock role	292
2.23.21.7 Active	292
2.23.21.8 Tx limit	292
2.23.21.9 Rx limit	293
2.23.30 Ethernet ports	293
2.23.30.1 Port	293
2.23.30.2 Connector	293
2.23.30.3 Private mode	293
2.23.30.4 Assignment	293
2.23.30.5 MDI mode	294
2.23.30.6 Clock role	294
2.23.40 Modem	294
2.23.40.5 Dial command	294
2.23.40.14 AT poll count	295
2.23.40.2 Echo-off command	295
2.23.40.9 Escape sequence	295
2.23.40.11 Init. dial	295
2.23.40.11 Init. answer	295
2.23.40.4 Initialization command	295
2.23.40.6 Request ID	296
2.23.40.3 Reset	296
2.23.40.1 Ring count	296
2.23.40.7 Answer command	296
2.23.40.8 Disconnect command	296
2.23.40.10 Escape prompt delay (ms)	296
2.23.40.13 Cycletime AT poll (s)	297
2.23.41 Mobile telephony	297
2.23.41.4 Connect monitoring	297
2.23.41.8 Enable HSUPA	297
2.23.41.2 Scan networks	297
2.23.41.6 History interval (sec)	298
2.23.41.3 Input PUK	298
2.23.41.11 Check while connected	298
2.23.41.10 Threshold 3G-to-2G (dB)	298
2.23.41.9 Signal check interval (min)	298
2.23.41.7 Syslog enabled	299
2.23.41.5 Tries	299
2.23.41.1 Profiles	299

2.23.50 Analog	301
2.23.50.8 Lifeline	301
2.23.50.1 Operating	301
2.24 Public Spot module	301
2.24.19 Add user wizard	301
2.24.19.5 Default runtime	302
2.24.19.6 Comment fields	302
2.24.19.2 Username pattern	302
2.24.19.8 Print comments on voucher	303
2.24.19.9 Maximal voucher validity period	303
2.24.19.3 Password length	303
2.24.19.4 SSID	303
2.24.19.7 Default starting time	303
2.24.19.10 Available expiry methods	304
2.24.3 Provider table	304
2.24.3.1 Name	304
2.24.3.2 Auth. server address	304
2.24.3.3 Auth. server port	305
2.24.3.4 Auth. server secret	305
2.24.3.9 Auth. server loopback addr.	305
2.24.3.11 Auth. server protocol	305
2.24.3.5 Acc. server address	305
2.24.3.6 Acc. server port	306
2.24.3.7 Acc. server secret	306
2.24.3.10 Acc. server loopback addr.	306
2.24.3.12 Acc. server protocol	306
2.24.3.8 Backup	306
2.24.2 User table	307
2.24.2.1 Name	307
2.24.2.2 Password	307
2.24.2.3 MAC address	307
2.24.2.4 Comment	307
2.24.2.5 Provider	307
2.24.2.6 Expiry	307
2.24.31 Free networks	308
2.24.31.1 Host name	308
2.24.31.2 Mask	308
2.24.15 Port table	308
2.24.15.2 Port	308
2.24.15.3 Authentication necessary	308
2.24.8 Page table	309
2.24.8.1 Page	309
2.24.8.2 URL	309
2.24.8.3 Fallback	309
2.24.8.4 Type	309
2.24.8.5 Loopback address	309
2.24.20 VLAN table	310
2.24.20.1 VLAN-ID	310
2.24.7 Accounting cycle	310
2.24.1 Authentication mode	310
2.24.16 Auto-cleanup user table	310
2.24.30 Free server	311
2.24.22 Device hostname	311
2.24.14 Idle timeout	311
2.24.12 Communication port	311
2.24.21 Login page type	311
2.24.9 Roaming secret	312
2.24.17 Provide server database	312
2.24.6 Server subdir	312
2.24.5 Traffic limit bytes	312
2.24.18 Disallow multiple logins	312

2.25 RADIUS	313
2.25.4 Authentication timeout	313
2.25.5 Authentication retry	313
2.25.9 Backup query strategy	313
2.25.10 Server	313
2.25.10.12 Accounting interim interval	313
2.25.10.11 Accounting port	314
2.25.10.1 Authentication port	314
2.25.10.14 Auto-cleanup user table	314
2.25.10.5 Default realm	314
2.25.10.6 Empty realm	314
2.25.10.13 RADSEC port	315
2.25.10.2 Clients	315
2.25.10.3 Forward servers	315
2.25.10.7 Users	317
2.25.10.10 EAP	321
2.26 NTP	323
2.26.2 Operating	323
2.26.4 BC interval	323
2.26.3 BC mode	323
2.26.7 RQ interval	324
2.26.12 RQ tries	324
2.26.11 RQ address	324
2.26.11.1 RQ address	324
2.26.11.2 Loopback address	324
2.27 Mail	325
2.27.5 User name	325
2.27.7 E-mail sender	325
2.27.11 Loopback address	325
2.27.6 Password	325
2.27.4 POP3 port	326
2.27.3 POP3 server	326
2.27.10 Buffers	326
2.27.8 Send again (min)	326
2.27.2 SMTP port	326
2.27.1 SMTP server	326
2.27.9 Hold time (hrs)	327
2.30 IEEE802.1x	327
2.30.3 Radius server	327
2.30.3.1 Name	327
2.30.3.2 IP address	327
2.30.3.3 Port	328
2.30.3.4 Secret	328
2.30.3.5 Backup	328
2.30.3.6 Loopback address	328
2.30.3.7 Protocol	328
2.30.4 Ports	329
2.30.4.10 Re-authentication	329
2.30.4.11 Re-authorization interval	329
2.30.4.12 Key transmission	329
2.30.4.13 Key transmission interval	329
2.30.4.2 Port	329
2.30.4.4 Re-authentication, max.	330
2.30.4.5 Max-Req	330
2.30.4.6 Tx period	330
2.30.4.7 Supp-Timeout	330
2.30.4.8 Server-Timeout	330
2.30.4.9 Quiet period	331
2.31 PPPoE	331
2.31.1 Operating	331
2.31.3 Service	331

2.31.4 Session-Limit	331
2.31.2 Name list	332
2.31.2.1 Peer	332
2.31.2.2 Short-hold time	332
2.31.2.3 MAC address	332
2.31.5 Ports	332
2.31.5.2 Port	332
2.31.5.3 Enable PPPoE	332
2.32 VLAN	333
2.32.4 Operating	333
2.32.5 Tag value	333
2.32.1 Networks	333
2.32.1.1 Name	333
2.32.1.2 VLAN-ID	333
2.32.1.4 Ports	334
2.32.2 Port table	334
2.32.2.1 Port	334
2.32.2.4 Allow all VLANs	334
2.32.2.5 Port VLAN ID	334
2.32.2.6 Tagging mode	335
2.33 Voice Call Manager	335
2.33.1 Operating	335
2.33.2 General	335
2.33.2.10 Analog gateway codecs	335
2.33.2.11 ClnPartyNumType	336
2.33.2.13 Convert canonicals	336
2.33.2.9 Country	336
2.33.2.1 Domain	336
2.33.2.4 Echo_Canceler	337
2.33.2.6 Incoming packet reduction	337
2.33.2.8 ISDN gateway codecs	337
2.33.2.3 Local authentication	337
2.33.2.5 Outgoing packet reduction	337
2.33.2.2 Overlap timeout	338
2.33.2.7 Reduced packet size	338
2.33.2.12 Register time	338
2.33.2.16 RTP-DSCP	338
2.33.2.15 SIP-DSCP	339
2.33.2.14 Symmetric RTP	339
2.33.3 Users	339
2.33.3.1 SIP-User	339
2.33.3.2 ISDN user	341
2.33.3.3 Analog user	345
2.33.3.4 Extensions	348
2.33.4 Lines	350
2.33.4.1 SIP provider	350
2.33.4.2 SIP-PBX	358
2.33.4.3 ISDN	362
2.33.4.4 Predefined destination	364
2.33.4.5 Source filters	364
2.33.4.6 Analog	365
2.33.5 Call router	367
2.33.5.1 Call routing	367
2.33.7 Groups	371
2.33.7.1 Groups	371
2.33.8 Logging	373
2.33.8.1 Call data records	373
2.34 Printer	374
2.34.1 Printer	374
2.34.1.1 Printer	374
2.34.1.2 RawIP port	374

2.34.1.3 LPD port	374
2.34.1.4 Operating	374
2.34.1.5 Bidirectional	374
2.34.1.6 Reset on open	375
2.34.2 Access list	375
2.34.2.1 IP address	375
2.34.2.2 IP netmask	375
2.34.2.3 Routing tag	375
2.35 ECHO server	376
2.35.1 Operating	376
2.35.3 TCP timeout	376
2.35.2 Access table	376
2.35.2.1 IP address	376
2.35.2.2 Netmask	376
2.35.2.3 Protocol	376
2.35.2.4 Operating	377
2.35.2.5 Comment	377
2.36 Performance monitoring	377
2.36.2 RttMonAdmin	377
2.36.2.1 Index	377
2.36.2.4 Type	377
2.36.2.6 Frequency	377
2.36.2.7 Timeout	377
2.36.2.9 Status	378
2.36.3 RttMonEchoAdmin	378
2.36.3.1 Protocol	378
2.36.3.17 Interval	378
2.36.3.18 Packet count	378
2.36.3.2 Destination address	378
2.36.3.255 Index	378
2.36.3.3 Packet size	379
2.36.3.5 Destination port	379
2.36.4 RttMonStatistics	379
2.36.4.10 Jitter-Min-Pos-SD	379
2.36.4.11 Jitter-Max-Pos-SD	379
2.36.4.12 Jitter-Count-Pos-SD	379
2.36.4.13 Jitter-Sum-Pos-SD	379
2.36.4.16 Jitter-Min-Pos-DS	379
2.36.4.17 Jitter-Max-Pos-DS	379
2.36.4.18 Jitter-Count-Pos-DS	379
2.36.4.19 Jitter-Sum-Pos-DS	380
2.36.4.2 Completions	380
2.36.4.22 Jitter-Min-Neg-SD	380
2.36.4.23 Jitter-Max-Neg-SD	380
2.36.4.24 Jitter-Count-Neg-SD	380
2.36.4.25 Jitter-Sum-Neg-SD	380
2.36.4.255 Index	380
2.36.4.28 Jitter-Min-Neg-DS	380
2.36.4.29 Jitter-Max-Neg-DS	380
2.36.4.30 Jitter-Count-Neg-DS	381
2.36.4.31 Jitter-Sum-Neg-DS	381
2.36.4.34 Packet-Loss-SD	381
2.36.4.35 Packet-Loss-DS	381
2.36.4.4 RTT-Count	381
2.36.4.5 RTT-Sum	381
2.36.4.62 Average-Jitter	381
2.36.4.63 Average-Jitter-SD	381
2.36.4.64 Average-Jitter-DS	381
2.36.4.8 RTT-Min	381
2.36.4.9 RTT-Max	382
2.37 WLAN management	382

2.37.6 Autoaccept AP	382
2.37.7 Accept AP	382
2.37.9 Disconnect AP	382
2.37.5 CAPWAP port	383
2.37.8 Provide default configuration	383
2.37.31 Interval for status table cleanup	383
2.37.33 License limit	383
2.37.32 License count	383
2.37.19 Start automatic radio field optimization	383
2.37.30 Synch. WTP password	384
2.37.1 AP configuration	384
2.37.1.7 Control connection encryption default	384
2.37.1.8 Country default	384
2.37.1.5 WLAN module 1 default	386
2.37.1.6 WLAN module 2 default	386
2.37.1.1 Network profiles	387
2.37.1.10 Predef. intranets	395
2.37.1.2 Radio profiles	396
2.37.1.3 Common profiles	402
2.37.1.4 Access points	403
2.37.1.9 MAC address	408
2.37.1.12 DSCP for control packets	409
2.37.1.13 DSCP for data packets	409
2.37.1.14 Multicast networks	410
2.37.10 Notification	411
2.37.10.1 E-mail	411
2.37.10.3 E-mail receiver	411
2.37.10.5 Send SNMP trap for station table event	412
2.37.10.2 Syslog	412
2.37.10.4 Advanced	412
2.37.34 WLC cluster	413
2.37.34.4 WLC discovery	413
2.37.34.3 Static WLC list	413
2.37.34.2 WLC data tunnel active	414
2.37.27 Central firmware management	414
2.37.27.15 Firmware version management	414
2.37.27.16 Script management	415
2.37.27.11 Firmware repository URL	415
2.37.27.25 Firmware loopback address	416
2.37.27.14 Maximum number of loaded firmwares	416
2.37.27.12 Script repository URL	416
2.37.27.26 Script loopback address	416
2.37.27.13 Update firmware and script information	417
2.37.27.18 Reboot updated APs	417
2.37.17 RADIUS server	417
2.37.17.1 Type	417
2.37.17.2 IP address	417
2.37.17.3 Port	418
2.37.17.4 Secret	418
2.37.20 Access list	418
2.37.20.1 MAC address	418
2.37.20.2 Name	418
2.37.20.3 Comment	419
2.37.20.4 WPA passphrase	419
2.37.20.5 Tx limit	419
2.37.20.6 Rx limit	419
2.37.20.7 VLAN-ID	420
2.39 Certificates	420
2.39.1 SCEP client	420
2.39.1.1 Operating	420
2.39.1.9 Update	420

2.39.1.12 Check pending requests interval	420
2.39.1.10 Clear SCEP file system	420
2.39.1.3 CA certificate-update before expiration	421
2.39.1.8 Reinitialization	421
2.39.1.2 CA certificate-update before expiration	421
2.39.1.13 Trace level	421
2.39.1.11 Retry after error interval	421
2.39.1.7 Certificates	422
2.39.1.14 CAs	423
2.39.2 SCEP-CA	426
2.39.2.1 SCEP operating	426
2.39.2.7 Fingerprint algorithm	426
2.39.2.4 RA auto-approve	426
2.39.2.9 Reinitialize	426
2.39.2.6 Signature algorithm	426
2.39.2.3 Encryption algorithm	427
2.39.2.2 CA certificates	427
2.39.2.5 Client certificates	429
2.39.2.8 Certificate revocation lists	430
2.39.2.10 Notification	431
2.39.3 CRLs	431
2.39.3.1 Operating	431
2.39.3.5 Prefetch period	432
2.39.3.7 Refresh CRL now	432
2.39.3.6 Validity exceedance	432
2.39.3.4 Update before expiry	432
2.39.3.9 Loopback address	433
2.39.3.8 Alternative URL table	433
2.39.6 OCSP client	433
2.39.6.1 CA profile table	433
2.39.6.2 Responder profile table	435
2.40 GPS	435
2.40.1 Operating	435
2.41 UTM	436
2.41.2 Content filter	436
2.41.2.1 Operating	436
2.41.2.2 Global settings	436
2.41.2.3 Profiles	445
2.42 ADSL	461
2.42.1 Trace mode	461
2.42.4 Monitoring time (h)	461
2.42.3 Line failures	461
2.52 COM ports	462
2.52.1 Devices	462
2.52.1.1 Device type	462
2.52.1.4 Service	462
2.52.2 COM-port server	462
2.52.2.1 Operational	462
2.52.2.2 COM-port settings	463
2.52.2.3 Network settings	465
2.52.3 WAN	468
2.52.3.1 Devices	468
2.53 Temperature monitor	468
2.53.1 Upper-limit degrees	468
2.53.2 Lower-limit degrees	469
2.54 TACACS	469
2.54.3 Accounting	469
2.54.1 Authentication	469
2.54.2 Authorization	469
2.54.10 Fallback to local users	469
2.54.6 Shared secret	470

2.54.12 SNMP-GET requests accounting	470
2.54.11 SNMP-GET requests authorization	470
2.54.13 Bypass-Tacacs-for-CRON/Scripts/Action-table	471
2.54.7 Encryption	471
2.54.14 Include value into authorization request	471
2.54.9 Server	471
2.54.9.1 Server address	472
2.54.9.2 Loopback address	472
2.54.9.3 Compatibility mode	472
2.56 Autoload	472
2.56.1 Firmware and loader	472
2.56.2 Configuration and script	473
2.59 WLAN management	473
2.59.120 Log entries	473
2.59.1 Static WLC configuration	473
2.59.1.1 IP address	473
2.59.1.2 Port	474
2.59.1.3 Loopback address	474
2.60 Autoload	474
2.60.1 Network	474
2.60.1.1 Firmware	475
2.60.1.2 Configuration	476
2.60.1.3 Script	476
2.60.1.4 TFTP client	477
2.60.56 USB	477
2.60.56.1 Firmware and loader	477
2.60.56.2 Configuration and script	477
3 Firmware	480
3.7 Feature word	480
3.3 Firmsafe mode	480
3.4 Firmsafe timeout	480
3.1 Version table	481
3.1.1 Interface	481
3.1.2 Module	481
3.1.3 Version	481
3.1.4 Serial number	481
3.2 Table Firmsafe	481
3.2.1 Position	481
3.2.2 Status	481
3.2.3 Version	481
3.2.4 Date	481
3.2.5 Size	482
3.2.6 Index	482
4 Other	484
4.5 Cold boot	484
4.2 System boot	484
4.1 Manual dialing	484
4.1.2 Disconnect	484
4.1.1 Connect	484
4.1.4 Test call	484
4.6 Voice Call Manager	484
4.6.1 Lines	484
4.6.1.2 Register	484
4.6.1.1 Unregister	485
4.6.2 Groups	485
4.6.2.1 Show	485

1 Introduction

1.1 About this documentation

Components of the documentation

The documentation of your device consists of the following parts:

■ Installation Guide

The Quickstart user guide answers the following questions:

- Which software has to be installed to carry out a configuration?
- How is the device connected up?
- How can the device be contacted with LANconfig, WEBconfig or via the serial interface?
- How do I start the Setup Wizard (e.g. to set up Internet access)?
- How do I reset the device?
- Where can I find information and support?

■ User manual and Quick Reference Guide

It contains all information you need to put your device into operation. It also contains all of the important technical specifications.

■ Manual on PBX functions (only for models with VoIP support)

The PBX Functions manual gives you detailed step-by-step instructions on commissioning a LANCOM VoIP Router as a PBX (private branch exchange) for a single location. Also described are the main operating instructions for users, and how to connect terminal equipment.

■ Reference manual

It goes into detail on topics that apply to a variety of models.

The descriptions in the Reference Manual are based predominantly to the configuration with LANconfig. Also given for each LANconfig dialog is the corresponding path to find the parameters when working with WEBconfig, for example:

LANconfig: Wireless LAN ► 802.11i/WEP ► WPA or Private WEP settings

WEBconfig: LCOS Menu Tree ► Setup ► Interfaces ► WLAN ► Encryption

The paths for configuration via CLI/Telnet can be derived from this and are therefore not listed explicitly listed. The Telnet path to the encryption setting is, for example:

```
cd /Setup/Interfaces/WLAN/Encryption
```

■ Menu Reference Guide

The Menu Reference Guide comprehensively describes all of the parameters in LCOS, the operating system used by LANCOM devices. This guide is an aid to users during the configuration of devices by means of WEBconfig or the telnet console.

The parameters are listed in the alphabetical order of the paths as they appear when carrying out a configuration with WEBconfig. Each parameter is described briefly and the possible values for input are listed, as are the default values.



All documents for your product which are not shipped in printed form are available as an Acrobat document (PDF file) from www.lancom.eu/download or on the data medium supplied.

LCOS , the operating system of the LANCOM devices

All Router, Gateways, Controller and Access Points of LANCOM Systems use the same operating system, LCOS. A proprietary development of LANCOM Systems, this operating system is highly resistant to external attack and provides a high level of security. The consistent use of LCOS also ensures that operating LANCOM products is easy and uniform between products. The extensive feature set with all LANCOM products is immediately available. Free, regular software updates are constantly under development.

This manual works with the following definitions of software, hardware and manufacturer:

- LCOS describes the hardware-independent operating system
- LANCOM is the general term for all LANCOM routers and LANCOM Router access points
- LANCOM Systems is shorthand for the manufacturer, LANCOM Systems GmbH

Applicability

This Menu Reference Guide applies to all LANCOM routers and LANCOM Router access points equipped with firmware version 8.50 or later.

The functions and settings described in this Menu Reference Guide are not all supported by all models or all firmware versions.

This documentation was created by...

...several members of our staff from a variety of departments in order to ensure you the best possible support when using your LANCOM product.

If you should find any mistakes, have a criticism, or wish to suggest any improvements, please do not hesitate to send an e-mail directly to:

info@lancom.de



If you have any questions on the content in this manual, or if you require any further support, our Internet server www.lancom.de is available to you around the clock. The area 'Support' will help you with many answers to frequently asked questions (FAQs). Furthermore, the KnowledgeBase offers you a large reserve of information. The latest drivers, firmware, utilities and documentation are constantly available for download.

You can also refer to the LANCOM Support department. For telephone numbers and contact addresses of LANCOM Support, please see the enclosed leaflet or the LANCOM Systems web site.

1.2 Configuration with Telnet

Open Telnet session

To commence the configuration, start Telnet from the Windows command line with command:

```
C:\>telnet 10.0.0.1
```

Telnet establishes a connection to the device with the IP address entered.

After entering the password (assuming one has been set to protect the configuration) all of the configuration commands are available to you.



Linux and Unix additionally support Telnet sessions via SSL-encrypted connections.

Depending on the distribution it may be necessary to replace the standard Telnet application with an SSL-capable version. Start the encrypted Telnet connection with the following command:

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

Changing the console language

Terminal mode is available in English or German. LANCOM devices are set with English as the standard console language. . If necessary, change the console language with the following commands:

WEBconfig: LCOS menu tree ► Setup ► Config-Module ► Language

Close the Telnet session

To close the Telnet session, enter the command `exit` at the command prompt:

```
C:\>exit
```

Structure of the command-line interface

The LANCOM command-line interface is always structured as follows:

```

Telnet 192.168.2.23
#
Connection No.: 002 <LAN>
root@:/
> dir
Status  MENU:
Setup   MENU:
Firmware MENU:
Other   MENU:
root@:/
> -

```

- **Status**
Contains the status and statistics of all internal modules in the device
- **Setup**
Contains all adjustable parameters of all internal modules in the device
- **Firmware**
Contains the firmware management
- **Other**
Contains actions for establishing and terminating connections, reset, reboot and upload.

Command-line commands

The LANCOM command-line interface can be operated with the following DOS- or UNIX-style commands. The LCOS menu commands that are available to you can be displayed at any time by entering HELP at the command line.



Supervisor rights are necessary to execute some commands.

Command	Description
beginscript	Resets the console session to script mode. In this state, commands entered are not transferred directly to the LANCOM's configuration RAM but initially to the device's script memory.
cd [PATH]	Switch to the current directory. Various abbreviations can be used, such as replacing " cd ../.." with "cd ..", etc.
del [PATH]*	Deletes the table in the branch of the menu tree defined with Path.
default [-r] [PATH]	Resets individual parameters, tables or entire menu trees back to their default configuration. If PATH indicates a branch of the menu tree, then the option -r (recursive) must be entered.
dir [PATH] list [PATH] ls [PATH] ll [PATH]	Displays the current directory content. The suffix parameter "-a" lists the SNMP IDs associated with the content of the query. This starts the output of the SNMP ID from the device, followed by the SNMP ID of the current menu. Before each entry you will see the SNMP IDs of the sub-points.
do [PATH] [<Parameter>]	Executes the action [PATH] in the current directory. Other parameters can be entered in addition.
echo <ARG>...	Display argument on console
exit/quit/x	Ends the command line session
feature <code>	Activation of a software feature with the feature code as entered
flash Yes/No	Changes to the configuration using commands in the command line are written directly to the boot-resistant Flash memory of the devices as standard (flash yes). If updating the configuration is suppressed in Flash (flash no), changes are only stored in RAM (deleted on booting).
history	Displays a list of recently executed commands. Command "!#," can be used to directly call the list commands using their number (#): For example, "!3," runs the third list command.
killscript	Deletes the script session contents yet to be processed. The script session is selected by its name.
loadconfig	Load configuration into device via TFTP client
loadfirmware	Load firmware into device via TFTP client
loadscript	Load script into device via TFTP client

Command	Description
passwd	Change password
passwd -n new [old]	Change password (no prompt)
ping [IP address or name]	Sends an ICMP echo request to the IP address specified
readconfig	Display of the entire configuration in the device syntax
readmib	Display of the SNMP Management Information Base
readscript [-n] [-d] [-c] [-m] [PATH]	In a console session, the readscript command generates a text dump of all commands and parameters required to configure the LANCOM in its current state.
repeat <INTERVAL> <Command>	Repeats the command every INTERVAL seconds until the process is ended with new input
sleep [-u] value[suffix]	Delays the processing of configuration commands by a particular time or terminates them at a particular time. Permissible suffixes are s, m and h for seconds, minutes and hours. If no suffix is defined, the command uses milliseconds. With option switch -u, the sleep command accepts times in format MM/DD/YYYY hh:mm:ss (English) or in format TT.MM.JJJJ hh:mm:ss (German). Times will only be accepted if the system time has been set.
stop	Ends the PING command
set [PATH] <value(s)>	Sets a configuration parameter to a particular value. If the configuration parameter is a table value, a value must be specified for each column. Entering the * character leaves any existing table entry unchanged.
set [PATH] ?	Listing of the possible input values for a configuration parameter. If no name is specified, the possible input values for all configuration parameters in the current directory are specified.
setenv <NAME> <VALUE>	Set environment variable
unsetenv <NAME>	Delete environment variable
getenv <NAME>	Display environment variable (no line feed)
printenv	Display the entire environment
show <Options>	Display of special internal data. show ? displays all available information, such as most recent boot processes (Äbootlog,Ä), fire-wall filter rules (Äfilter,Ä), VPN rules (ÄVPN,Ä) and memory usage (Ämem,Ä and Äheap,Ä)
sysinfo	Display of system information (e.g. hardware/software version)
testmail	Sends an e-mail. See 'testmail ?' for parameters
time	Set time (DD.MM.YYYY hh:mm:ss)
trace	Configuration of the diagnostics display.
who	List active sessions
writeconfig	Load a new configuration file in the device syntax. All subsequent lines are interpreted as configuration values until two blank lines occur
writelflash	Load a new firmware file (only via TFTP)
!!	Repeat last command
!<num>	Repeat command <num> times
!<prefix>	Repeat last command beginning with <prefix>
#<blank>	Comment

■ PATH:

- Path name for a menu or parameter, separated by / or \
- .. means one level higher
- . means the current level

■ VALUE:

- Possible input value
- "" is a blank input value

■ NAME:

- Sequence of characters (made up of _ 0..9 A..Z)
- First character cannot be a digit
- Case insensitive

- All commands and directory/parameter names can be entered using their short-forms as long as they are unambiguous. For example, command Äsysinfo,Ä can be shortened to Äsys,Ä and Äcd

Management, to , ma. Input , /s, is not valid, however, since it corresponds to both , /Setup, and , /Status.

- Directories can be addressed with the corresponding SNMP ID. For example, the command "cd /2/8/10/2" has the same effect as "cd /Setup/IP-router/Firewall/Rules".
- Multiple values in a table row can be changed with **one** command, for example in the rules table of the firewall:
 - set WINS UDP sets the protocol of the WINS rule to UDP
 - set WINS UDP ANYHOST sets the protocol of the WINS rule to UDP and the destination to ANYHOST
 - set WINS * ANYHOST also sets the destination of the WINS rule to ANYHOST; the asterisk means that the protocol remains unchanged
- The values in a table row can alternatively be addressed via the column name or the position number in curly brackets. The command set ? in the table shows the name, the possible input values and the position number for each column. For example, in the rules table of the firewall, the destination has the number 4:
 - set WINS {4} ANYHOST sets the destination of the WINS rule to ANYHOST
 - set WINS {destination} ANYHOST also sets the destination of the WINS rule to ANYHOST
 - set WINS {dest} ANYHOST sets the destination of the WINS rule to ANYHOST, because specifying "dest" here is sufficient to uniquely identify the column name.
- Names that contain spaces must be enclosed within quotation marks (, ,).
- A command-specific help function is available for actions and commands (call the function with a question mark as the parameter). For example, 'ping ?' shows the options of the integrated ping command.
- Enter , on the command line for a complete listing of the console commands available.

Functions for editing commands

The following commands can be used to edit commands on the command line. The , ESC key sequences, show (for comparison) the shortcuts used on typical VT100/ANSI terminals:

Function	Esc key sequences	Description
Up arrow	ESC [A	In the list of commands last run, jumps one position up (in the direction of older commands).
Down arrow	ESC [B	In the list of commands last run, jumps one position down (in the direction of newer commands).
Right arrow	Ctrl-F ESC [C	Moves the insert cursor one position to the right.
Left arrow	Ctrl-B ESC [D	Moves the insert cursor one position to the left.
Home or Pos1	Ctrl-A ESC [A ESC [1^ (Moves the insert cursor to the first character in the line.
End	Ctrl-E ESC [F ESC [O ESC [4^	Moves the insert cursor to the last character in the line.
Ins	ESC [ESC [2^	Switches between input and overwrite modes.
Del	Ctrl-D ESC <BS> ESC [3^	Deletes the character at the current position of the insert cursor or ends the Telnet session if the line is blank.
erase	<BS>	Deletes the next character to the left of the insert cursor.
erase-bol	Ctrl-U	Deletes all characters to the left of the insert cursor.
erase-eol	Ctrl-K	Deletes all characters to the right of the insert cursor.
Tabulator		<p>Completes the input from the current position of the insert cursor for a command or path of the LCOS menu structure:</p> <ul style="list-style-type: none"> ■ If there is only one possibility of completing the command/path, this is accepted by the line. ■ If there is more than one possibility of completing the command/path, this is indicated by an audible sound when pressing the Tab key. Pressing the Tab key again displays a list of all possibilities to complete the entry. Then enter e.g. another letter, to allow unambiguous completion of the input. ■ If there is no possibility of completing the command/path, this is indicated by an audible sound when pressing the Tab key. No further actions are run.

Function keys for the command line

WEBconfig: Setup ► Config ► Function keys

The function keys enable the user to save frequently used command sequences and to call them easily from the command line. In the appropriate table, commands are assigned to function keys F1 to F12 as they are entered in the command line.

■ Key

Name of function key.

Possible values:

- Selection from function keys F1 to F12.

Default:

- F1

■ Mapping

Description of the command/shortcut to be run on calling the function key in the command line.

Possible values:

- All commands/shortcuts possible in the command line

Default:

- Blank

Special values:

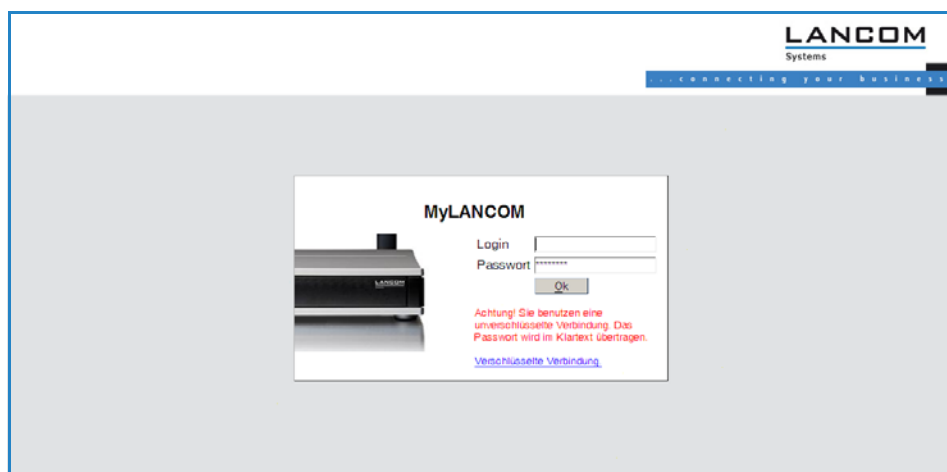
- The caret symbol ^ is used to represent special control commands with ASCII values below 32. ^a
- ^A stands for Ctrl-A (ASCII 1)
- ^Z stands for Ctrl-Z (ASCII 26)
- ^[stands for Escape (ASCII 27)
- ^^ A double caret symbol stands for the caret symbol itself.



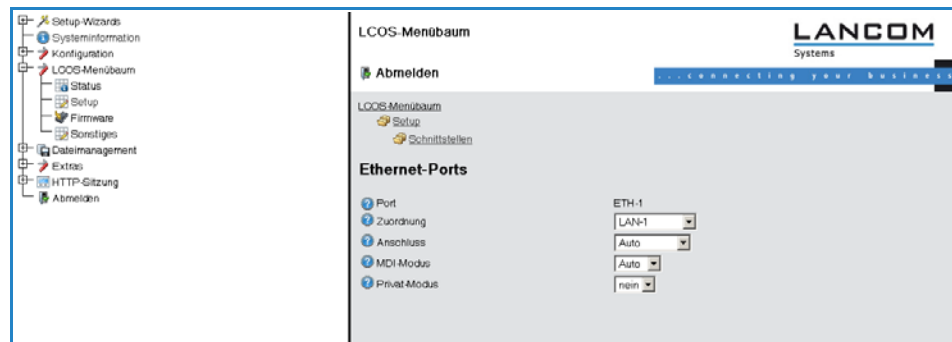
If a caret symbol is entered in a dialog field or editor followed directly by another character, the operating system may possibly interpret this sequence as another special character. By entering caret + A the Windows operating system outputs an Æ. To enter the caret character itself, enter a space in front of the subsequent characters. Sequence ^A is then formed from caret symbol + space + A.

1.3 Configuration with WEBconfig

Device settings can be configured from any web browser. The WEBconfig configuration software is an integral component of the LANCOM. All you need to work with WEBconfig is a web browser. In a network with a DHCP server, you can access the device simply by entering its IP address into your web browser.



The menu area „LCOS Menu Tree“ provides the configuration parameters in the same structure as they are used under Telnet. Clicking the question mark calls up help for each configuration parameter.



2 Setup

This menu allows you to adjust the settings for this device.

Telnet path: /Setup

2.1 Name

This field can be used to enter a name of your choice for this device.

Telnet path: /Setup

Possible values:

- Max. 16 characters

2.2 WAN

This menu contains the configuration of the Wide Area Network (WAN).

Telnet path: /Setup

2.2.18 Backup delay seconds

Wait time before establishing a backup connection in case a remote site should fail.

Telnet path: /Setup/WAN

Possible values:

- Max. 4 characters

Default: 30

2.2.10 Callback attempts

Set the number of callback attempts for automatic callback connections.

Telnet path: /Setup/WAN

Possible values:

- 0 to 9 attempts

Default: 3

2.2.9 Protect

Here you set the conditions to be satisfied in order for the device to accept incoming calls.

Telnet path: /Setup/WAN/Protect

Possible values:

- None: The device answers any call.
- Number: The device will receive a call only if the caller's number is transmitted and if that number is in the number list.
- Screened: The machine will only accept a call if the caller is in the number list, the caller's number is transmitted, and if the number has been checked by the exchange.

Default: None

2.2.2 Dialup peers

Here you configure the ISDN remote sites that your router is to connect to and exchange data with.

Telnet path: /Setup/WAN



If two remote-site lists contain identical names for remote sites (e.g. DSL broadband remote sites and Dialup peers), the LANCOM automatically takes the "fastest" interface when establishing the connection. The other interface is available for backup purposes. If the list does not specify DSL

broadband remote sites, access concentrators or services, then the router connects to the first AC that responds to the request over the exchange. For an existing DSLoL interface, the same entries apply as for a DSL interface. This information is entered into the list of DSL broadband remote sites.

2.2.2.1 Peer

Enter the name of the remote site here.

Telnet path: /Setup/WAN/Dialup-Peers

Possible values:

- Select from the list of defined peers.

Default: Blank

2.2.2.2 Dialup remote

A telephone number is only required if the remote is to be called. The field can be left empty if calls are to be received only. Several numbers for the same remote can be entered in the round-robin list.

Telnet path: /Setup/WAN/Dialup-Peers

Possible values:

- Max. 31 characters

Default: Blank

2.2.2.3 B1 DT

The connection is terminated if it remains unused for the time set here.

Telnet path: /Setup/WAN/Dialup-Peers

Possible values:

- 0 to 9999

Default: 0

2.2.2.4 B2 DT

Hold time for bundling: When channels are bundled, the second B channel will be terminated if it is not used for the time entered here.

Telnet path: /Setup/WAN/Dialup-Peers

Possible values:

- 0 to 9999

Default: 0

2.2.2.5 WAN layer

From the layer list, select an entry that is to be used for this remote site.

The layer list already contains a number of entries with popular standard settings. For example, you should use the PPPHDL entry to establish a PPP connection to an Internet provider.

Telnet path: /Setup/WAN/Dialup-Peers

Possible values:

- Select from the list of defined layers.

Default: Blank

2.2.2.6 Callback

With callback activated, an incoming call from this remote site will not be answered, but it will be called back instead.

This is useful if, for example, telephone fees are to be avoided at the remote site.

Activate a check of the name if you want to be sure that the remote site is authenticated before the callback.

Select the fast option if the callback is to follow within seconds. The remote site must also support this method and the expect-callback option must be activated. Additionally, the remote site must be entered into the number list.

Telnet path: /Setup/WAN/Dialup-Peers

Possible values:

- No: There is no return call.
- Auto: If the remote site is found in the numbers list, this number is called back. Initially the call is rejected and, as soon as the channel is free again, a return call is made (last approx. 8 seconds). If the remote site is not found in the numbers list, the DEFAULT remote site is initially taken and the return call is negotiated during the protocol negotiation. The call is charged with one unit.
- Name: Before a return call is made, the protocol is always negotiated even if the remote site is found in the numbers list (e.g. for Windows computers that dial-in to the device). Small call charges are incurred for this.
- Fast: If the remote site is found in the numbers list, the return call is made quickly, i.e. the LANCOM sends a special signal to the remote site and it calls back as soon as the channel is free again. The connection is established within about 2 seconds. If the remote site does not cancel the call immediately after the signal, then two seconds later it reverts to the normal return call procedure (lasts about 8 seconds). This procedure is available with DSS1 connections only.
- Looser: Use the "looser" option if a return call from the remote site is expected. This setting fulfills two jobs in one. Firstly it ensures that a connection it established itself terminates if a call arrives from the remote site that was just called, and secondly this setting activates the function that reacts to the procedure for fast return calls. This means that to use fast return calls, the caller must be in 'Looser' mode and, at the called party, the return call must be set to 'LANCOM Systems'.

Default: No



The setting 'Name' offers the highest security if there is an entry in the numbers list and in the PPP list. The setting 'LANCOM' enables the fastest method of call-back between two routers from LANCOM Systems.



For Windows remote sites, ensure that you select the setting 'Name'.

2.2.3 RoundRobin

If a remote site can be reached at various call numbers, you can enter these numbers into this list.

Telnet path: /Setup/WAN

2.2.3.1 Peer

Here you select the name of a remote site from the list of remote sites.

Telnet path: /Setup/WAN/RoundRobin

Possible values:

- Select from the list of defined peers.

Default: Blank

2.2.3.2 Round robin

Specify here the other call numbers for this peer. Separate the individual call numbers with hyphens.

Telnet path: /Setup/WAN/RoundRobin

2.2.3.3 Head

Specify here whether the next connection is to be established to the number last reached successfully, or always to the first number.

Telnet path: /Setup/WAN/RoundRobin

Possible values:

- First
- Last

Default: Last

2.2.4 Layer

Here you collect individual protocols into 'layers' that are to be used to transfer data to other routers.

Telnet path: /Setup/WAN

2.2.4.1 WAN layer

This name is used for selecting the layer in the list of remote stations.

Telnet path: /Setup/WAN/Layer

Possible values:

- Max. 9 characters

Default: Blank

2.2.4.2 Encapsulation

Additional encapsulations can be set for data packets.

Telnet path: /Setup/WAN/Layer

Possible values:

- Transparent: No additional encapsulation
- Ethernet: Encapsulation as Ethernet frames.
- LLC-MUX: Multiplexing via ATM with LLC/SNAP encapsulation as per RFC 2684. Several protocols can be transmitted over the same VC (virtual channel).
- VC-MUX: Multiplexing via ATM by establishing additional VCs as per RFC 2684.

Default: ETHER

2.2.4.3 Layer 3

The following options are available for the network layer:

Telnet path: /Setup/WAN/Layer

Possible values:

- Transparent: No additional header is inserted.
- PPP: The connection is established according to the PPP protocol (in synchronous mode, i.e. bit oriented).
 - The configuration data are taken from the PPP table.
- AsyncPPP: Like 'PPP', but here the asynchronous mode is used instead. PPP works with characters.
- ... with script All options can be executed with their own script. The script is specified in the script list.
- DHCP: Allocation of network parameters by DHCP.

Default: PPP

2.2.4.4 Layer 2

This field configures the upper sublayer of the data link layer.

Telnet path: /Setup/WAN/Layer

Possible values:

- Transparent: No additional header is inserted.
- X.75LAPB: Connections are established with X.75 and LAPM (Link Access Procedure Balanced).
- PPPoE: PPP information is encapsulated in Ethernet frames

Default: X.75LAPB

2.2.4.5 Layer 2 options

Here you can activate the compression of transmitted data and channel bundling. These options are only come into effect if they are supported by the interfaces used and by the selected Layer 2 and Layer 3 protocols. For further information please refer to section 'ISDN channel bundling with MLPPP'

Telnet path: /Setup/WAN/Layer

Possible values:

- None
- Compression
- Channel bundling
- Compr. + bundling

Default: None

2.2.4.6 Layer 1

In this field the lower section of the security layer (Data Link Layer) is configured.

Telnet path: /Setup/WAN/Layer

Possible values:

- AAL-5: ATM adaptation layer
- ETH: Transparent Ethernet as per IEEE 802.3.
- HDLC64K: Securing and synchronization of data transmission as per HDLC (in 7 or 8-bit mode).
- HDLC56K: Securing and synchronization of data transmission as per HDLC (in 7 or 8-bit mode).
- V110_9K6: Transmission as per V.110 at max. 9,600 bps, e.g. for dialing in by HSCSD mobile phone
- V110_19K2: Transmission as per V.110 at max. 19,200 bps
- V110_38K4: Transmission as per V.110 at max. 38,400 bps
- Serial: For connections by analog modem or cellular modem with AT interface. The modem can be connected to the device at its serial interface (outband) or to a USB interface by means of a USB-to-serial adapter. Some models feature a CardBus slot that accommodates suitable cards. Some models have an internal integrated modem.
- Modem: For connections via the internal modem emulation when operating as a V.90 host modem over ISDN. Operation of the internal modem may require an additional software option for the device.
- VDSL: VDSL2 data transmission as per ITU G.993.2

Default: HDLC64K



The range of available values depends on the hardware model at hand.

2.2.5 PPP

In order for the router to be able to establish PPP or PPTP connections, you must enter the corresponding parameters (such as name and password) for each remote site into this list.

Telnet path: /Setup/WAN

2.2.5.1 Peer

Enter the name of the remote site here. This name has to agree with the entry in the list of peers/remote sites. You can also select a name directly from the list of peers / remote sites.

Telnet path: /Setup/WAN/PPP

Possible values:

- Select from the list of defined peers.

Default: Blank

Special values: DEFAULT: During PPP negotiations, a remote site dialing-in to the LANCOM logs on with its name. The LANCOM can use the name to retrieve the permitted values for authentication from the PPP table. At the start of the negotiation, the remote site occasionally cannot be identified by call number (ISDN dial-in), IP address (PPTP dial-in) or MAC address (PPPoE dial-in). It is thus not possible to determine the permitted protocols in this first step. In these cases, authentication is performed first with those protocols enabled for the remote site with name DEFAULT. If the remote site is authenticated successfully with these settings, the protocols permitted for the remote site can also be determined.

If authentication uses a protocol entered under DEFAULT, but which is not permitted for the remote site, then authentication is repeated with the permitted protocols.

2.2.5.10 Rights

Specifies the protocols that can be routed to this remote site.

Telnet path: /Setup/WAN/PPP

Possible values:

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

Default: IP

2.2.5.11 Authent. response

Method for securing the PPP connection that the router offers when dialing into a remote site.

Telnet path: /Setup/WAN/PPP

Possible values:

- PAP
- CHAP
- MS-CHAP
- MS-CHAPv2 (multiple entries can be selected)

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



The LANCOM only uses the protocols enabled here—other negotiations with the remote site are not possible.

2.2.5.2 Authent. request

Method for securing the PPP connection that the router expects from the remote site.

Telnet path: /Setup/WAN/PPP

Possible values:

- PAP
- CHAP

- MS-CHAP
- MS-CHAPv2
- (Multiple entries can be selected)

Default: No entry

2.2.5.3 Password

Password transferred from your router to the remote site (if required). A * in the list indicates that an entry exists.

Telnet path: /Setup/WAN/PPP

Possible values:

- Max. 32 characters

Default: Blank

2.2.5.4 Time

Time between two tests of the connection with LCP (see also LCP). This time is entered in multiples of 10 seconds (e.g. 2 for 20 seconds). The value is also the time between two tests of the connection as per CHAP. This time is entered in minutes. For remote sites running the Windows operating system the time must be set to 0.

Telnet path: /Setup/WAN/PPP

Possible values:

- Max. 10 characters

Default: 0

2.2.5.5 Try

Number of retries for the test attempt. Multiple retries reduces the impact from temporary line faults. The connection is only terminated if all tries prove unsuccessful. The time between two retries is one tenth (1/10) of the time between two tests. This value is also the maximum number of "Configure Requests" that the router sends before assuming a line fault and tearing down the connection itself.

Telnet path: /Setup/WAN/PPP

Possible values:

- Max. 10 characters

Default: 5

2.2.5.6 Username

Name with which your router logs in to the remote site. If there is no entry here, your router's device name is used.

Telnet path: /Setup/WAN/PPP

Possible values:

- Max. 64 characters

2.2.5.7 Conf

This parameter affects the mode of operation of the PPP. The parameter is defined in RFC 1661 and is not described in further detail here. If you are unable to establish PPP connections, you can refer to this RFC in conjunction with the PPP statistics of the router for information on fault rectification. The default settings are generally sufficient. This parameter can only be changed with LANconfig, SNMP or TFTP.

Telnet path: /Setup/WAN/PPP

Possible values:

- Max. 10 characters

Default: 10

2.2.5.8 Fail

This parameter affects the mode of operation of the PPP. The parameter is defined in RFC 1661 and is not described in further detail here. If you are unable to establish PPP connections, this RFC in conjunction with the PPP statistics of the router provides information on fault rectification. The default settings are generally sufficient. This parameter can only be changed with LANconfig, SNMP or TFTP.

Telnet path: /Setup/WAN/PPP

Possible values:

- Max. 10 numerical characters

Default: 5

2.2.5.9 Term

This parameter affects the mode of operation of the PPP. The parameter is defined in RFC 1661 and is not described in further detail here. If you are unable to establish PPP connections, this RFC in conjunction with the PPP statistics of the router provides information. The default settings are generally sufficient. This parameter can only be changed with LANconfig, SNMP or TFTP.

Telnet path: /Setup/WAN/PPP

Possible values:

- Max. 10 numerical characters

Default: 2

2.2.6 Incoming calling numbers

Based on the telephone numbers in this list, your router can identify which remote site is making the incoming call.

Telnet path: /Setup/WAN

2.2.6.1 Dialup remote

Here you enter the call number that is transmitted when you are called from the remote site.

Generally this is the number of the remote site combined with the corresponding local area code with the leading zero, e.g. 0221445566.

For remote sites in other countries, you must add the corresponding country code with two leading zeros, e.g. 0049221445566.

Telnet path: /Setup/WAN/Incoming-Calling-Numbers

2.2.6.2 Peer

Enter the name of the relevant remote site.

Once a router has identified a remote site by means of its call number, the list of peers/remote sites is searched for an entry with that name and the associated settings are used for the connection.

Telnet path: /Setup/WAN/Incoming-Calling-Numbers

Possible values:

- Select from the list of defined peers.

Default: Blank

2.2.8 Scripts

If a login script has to be processed when connecting to a remote site, enter the script here.

Telnet path: /Setup/WAN

2.2.8.1 Peer

Enter the name of the remote site here. The remote site should already have been entered into the list of peers / remote sites.

You can also select an entry directly from the list of peers / remote sites.

Telnet path: /Setup/WAN/Scripts

Possible values:

- Select from the list of defined peers.

Default: Blank

2.2.8.2 Scripts

Specify here the login script for this peer.

In order for this script to be used, a layer with the appropriate protocol for this peer must be set up in the list or peers / remote sites.

Telnet path: /Setup/WAN/Scripts

2.2.11 Router interface

Enter here further settings for each WAN interface used by the router, for example the calling numbers to be used.

Telnet path: /Setup/WAN

2.2.11.1 Ifc

WAN interface to which the settings in this entry apply.

Telnet path: /Setup/WAN/Router-Interface

Possible values:

- Select from the list of available WAN interfaces, e.g. S0-1, S0-2 or EXT.

2.2.11.2 MSN/EAZ

Specify here for this interface the call numbers for which the router should accept incoming calls. As a rule these numbers are the call numbers of the ISDN interface (MSN) without an area code, or the internal call number (internal MSN) behind a PBX, as appropriate. Multiple number can be entered by separating them with a semi-colon. The first call number is used for outgoing calls.

Telnet path: /Setup/WAN/Router-Interface

Possible values:

- Max. 30 characters

Default: Blank



If you specify any number outside of your MSN number pool, the router will accept no calls at all.



If you do not enter a number here, the router will accept all calls.

2.2.11.3 CLIP

Activate this option if a peer called by the router should not see your call number.

Telnet path: /Setup/WAN/Router-Interface

Possible values:

- On
- Off

Default: Off



This function must be supported by your network operator.

2.2.11.8 Y Connection

In the router interface list, the entry for the Y connection determines what happens when channel bundling is in operation and a request for a second connection arrives.

Y connection on: The router interrupts channel bundling to establish the second connection to the other remote device. If the second channel becomes free again, it is automatically used for channel bundling again (always for static bundling, when required for dynamic bundling).

Y connection off: The router maintains the existing bundled connection; the second connection must wait.

Telnet path: /Setup/WAN/Router-Interface

Possible values:

- On
- Off

Default: On



Please note that channel bundling incurs costs for two connections. No further connections can be made over LANCAP! Only use channel bundling when the full transfer speed is required and used.

2.2.11.9 Accept calls

Specify here whether calls to this ISDN interface should be answered or not.

Telnet path: /Setup/WAN/Router-Interface

Possible values:

- All
- None

Default: All



If you have specified an MSN for device configuration (Management / Admin), all calls with this MSN will be accepted, whatever you select here.

2.2.13 Manual dialing

This menu contains the settings for manual dialing.

Telnet path: /Setup/WAN

2.2.13.2 Disconnect

Terminates a connection to the remote site which is entered as a parameter.

Telnet path: /Setup/WAN/Manual-Dialing

Possible values:

- Parameter: Name of a remote site defined in the device.

2.2.13.1 Connect

Establishes a connection to the remote site which is entered as a parameter.

Telnet path: /Setup/WAN/Manual-Dialing

Possible values:

- Parameter: Name of a remote site defined in the device.

2.2.17 Channel list

Here you can specify the physical channels to be used for establishing connections to specific remote sites.

Telnet path: /Setup/WAN

2.2.30.1 Peer

Here you select the name of a remote site from the list of remote sites.

Telnet path: /Setup/WAN/Channel-List

Possible values:

- Select from the list of defined peers.

Default: Blank

2.2.17.2 Min

Define how many channels are to be established to this remote site.

Initially the number of channels established is that specified under Minimum. Further channels will be opened if required, but never more than the number defined under Maximum.

Telnet path: /Setup/WAN/Channel-List

Possible values:

- Max. 2 characters

Default: 0

2.2.17.3 Max

Define how many channels are to be established to this remote site.

Initially the number of channels established is that specified under Minimum. Further channels will be opened if required, but never more than the number defined under Maximum.

Telnet path: /Setup/WAN/Channel-List

Possible values:

- Max. 2 characters

Default: 0

2.2.17.4 Head

Here you can define which, and in what order, channels or interfaces are used for this connection. This is especially worthwhile if you want to fix a connection to certain interfaces or when channel bundling should use more than 2 channels. Leaving this field empty allows all available channels or interfaces to be used in any order.

A channel is defined by specifying the interface name (e.g. S0, G703 or EXT, if available), followed by a hyphen, followed by the interface number (except for X21, which is explicit even without an interface number). For some interfaces, it may be necessary to additionally specify a channel number (e.g. S0-1-2 refers to channel 2 on S0 bus 1). Further channel definitions are separated by a semi-colon.

For example, S01 is both channels on S0 bus 1, S0-3-2 is the second channel on the third S0 bus. Entering S0-1-1;S0-3-2 into the field will cause the channels to be used in that order.

Telnet path: /Setup/WAN/Channel-List

Possible values:

- List of possible interfaces.

Default: Blank



ADSL and DSL may be valid interface names, but they are already used by the corresponding DSL ports in the remote-site entry, or they are specified by the layer being used.

2.2.19 DSL broadband peers

Here you configure the DSL broadband remote sites that your router is to connect to and exchange data with.

Telnet path: /Setup/WAN

2.2.19.1 Peer

Enter the name of the remote site here.

Telnet path: /Setup/WAN/DSL-Broadband-Peers

Possible values:

- Select from the list of defined peers.

Default: Blank

2.2.19.10 Service name

The service parameters help you to specify your Internet provider. Contact your provider to obtain these parameters.

Telnet path: /Setup/WAN/DSL-Broadband-Peers/Service-Name

Possible values:

- Max. 32 numerical characters

Default: Blank

2.2.19.11 ATM-VPI

Enter the VPI (Virtual Path Identifier) and the VCI (Virtual Channel Identifier) for your ADSL connection here. These values are communicated to you by your ADSL network operator. Typical values for VPI/VCI are, for example: 0/35, 0/38, 1/32, 8/35, 8/48.

Telnet path: /Setup/WAN/DSL-Broadband-Peers

Possible values:

- Max. 10 characters

Default: 0

2.2.19.12 ATM-VCI

Enter the VPI (Virtual Path Identifier) and the VCI (Virtual Channel Identifier) for your ADSL connection here. These values are communicated to you by your ADSL network operator. Typical values for VPI/VCI are, for example: 0/35, 0/38, 1/32, 8/35, 8/48.

Telnet path: /Setup/WAN/DSL-Broadband-Peers

Possible values:

- Max. 10 characters

Default: 0

2.2.19.13 User def. MAC

Enter the MAC address of your choice is a user-defined address is required.

Telnet path: /Setup/WAN/DSL-Broadband-Peers

Possible values:

- Max. 12 characters

Default: 0

2.2.19.14 DSL interface(s)

Enter the port number of the DSL port here. It is possible to make multiple entries. Separate the list entries either with commas (1,2,3,4) or divide it into ranges (1-4). Activate channel bundling in the relevant layer to bundle the DSL lines.

Telnet path: /Setup/WAN/DSL-Broadband-Peers/DSL-Ifc(s)

Possible values:

- Maximum 8 alphanumerical characters

Default: Blank

2.2.19.15 MAC type

Here you select the MAC addresses which are to be used. If a certain MAC address (user defined) is to be defined for the remote site, this can be entered into the following field.

If local is selected, the device MAC addresses are used to form further virtual addresses for each WAN connection.

If global is selected, the device MAC address is used for all connections.

Telnet path: /Setup/WAN/DSL-Broadband-Peers

Possible values:

- Globally
- Local
- User defined

Default: Local

2.2.19.16 VLAN-ID

Here you enter the specific ID of the VLAN to identify it explicitly on the DSL connection.

Telnet path: /Setup/WAN/DSL-Broadband-Peers

Possible values:

- Max. 10 characters

Default: 0

2.2.19.2 Short holding time

This value specifies the number of seconds that pass before a connection to this remote site is terminated if no data is being transferred.

Telnet path: /Setup/WAN/DSL-Broadband-Peers

Possible values:

- Max. 10 characters

Default: 0

Special values: 9999: With the value 9999, connections are established immediately and without a time limit.

2.2.19.3 AC name

The parameters for access concentrator and service are used to explicitly identify the Internet provider. These parameters are communicated to you by your Internet provider.

Telnet path: /Setup/WAN/DSL-Broadband-Peers

Possible values:

- Max. 64 characters

Default: Blank

2.2.19.10 Service name

The parameters for access concentrator and service are used to explicitly identify the Internet provider. These parameters are communicated to you by your Internet provider.

Telnet path: /Setup/WAN/DSL-Broadband-Peers

Possible values:

- Max. 32 characters

Default: Blank

2.2.19.5 WAN layer

Select the communication layer to be used for this connection. How to configure this layer is described in the following section.

Telnet path: /Setup/WAN/DSL-Broadband-Peers

Possible values:

- Max. 9 characters

Default: Blank

2.2.19.9 AC name

Parameters for the access concentrator and the service uniquely identify the Internet provider. The Internet provider can inform you of these parameters.

Telnet path: /Setup/WAN/DSL-Broadband-Peers/AC-Name

Possible values:

- Max. 64 numerical characters

Default: Blank

2.2.20 IP list

If certain remote sites do not automatically transmit the IP parameters needed for a connection, then enter these values here.

Telnet path: /Setup/WAN

2.2.20.1 Peer

Specify here a NetBIOS name server to be used in case the first NBNS server fails.

Telnet path: /Setup/WAN/IP-List

Possible values:

- Select from the list of defined peers.

Default: Blank

2.2.20.2 IP address

If your Internet provider has supplied you with a fixed, publicly accessible IP address, you can enter this here. Otherwise leave this field empty.

If you use a private address range in your local network and the device is to be assigned with one of these addresses, do not enter the address here but under intranet IP address instead.

Telnet path: /Setup/WAN/IP-List

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.2.20.3 IP netmask

Specify here the netmask associated with the address above.

Telnet path: /Setup/WAN/IP-List

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.2.20.4 Gateway

Enter the address of the standard gateway here.

Telnet path: /Setup/WAN/IP-List

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.2.20.5 DNS default

Specify here the address of a name server to which DNS requests are to be forwarded.

This field can be left empty if you have an Internet provider or other remote site that automatically assigns a name server to the router when it logs in.

Telnet path: /Setup/WAN/IP-List

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.2.20.6 DNS backup

Specify here a name server to be used in case the first DNS server fails.

Telnet path: /Setup/WAN/IP-List

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.2.20.7 NBNS default

Specify here the address of a NetBIOS name server to which NBNS requests are to be forwarded.

This field can be left empty if you have an Internet provider or other remote site that automatically allocates a NetBIOS name server to the router when it logs in.

Telnet path: /Setup/WAN/IP-List

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.2.20.8 NBNS backup

IP address of the NetBIOS name server for the forwarding of NetBIOS requests. Default: 0.0.0.0 The IP address of the LANCOM wireless in this network is communicated as the NBNS server if the NetBIOS proxy is activated for this network. If the NetBIOS proxy is not active for this network, then the IP address in the global TCP/IP settings is communicated as the NBNS server.

Telnet path: /Setup/WAN/IP-List

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.2.20.9 Masquerading IP address

The masquerading IP address is optional. This is used as an alternative address which masks the actual address assigned when the connection was established.

If the masquerading IP address is not set, then the address assigned when the connection was established is used for masquerading.

Telnet path: /Setup/WAN/IP-List

Possible values:

- Valid IP address.

Default: 00.0.0



This setting is necessary when a private address is assigned during the PPP negotiation (172.16.x.x). Normal masquerading is thus impossible as this type of address is filtered in the Internet.

2.2.21 PPTP peers

This table displays and adds the PPTP remote sites.

Telnet path: /Setup/WAN

2.2.21.1 Peer

This name from the list of DSL broadband peers.

Telnet path: /Setup/WAN/PPTP-Peers

Possible values:

- Select from the list of defined peers.

Default: Blank

2.2.21.3 Port

IP port used for running the PPTP protocol. According to the protocol standard, port '1,723' should always be specified.

Telnet path: /Setup/WAN/PPTP-Peers

Possible values:

■ Max. 10 characters

Default: 0

2.2.21.4 SH time

This value specifies the number of seconds that pass before a connection to this remote site is terminated if no data is being transferred.

Telnet path: /Setup/WAN/PPTP-Peers

Possible values:

■ Max. 10 characters

Default: 0

Special values: With the value 9999, connections are established immediately and without a time limit.

2.2.21.5 Routing tag

Routing tag for this entry.

Telnet path: /Setup/WAN/PPTP-Peers

Possible values:

■ Max. 10 characters

Default: 0

2.2.21.6 IP address

Specify the IP address of the PPTP remote station here.

Telnet path: /Setup/WAN/PPTP-Peers/IP-Address

Possible values:

■ Maximum 63 alphanumerical characters

Default: Blank

2.2.22 RADIUS

This menu contains the settings for the RADIUS server.

Telnet path: /Setup/WAN

2.2.22.1 Operating

Switches RADIUS authentication on/off.

Telnet path: /Setup/WAN/RADIUS

Possible values:

■ Yes

■ No

Default: No

2.2.22.3 Authentication port

The TCP/UDP port over which the external RADIUS server can be reached.

Telnet path: /Setup/WAN/RADIUS

Possible values:

- Max. 10 characters

Default: 1812

2.2.22.10 Authentication protocols

Method for securing the PPP connection permitted by the external RADIUS server.

Do not set a method here if the remote site is an Internet provider that your router is to call.

Telnet path: /Setup/WAN/RADIUS

Possible values:

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

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



If all methods are selected, the next available method of authentication is used if the previous one failed. If none of the methods are selected, authentication is not requested from the remote site.

2.2.22.6 CLIP operation

When remote sites dial in, the internal call number list, or alternatively an external RADIUS server, can be used for authentication.

Telnet path: /Setup/WAN/RADIUS

Possible values:

- Yes: Enables the use of an external RADIUS server for the authentication of dial-in remote sites. A matching entry in the call number list takes priority however.
- No: No external RADIUS server is used for authentication of dial-in remote sites.
- Exclusive: Enables the use of an external RADIUS server as the only possibility for authenticating dial-in remote sites. The call number list is ignored.

Default: No



The dial-in remote sites must be configured in the RADIUS server such that the name of the entry corresponds to the call number of the remote site dialing in.

2.2.22.7 CLIP password

Password for the log-in of dial-in remote sites to the external RADIUS server.

Telnet path: /Setup/WAN/RADIUS

Possible values:

- Max. 31 characters

Default: Blank



The dial-in remote sites must be configured in the RADIUS server such that all the entries for all call numbers use the password configured here.

2.2.22.8 Loopback addr.

This is where you can configure an optional sender address to be used instead of the one otherwise automatically selected for the destination address.

If you have configured loopback addresses, you can specify them here as sender address.

Various forms of entry are accepted:

Name of the IP networks whose addresses are to be used.

"INT" for the address of the first intranet.

"DMZ" for the address of the first DMZ (Note: If there is an interface named "DMZ", its address will be taken).

LB0 ... LBF for the 16 loopback addresses.

Furthermore, any IP address can be entered in the form x.x.x.x.

Telnet path: /Setup/WAN/RADIUS

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LB0 to LBF for the 16 loopback addresses
- Any valid IP address

Default: Blank



If the list of IP networks or loopback addresses contains an entry named 'DMZ' then the associated IP address will be used.

2.2.22.5 PPP operation

When PPP remote sites dial in, the internal user authentication data from the PPP list, or alternatively an external RADIUS server, can be used for authentication.

Telnet path: /Setup/WAN/RADIUS

Possible values:

- Yes: Enables the use of an external RADIUS server for authentication of PPP remote sites. A matching entry in the PPP list takes priority however.
- No: No external RADIUS server is used for authentication of PPP remote sites.
- Exclusive: Enables the use of an external RADIUS server as the only possibility for authenticating PPP remote sites. The PPP list is ignored.

Default: No



If you switch the PPP mode to 'Exclusive', the internal user authentication data is ignored, otherwise these have priority.

2.2.22.9 Protocol

RADIUS over UDP or RADSEC over TCP with TLS can be used as the transmission protocol for authentication on an external server.

Telnet path: /Setup/WAN/RADIUS

Possible values:

- RADIUS
- RADSEC

Default: RADIUS

2.2.22.4 Secret

Specify here the key (shared secret) of your RADIUS server from which users are managed centrally.

Telnet path: /Setup/WAN/RADIUS

Default: Blank

2.2.22.2 Server address

Specify here the IP address of your RADIUS server from which users are managed centrally.

Telnet path: /Setup/WAN/RADIUS

Possible values:

■ Valid IP address.

Default: 0.0.0.0

2.2.23 Polling table

In this table, up to 4 IP addresses can be specified for non-PPP-based remote sites which are to be accessed for connection monitoring purposes.

Telnet path: /Setup/WAN

2.2.21.1 Peer

Name of the remote site which is to be checked with this entry.

Telnet path: /Setup/WAN/Polling-Table

Possible values:

■ Select from the list of defined peers.

Default: Blank

2.2.23.2 IP address-1

IP addresses for targeting with ICMP requests to check the remote site.

Telnet path: /Setup/WAN/Polling-Table

Possible values:

■ Valid IP address.

Default: 0.0.0.0

2.2.23.3 Time

Enter the ping interval in seconds here.

Telnet path: /Setup/WAN/Polling-Table

Possible values:

■ Max. 10 characters

Default: 0

Special values: If you enter 0 here and for the re-tries, the default values will be used.

2.2.23.4 Try

If no reply to a ping is received then the remote site will be checked in shorter intervals. The device then tries to reach the remote site once a second. The number of retries defines how many times these attempts are repeated. If the value "0" is entered, then the standard value of 5 retries applies.

Telnet path: /Setup/WAN/Polling-Table

Possible values:

- 0 to 255
- 0: Use default
- Default: 5 retries

Default: 0

2.2.23.5 IP address-2

IP addresses for targeting with ICMP requests to check the remote site.

Telnet path: /Setup/WAN/Polling-Table

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.2.23.6 IP address-3

IP addresses for targeting with ICMP requests to check the remote site.

Telnet path: /Setup/WAN/Polling-Table

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.2.23.7 IP address-4

IP addresses for targeting with ICMP requests to check the remote site.

Telnet path: /Setup/WAN/Polling-Table

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.2.22.8 Loopback addr.

Sender address sent with the ping; this is also the destination for the answering ping. The following can be entered as the loopback address: Name of a defined IP network. 'INT' for the IP address in the first network with the setting 'Intranet'. 'DMZ' for the IP address in the first network with the setting 'DMZ'.

Telnet path: /Setup/WAN/Polling-Table

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LB0 to LBF for the 16 loopback addresses
- Any valid IP address

Default: Blank



If the list of IP networks or loopback addresses contains an entry named 'DMZ' then the associated IP address will be used. Name of a loopback address. Any other IP address.

2.2.24 Backup peers

This table is used to specify a list of possible backup connections for each remote site.

Telnet path: /Setup/WAN

2.2.24.1 Peer

Here you select the name of a remote site from the list of remote sites.

Telnet path: /Setup/WAN/Backup-Peers

Possible values:

- Select from the list of defined peers.

Default: Blank

2.2.24.2 Alternative peers

Specify here one or more remote sites for backup connections.

Telnet path: /Setup/WAN/Backup-Peers

Possible values:

- List of backup peers.

Default: Blank

2.2.24.3 Head

Specify here whether the next connection is to be established to the number last reached successfully, or always to the first number.

Telnet path: /Setup/WAN/Backup-Peers

Possible values:

- Last
- First

Default: Last

2.2.25 Action table

With the action table you can define actions that are executed when the status of a WAN connection changes.

Telnet path: /Setup/WAN

2.2.25.1 Index

The index gives the position of the entry in the table, and thus it must be unique. Entries in the action table are executed consecutively as soon as there is a corresponding change in status of the WAN connection. The entry in the field "Check for" can be used to skip lines depending on the result of the action. The index sets the position of the entries in the table (in ascending order) and thus significantly influences the behavior of actions when the option "Check for" is used. The index can also be used to actuate an entry in the action table via a cron job, for example to activate or deactivate an entry at certain times.

Telnet path: /Setup/WAN/Action-Table

Possible values:

- Max. 10 characters

Default: 0

2.2.25.2 Host name

Action name. This name can be referenced in the fields "Action" and "Check for" with the place holder %h (host name).

Telnet path: /Setup/WAN/Action-Table

Possible values:

- Max. 64 characters

Default: Blank

2.2.25.3 Peer

A change in status of this remote site triggers the action defined in this entry.

Telnet path: /Setup/WAN/Action-Table

Possible values:

- Select from the list of defined peers.

Default: Blank

2.2.25.4 Lock time

Prevents this action from being repeated within the period defined here in seconds.

Telnet path: /Setup/WAN/Action-Table

Possible values:

- Max. 10 characters

Default: 0

2.2.25.5 Condition

The action is triggered when the change in WAN-connection status set here occurs.

Telnet path: /Setup/WAN/Action-Table

Possible values:

- Establish: The action is triggered when the connection has been established successfully.
- Disconnect: The action is triggered when the device itself terminates the connection (e.g. by manual disconnection or when the hold time expires).
- End: The action is triggered on disconnection (whatever the reason for this).
- Failure: This action is triggered on disconnects that were not initiated or expected by the device.
- Establish failure: This action is triggered when a connection establishment was started but not successfully concluded.

Default: Establish

2.2.25.6 Action

Here you describe the action that should be executed when there is a change in the status of the WAN connection. Only one action can be triggered per entry.

Telnet path: /Setup/WAN/Action-Table

Possible values:

- exec: – This prefix initiates any command as it would be entered at the Telnet console. For example, the action "exec:do /o/m/d" terminates all current connections.
- dnscheck: – This prefix initiates a DSN name resolution. For example, the action "dnscheck:myserver.dyndns.org" requests the IP address of the indicated server.
- http: – This prefix initiates an HTTP-get request. For example, you can use the following action to execute a DynDNS update at dyndns.org:

- `http://username:password@members.dyndns.org/nic/update?system=dyndns&hostname=%h&myip=%a`
- The meaning of the place holders %h and %a is described below.
- `https:` – Like “`http:`”, except that the connection is encrypted.
- `gnudip:` – This prefix initiates a request to the corresponding DynDNS server via the GnuDIP protocol. For example, you can use the following action to use the the GnuDIP protocol to execute a DynDNS update at a DynDNS provider:
- `gnudip://gnudipsrv?method=tcp&user=myserver&domn=mydomain.org`
- `&pass=password&reqc=0&addr=%a`
- The line-break is for legibility only and is not to be entered into the action. The meaning of the place holder %a is described below.
- `repeat:` – This prefix together with a time in seconds repeats all actions with the condition “Establish” as soon as the connection has been established. For example, the action “repeat 300” causes all of the establish actions to be repeated every 5 minutes.
- `mailto:` – This prefix causes an e-mail to be sent. For example, you can use the following action to send an e-mail to the system administrator when a connection is terminated:
- `mailto:admin@mycompany.com?subject=VPN connection broken at %t?body=VPN connection to Sub-sidiary 1 was broken.`
- Optional variables for the actions:
- %a – WAN IP address of the WAN connection relating to the action.
- %H – Host name of the WAN connection relating to the action.
- %h – Like %h, except the hostname is in small letters
- %c – Connection name of the WAN connection relating to the action.
- %n – Device name
- %s – Device serial number
- %m – Device MAC address (as in Sysinfo)
- %t – Time and date in the format YYYY-MM-DD hh:mm:ss
- %e – Description of the error that was reported when connection establishment failed.
- The result of the actions can be evaluated in the “Check for” field.

Default: Blank

2.2.25.7 Check for

The result of the action can be evaluated here to determine the number of lines to be skipped in the processing of the action table.

Telnet path: /Setup/WAN/Action-Table

Possible values:

- `contains=` – This prefix checks if the result of the action contains the defined string.
- `isequal=` – This prefix checks if the result of the action is exactly equal to the defined string.
- `?skipiftrue=` – This suffix skips the defined number of lines in the list of actions if the result of the “contains” or “isequal” query is TRUE.
- `?skipiffalse=` – This suffix skips the defined number of lines in the list of actions if the result of the “contains” or “isequal” query is FALSE.
- Optional variables for the actions:
- As with the definition of the action.

Default: Blank

2.2.25.8 Operating

Activates or deactivates this entry.

Telnet path: /Setup/WAN/Action-Table

Possible values:

- Yes

- No

Default: Yes

2.2.25.9 Owner

Owner of the action. The exec actions are executed with the rights of the owner. If the owner does not have the necessary rights (e.g. administrators with write access) then the action will not be carried out.

Telnet path: /Setup/WAN/Action-Table

Possible values:

- Select from the administrators defined in the device.

Default: root

2.2.26 MTU list

This table allows you to set alternative MTU (Maximum Transfer Unit) values to those automatically negotiated by default.

Telnet path: /Setup/WAN

2.2.26.1 Peer

Enter the name of the remote site here. This name has to agree with the entry in the list of peers/remote sites. You can also select a name directly from the list of peers / remote sites.

Telnet path: /Setup/WAN/MTU-List

Possible values:

- Select from the list of defined peers.

Default: Blank

2.2.26.2 MTU

Here you can manually define a maximum MTU per connection in addition to the automatic MTU settings. Enter the maximum IP packet length/size in bytes. Smaller values lead to greater fragmentation of the payload data.

Telnet path: /Setup/WAN/MTU-List

Possible values:

- Max. 4 characters

Default: 0

2.2.30 Additional PPTP gateways

Here you can define up to 32 additional gateways to ensure the availability of PPTP peers. Each of the PPTP peers has the possibility of using up to 33 gateways. The additional gateways can be defined in a supplementary list.

Telnet path: /Setup/WAN

2.2.30.1 Peer

Here you select the PPTP remote site that this entry applies to.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Select from the list of defined PPTP remote stations.

Default:

- Blank

2.2.30.3 Gateway-1

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default:

- Blank

2.2.30.4 Rtg-Tag-1

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default:

0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.5 Gateway-2

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default:

- Blank

2.2.30.6 Rtg-Tag-2

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default:

0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.7 Gateway-3

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.8 Rtg-Tag-3

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.9 Gateway-4

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.10 Rtg tag 4

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.11 Gateway 5

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.12 Rtg-Tag-5

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.13 Gateway 6

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.14 Rtg-Tag-6

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.15 Gateway-7

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.16 Rtg-Tag-7

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.17 Gateway-8

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.18 Rtg-Tag-8

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.19 Gateway-9

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.20 Rtg-Tag-9

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.21 Gateway-10

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.22 Rtg-Tag-10

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.23 Gateway-11

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.24 Rtg-Tag-11

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.25 Gateway-12

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.26 Rtg-Tag-12

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.27 Gateway-13

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.28 Rtg-Tag-13

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.29 Gateway-14

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways/Gateway-14

Possible values:

- IP address or 63 alphanumerical characters.

Default: Blank

2.2.30.30 Rtg-Tag-14

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.31 Gateway-15

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.32 Rtg-Tag-15

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.33 Gateway-16

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.34 Rtg-Tag-16

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.35 Gateway-17

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.36 Rtg-Tag-17

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.37 Gateway-18

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.38 Rtg-Tag-18

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.39 Gateway-19

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.40 Rtg-Tag-19

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.41 Gateway-20

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways/Gateway-20

Possible values:

- IP address or 63 alphanumerical characters.

Default: Blank

2.2.30.42 Rtg-Tag-20

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.43 Gateway-21

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.44 Rtg-Tag-21

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.45 Gateway-22

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.46 Rtg-Tag.22

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.47 Gateway-23

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.48 Rtg-Tag-23

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.49 Gateway-24

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.50 Rtg-Tag-24

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.51 Gateway-25

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.52 Rtg-Tag-25

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.53 Gateway-26

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.54 Rtg-Tag-26

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.55 Gateway-27

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumerical characters.

Default: Blank

2.2.30.56 Rtg-Tag-27

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.57 Gateway-28

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways/Gateway-28

Possible values:

- IP address or 63 alphanumeric characters.

Default: Blank

2.2.30.58 Rtg-Tag-28

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.59 Gateway-29

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumeric characters.

Default: Blank

2.2.30.60 Rtg-Tag-29

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.61 Gateway-30

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumeric characters.

Default: Blank

2.2.30.62 Rtg-Tag-30

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.63 Gateway-31

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways/Gateway-31

Possible values: IP address or 63 alphanumeric characters.

Default: Blank

2.2.30.64 Rtg-Tag-31

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.65 Gateway-32

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- IP address
- Maximum 63 alphanumeric characters.

Default: Blank

2.2.30.66 Rtg-Tag-32

Enter the routing tag for setting the route to the relevant remote gateway.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Maximum 5 characters.

Default: 0



If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

2.2.30.2 Begin with

Here you select the order in which the entries are to be tried.

Telnet path: /Setup/WAN/Additional-PPTP-Gateways

Possible values:

- Last used: Selects the entry for the connection which was successfully used most recently.
- First: Selects the first of the configured remote sites.
- Random: Selects one of the configured remote sites at random. This setting provides an effective measure for load balancing between the gateways at the headquarters.

Default:

- Last used

2.3 Charges

This menu contains the settings for charge management.

Telnet path: /Setup

2.3.12 Reset budgets

If you wish to extend the online budget for one-time events, such as when downloading a very large file from the Internet, you do not necessarily have to change the time limit. In these cases you can manually reset the limit.

Telnet path: /Setup/Charges

Default: Blank

2.3.1 Budget units

Specify here the maximum number of budget units that can be consumed in the time period defined above. Once this limit is reached, the router establishes no further connections.

Telnet path: /Setup/Charges

Possible values:

- Max. 10 characters

Default: 830

2.3.16 Activate additional budget

Activating an additional time limit releases this amount of time for consumption in the current period. In the next period, the normal time limit applies again.

Telnet path: /Setup/Charges

2.3.8 DSL broadband minutes budget

Specify here the maximum number of online minutes that can be consumed in the time period defined above. Once this limit is reached, the router establishes no further connections.

Telnet path: /Setup/Charges

Possible values:

- Max. 10 characters

Default: 600

2.3.13 Dialup minutes budget

Specify here the maximum number of online minutes that can be consumed in the time period defined above. Once this limit is reached, the router establishes no further connections.

Telnet path: /Setup/Charges

Possible values:

- Max. 10 characters

Default: 210

2.3.6 Total units

Displays the total of budgeted units used until now on all interfaces.

Telnet path: /Setup/Charges

Default: 10

2.3.11 Additional DSL broadband budget

Specify here the number of additional online minutes that are permitted within the above time period if the reserve is activated.

Telnet path: /Setup/Charges

Possible values:

- Max. 10 characters

Default: 300

2.3.3 Spare units

Displays the number of charge units remaining for dial-in connections in the current period.

Telnet path: /Setup/Charges

2.3.9 Spare DSL broadband minutes

Displays the number of minutes remaining for DSL broadband connections in the current period.

Telnet path: /Setup/Charges

2.3.14 Spare dialup minutes

Displays the number of minutes remaining for dial-in connections in the current period.

Telnet path: /Setup/Charges

2.3.10 Router DSL broadband budget

Displays the number of minutes used by DSL broadband connections in the current time period.

Telnet path: /Setup/Charges

2.3.4 Router units

Displays the number of minutes used by router connections in the current time period.

Telnet path: /Setup/Charges

2.3.15 Router ISDN serial minutes active

Displays the number of minutes used by dial-in connections in the current time period.

Telnet path: /Setup/Charges

2.3.2 Days per period

Specify a period in days that will serve as the basis for the controlling the charges and time limits.

Telnet path: /Setup/Charges

Possible values:

- Max. 10 characters

Default: 1

2.3.5 Table budget

This table displays an overview of configured budgets for your interfaces, sorted by budget units.

Telnet path: /Setup/Charges

2.3.5.1 Ifc.

The interface referred to by the entry.

Telnet path: /Setup/Charges/Table-Budget

2.3.5.2 Budget units

Displays the budget units used up for this interface.

Telnet path: /Setup/Charges/Table-Budget

2.3.5.3 Spare units

Displays the remaining budgeted units for this interface.

Telnet path: /Setup/Charges/Table-Budget

2.3.5.4 Units

Displays the budgeted units used until now for this interface.

Telnet path: /Setup/Charges/Table-Budget

2.3.7 Time table

This table displays an overview of configured budgets for your interfaces, sorted by budget minutes.

Telnet path: /Setup/Charges

2.3.7.1 Ifc.

The interface referred to by the entry.

Telnet path: /Setup/Charges/Time-Table

2.3.7.2 Budget minutes

Displays the budgeted minutes used up for this interface.

Telnet path: /Setup/Charges/Time-Table

2.3.7.3 Spare minutes

Displays the remaining budgeted minutes for this interface.

Telnet path: /Setup/Charges/Time-Table

2.3.7.4 Minutes active

Displays the budgeted minutes of activity for data connections on this interface.

Telnet path: /Setup/Charges/Time-Table

2.3.7.5 Minutes passive

Displays the budgeted minutes that this interface was connected passively.

Telnet path: /Setup/Charges/Time-Table

2.4 LAN

This item contains the settings for the LAN.

Telnet path: /Setup/LAN

2.4.3 Spare heap

The spare-heap value indicates how many blocks of the LAN heap are reserved for communication with the device over HTTP(S)/Telnet(S)/SSH. This heap is used to maintain the device's accessibility even in case of maximum load (or if queue blocks get lost). If the number of blocks in the heap falls below the specified value, received packets are rejected immediately (except for TCP packets sent directly to the device).

Telnet path: /Setup/LAN/Spare-Heap

Possible values:

- Max. 3 numeric characters in the range 0 – 999

Default: 10

2.4.2 MAC-Address

This is the hardware address of the network adapter in your device.

Telnet path: /Setup/LAN/MAC-Address

2.4.9 Trace level

The output of trace messages for the LAN-Data-Trace can be restricted to contain certain content only.

Telnet path: /Setup/LAN/Trace-Level

Possible values:

- Numerical characters from 0 to 255

Default: 255

Special values:

- 0: Reports that a packet has been received/sent
- 1: Adds the physical parameters for the packets (data rate, signal strength...)
- 2: Adds the MAC header
- 3: Adds the Layer-3 header (e.g. IP/IPX)
- 4: Adds the Layer-4 header (TCP, UDP...)
- 5: Adds the TCP/UDP payload
- 255: Output is not limited

2.4.8 Trace MAC

Use this value to limit the Ethernet trace to those packets that have the specified MAC address as their source or destination address.

Telnet path: /Setup/LAN/Trace-MAC

Possible values:

- 12 hexadecimal characters

Default: 000000000000

Special values: If set to 000000000000, the Ethernet trace outputs all packages.

2.4.10 IEEE802.1x

This menu contains the settings for the integrated 802.1x supplicant. The device requires these settings, for example, if it is connected to an Ethernet switch with activated 802.1x authentication.

Telnet path: /Setup/LAN/IEEE802.1x

2.4.10.1 Supplicant Ifc setup

This table controls the function of the integrated 802.1x supplicant for the available LAN interfaces.

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

2.4.10.1.1 Ifc

Here you select the LAN interface that the settings for the 802.1x supplicant apply to.

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

Possible values:

- Choose from the LAN interfaces available in the device, e.g. LAN-1 or LAN-2.

Default: LAN-1

2.4.10.1.2 Method

Here you select the method to be used by the 802.1x supplicant for authentication.

Telnet path: /Setup/LAN/IEEE802.1x/Supplicant-Ifc-Setup/Method

Possible values:

- None
- MD5
- TLS
- TTLS/PAP
- TTLS/CHAP
- TTLS/MSCHAP
- TTLS/MSCHAPv2
- TTLS/MD5
- PEAP/MSCHAPv2
- PEAP/GTC

Default: None

Special values: The value "None" disables the 802.1x supplicant for the respective interface.

2.4.10.1.3 Credentials

Depending on the EAP/802.1X method, enter the credentials necessary to login. TLS requires nothing to be entered here. The authentication is carried out with the EAP/TLS certificate stored in the file system. For all other methods, enter the user name and password in the format 'user:password'.

Telnet path: /Setup/LAN/IEEE802.1x/Supplicant-Ifc-Setup/Credentials

Possible values:

- Max. 64 alphanumerical characters

Default: Blank

2.5 Bridge

This menu contains the settings for the bridge.

Telnet path: /Setup/Bridge



These bridge settings are included to maintain compatibility to earlier firmware versions. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.5.4 Aging minutes

Here you can specify a time period in minutes after which the bridge table is updated automatically, i.e. any MAC addresses that have not been contacted are removed from the list.

Telnet path: /Setup/Bridge/Aging-Minutes

Possible values:

- Max. 63 numerical characters

Default: 30

2.5.1 Operating

This is where you can activate or deactivate the remote bridge. The remote bridge couples two remote networks as if they were physically connected. This makes them completely independent of the employed network protocols.

LANconfig description: Remote bridge enabled

Telnet path: /Setup/Bridge/Operating

LANconfig path: Bridge/General

Possible values:

-

Possible LANconfig values:

- On
- Off

Default: Off

2.5.2 Peer

Choose the name of the remote site here. If the remote station is to be actively contacted, then this must be an entry from the list of defined peers.

LANconfig description:

Telnet path: /Setup/Bridge/Peer

LANconfig path: Bridge/General

Possible values:

- Entry from the list of defined peers

Possible LANconfig values:

- Entry from the list of defined peers

Default: Blank

2.5.7 LAN interface

Here you select the interface to which the bridge settings apply.

Telnet path: /Setup/Bridge/LAN-Interface

Possible values:

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

Default: LAN-1

2.5.8 VLAN-ID

Enter the ID of the VLAN with the active bridge here.

Telnet path: /Setup/Bridge/VLAN-ID

Possible values:

- Numeric value from 0 – 4096

Default: 0

2.5.3 Bridge table

This status table displays information about the MAC addresses known to the bridge with the following values:

- MAC address of a local or remote computer
- Time when a packet was last received from the MAC address (in milliseconds of operating time)
- Flags indicating from where the MAC address was learned (local/remote) and what should happen with a package that is received from the MAC address
 - LAN-Dest.-Filter: Filtering of transmissions towards the LAN
 - LAN-Src.-Filter: Filtering of transmissions received from the LAN
 - WAN-Dest.-Filter: Filtering of transmissions towards the WAN WAN-Src.-Filter: Filtering of transmissions received from the LAN

Telnet path: /Setup/Bridge/Bridge-Table

2.5.5 LAN configuration

The settings for the filter options for local networks are located here.

LANconfig description: Local filtering

Telnet path: /Setup/Bridge/LAN-Config

LANconfig path: Bridge

2.5.5.1 Broadcast

Specify here whether broadcast packets from the LAN should be transmitted or not.

LANconfig description: Broadcasts

Telnet path: /Setup/Bridge/LAN-Config/Broadcast

LANconfig path: Bridge/Local filtering

Possible values:



Possible LANconfig values:

- Never transmit
- Always transmit
- Only when connected

Default: Always transmit

2.5.5.2 Multicast

Specify whether multicast packets from the local network should be transmitted always, never or only when connected.

LANconfig description: Multicast

Telnet path: /Setup/Bridge/LAN-Config/Multicast

LANconfig path: Bridge/Local filtering

Possible values:



Possible LANconfig values:

- Never transmit
- Always transmit
- Only when connected

Default: Always transmit

2.5.5.3 Destination address

The settings here control the filtering of incoming packets according to their destination addresses.

Telnet path: /Setup/Bridge/LAN-Config./Dest.-Address

2.5.5.3.1 Filter type

Here you specify the criteria which are to be used for filtering the destination addresses.

LCOS Menu Tree/Setup/Bridge/LAN-Config./Dest.-Address/Filter-Type

Possible values:

- Positive: Only the addresses contained in the filter table are filtered out; all the others are allowed through
- Negative: Only the addresses contained in the filter table are allowed through; all the others are filtered out

Default: Positive

2.5.5.3.2 Filter table

Packets from the local network sent to the addresses in this table will be filtered out or allowed to pass, depending on the filter type.

Telnet path: /Setup/Bridge/LAN-Config./Dest.-Address/Filter-Table

2.5.5.3.2.1 Destination address

Enter the address which is to be filtered here.

Telnet path: /Setup/Bridge/LAN-Config./Dest.-Address/Filter-Table/Dest.-Address

Possible values:

- Maximum 12 alphanumerical characters

Default: Blank

2.5.5.4 Source address

The settings for filtering the source addresses can be adjusted here.

Telnet path: /Setup/Bridge/LAN-Config./Src.-Address

2.5.5.4.1 Filter type

Here you specify the criteria which are to be used for filtering the source addresses.

Telnet path: /Setup/Bridge/LAN-Config./Src.-Address/Filter-Type

Possible values:

- Positive: Only the addresses contained in the filter table are filtered out; all the others are allowed through
- Negative: Only the addresses contained in the filter table are allowed through; all the others are filtered out

Default: Positive

2.5.5.4.2 Filter table

Packets from the local network sent from the addresses in this table will be filtered out or allowed to pass, depending on the filter type.

Telnet path: /Setup/Bridge/LAN-Config./Src.-Address/Filter-Table

2.5.5.4.2.1 Source address

Enter the address which is to be filtered here.

Telnet path: /Setup/Bridge/LAN-Config./Src.-Address/Filter-Table/Src.-Address

Possible values:

- Maximum 12 alphanumeric characters

Default: Blank

2.5.6 WAN configuration

The settings for the filter options for remote networks are located here.

LANconfig description: Remote filtering**Telnet path:** /Setup/Bridge/WAN-Config**LANconfig path:** Bridge

2.5.6.1 Broadcast

Specify here whether broadcast packets from the WAN should be transmitted or not.

LANconfig description: Broadcasts**Telnet path:** /Setup/Bridge/WAN-Config/Broadcast**LANconfig path:** Bridge/Remote filtering**Possible values:****Possible LANconfig values:**

- Never transmit
- Always transmit
- Only when connected

Default: Always transmit

2.5.6.2 Multicast

Specify whether multicast packets from the WAN should be transmitted always, never or only when connected.

LANconfig description: Multicast**Telnet path:** /Setup/Bridge/WAN-Config/Multicast**LANconfig path:** Bridge/Remote filtering**Possible values:****Possible LANconfig values:**

- Never transmit
- Always transmit
- Only when connected

Default: Always transmit

2.5.6.3 Destination address

The settings here control the filtering of incoming packets according to their destination addresses.

Telnet path: /Setup/Bridge/WAN-Config/Dest.-Address

2.5.6.3.1 Filter type

Here you specify the criteria which are to be used for filtering the destination addresses.

Telnet path: /Setup/Bridge/WAN-Config./Dest.-Address/Filter-Type**Possible values:**

- Positive: Only the addresses contained in the filter table are filtered out; all the others are allowed through
- Negative: Only the addresses contained in the filter table are allowed through; all the others are filtered out

Default: Positive

2.5.6.3.2 Filter table

Packets from the WAN sent to the addresses in this table will be filtered out or allowed to pass, depending on the filter type.

Telnet path: /Setup/Bridge/WAN-Config./Dest.-Address/Filter-Table

2.5.6.3.2.1 Destination address

Enter the address which is to be filtered here.

Telnet path: /Setup/Bridge/WAN-Config./Dest.-Address/Filter-Table/Dest.-Address

Possible values:

- Maximum 12 alphanumerical characters

Default: Blank

2.5.6.4 Source address

The settings for filtering the source addresses can be adjusted here.

Telnet path: /Setup/Bridge/WAN-Config./Src.-Address

2.5.6.4.1 Filter type

Here you specify the criteria which are to be used for filtering the source addresses.

Telnet path: /Setup/Bridge/WAN-Config./Src.-Address/Filter-Type

Possible values:

- Positive: Only the addresses contained in the filter table are filtered out; all the others are allowed through
- Negative: Only the addresses contained in the filter table are allowed through; all the others are filtered out

Default: Positive

2.5.6.4.2 Filter table

Packets from the WAN sent from the addresses in this table will be filtered out or allowed to pass, depending on the filter type.

Telnet path: /Setup/Bridge/WAN-Config./Src.-Address/Filter-Table

2.5.6.4.2.1 Destination address

Enter the address which is to be filtered here.

Telnet path: /Setup/Bridge/WAN-Config./Src.-Address/Filter-Table/Src.-Address

Possible values:

- Maximum 12 alphanumerical characters

Default: Blank

2.7 TCP-IP

This menu contains the TCP/IP settings.

Telnet path: /Setup

2.7.1 Operating

Activates or deactivates the TCP-IP module.

Telnet path: Setup/TCP-IP

Possible values:

■ Yes

■ No

Default: Yes

2.7.11 ARP aging minutes

Here you can specify the time in minutes after which the ARP table is updated automatically, i.e. any addresses that have not been contacted since the last update are removed from the list.

Telnet path: Setup/TCP-IP

Possible values:

■ 1 to 60 minutes

Default: 15 minutes

2.7.8 DNS backup

Specify here a name server to be used in case the first DNS server fails.

Telnet path: Setup/TCP-IP

Possible values:

■ Valid IP address.

Default: 00.0.0

2.7.7 DNS default

Specify here the address of a name server to which DNS requests are to be forwarded. This field can be left empty if you have an Internet provider or other remote site that automatically assigns a name server to the router when it logs in.

Telnet path: Setup/TCP-IP

Possible values:

■ Valid IP address.

Default: 00.0.0

2.7.22 ICMP on ARP timeout

When the LANCOM device receives a packet that it should transmit to the LAN it uses ARP requests to determine the recipient. If a request goes unanswered, the device returns a "ICMP host unreachable" message to the sender of the packet.

Telnet path: Setup/TCP-IP

2.7.10 NBNS backup

Specify here a NetBIOS name server to be used in case the first NBNS server fails.

Telnet path: Setup/TCP-IP

Possible values:

■ Valid IP address.

Default: 0.0.0.0

2.7.9 NBNS default

Specify here the address of a NetBIOS name server to which NBNS requests are to be forwarded. This field can be left empty if you have an Internet provider or other remote site that automatically allocates a NetBIOS name server to the router when it logs in.

Telnet path: Setup/TCP-IP

Possible values:

- Valid IP address.

Default: 00.0.0

2.7.20 Non-local ARP replies

When this option is activate the device will reply to ARP requests for its address even if the sender address is not located in its own local network.

Telnet path: Setup/TCP-IP

2.7.6 Access list

The access list contains those stations that are to be granted access to the device's configuration. If the table contains no entries, all stations can access the device.

Telnet path: Setup/TCP-IP

2.7.6.1 IP address

IP address of the station that is to be granted access to the device's configuration.

Telnet path: /Setup/TCP-IP/Access-List

Possible values:

- Valid IP address.

2.7.6.2 IP netmask

IP netmask of the station that is to be given access to the device's configuration.

Telnet path: /Setup/TCP-IP/Access-List

Possible values:

- Valid IP address.

2.7.6.3 Routing tag

Routing tag for selecting a specified route.

Telnet path: /Setup/TCP-IP/Access-List

Possible values: Max. 5 characters

2.7.16 ARP table

The address resolution protocol (ARP) determines the MAC address for a particular IP address and stores this information in the ARP table.

Telnet path: Setup/TCP-IP

2.7.16.1 IP address

IP address for which a MAC address was determined.

Telnet path: /Setup/TCP-IP/ARP-Table

Possible values:

- Valid IP address.

2.7.16.2 MAC address

MAC address matching the IP address in this entry.

Telnet path: /Setup/TCP-IP/ARP-Table

2.7.16.3 Last access

The time when this station last access the network.

Telnet path: /Setup/TCP-IP/ARP-Table

2.7.16.5 Ethernet port

Physical interface connecting the station to the device.

Telnet path: /Setup/TCP-IP/ARP-Table

2.7.16.6 Peer

Remote device over which the station can be reached.

Telnet path: /Setup/TCP-IP/ARP-Table

Possible values:

- Select from the list of defined peers.

2.7.16.7 VLAN-ID

VLAN ID of network where the station is located.

Telnet path: /Setup/TCP-IP/ARP-Table

2.7.16.8 Connect

Logical interface connecting the device.

Telnet path: /Setup/TCP-IP/ARP-Table/Connect

Possible values:

- A parameter from the list of logical interfaces.

2.7.17 Loopback list

This table is used to configure alternative addresses.

Telnet path: Setup/TCP-IP

2.7.17.1 Loopback address

You can optionally configure up to 16 loopback addresses here. The device considers each of these addresses to be its own address and behaves as if it has received the package from the LAN. This applies in particular to masked connections. Answers to packets sent to a loopback address are not masked.

Telnet path: /Setup/TCP-IP/Loopback-List

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LB0 to LBF for the 16 loopback addresses
- Any valid IP address

Default: 0.0.0.0

2.7.17.2 Name

You can enter a name with a max. 16 characters here

Telnet path: /Setup/TCP-IP/Loopback-List

Possible values:

■ Max. 16 characters

Default: Blank

2.7.17.3 Routing tag

Here you specify the routing tag that identifies routes to remote gateways that are not configured with their own routing tag (i.e. the routing tag is 0).

Telnet path: /Setup/TCP-IP/Loopback-List

Possible values:

■ 0 to max. 65,535

Default: 0

2.7.21 Alive test

This menu contains the settings for the alive test.

Telnet path: Setup/TCP-IP

2.7.21.6 Boot type

The way the boot is carried out: Warm start or cold start

Telnet path: /Setup/TCP-IP/Alive-Test

2.7.21.5 Fail limit

This parameter defines the number of consecutive failed tests before the device reboots.

Telnet path: /Setup/TCP-IP/Alive-Test

Possible values:

■ Max. 10 numeric characters in the range 0 – 4289999999

Default: 10

2.7.21.2 Test interval

Interval at which pings are sent

Telnet path: /Setup/TCP-IP/Alive-Test

2.7.21.4 Retry interval

Interval at which the retries are sent

Telnet path: /Setup/TCP-IP/Alive-Test

2.7.21.3 Retry count

Number of retries until the device boots

Telnet path: /Setup/TCP-IP/Alive-Test

2.7.21.1 Target address

IP address being pinged.

Telnet path: /Setup/TCP-IP/Alive-Test

Possible values:

- Valid IP address.

2.7.30 Network list

This table is used to define IP networks. These are referenced from other modules (DHCP server, RIP, NetBIOS, etc.) via the network names.

Telnet path: Setup/TCP-IP

2.7.30.1 Network name

Enter a unique name with max. 16 characters that the other modules (DHCP server, RIP, NetBIOS, etc.) can use to reference the network.

Telnet path: /Setup/TCP-IP/Network-List

Possible values:

- Max. 16 characters

Default: Blank

2.7.30.2 IP address

If you use a private address range in your local network, then enter an available address from this range here. IP masquerading conceals these addresses from remote networks, and these see only the Internet IP address of the corresponding remote station.

Telnet path: /Setup/TCP-IP/Network-List

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.7.30.3 IP netmask

If the intranet IP address you entered is an address from a private address range, then enter the associated netmask here.

Telnet path: /Setup/TCP-IP/Network-List

Possible values:

- Valid IP address.

Default: 255.255.255.0

2.7.30.4 VLAN-ID

A single physical interface can be used to connect multiple separate VLANs (which were separated by a switch previously). The router must be given its own address and/or its own network in each of these VLANs. For this purpose, the interfaces and also a VLAN can be assigned to each network. If a packet is received on an interface with this VLAN ID, then the package is assigned to the respective network, i.e. the network is only accessible for packets that come from the same VLAN. Packages coming from this network will be marked with this VLAN ID when being sent. A "0" stands for an untagged network (no VLAN). Caution: Changing the ID is very dangerous. It is very easy to lock yourself out of the device if you do not have access to the VLAN. Also note that this setting affects all of the traffic managed by this network. This includes all packets that are routed through this network.

Telnet path: /Setup/TCP-IP/Network-List

Possible values:

■ Max. 4,094

Default: 0

2.7.30.5 Interface

Here you select the interface that is to be allocated to the network. If a "random" choice is made here, then this network is accessible via any network interfaces that are not otherwise bound to a network.

Telnet path: /Setup/TCP-IP/Network-List

Possible values:

- Any
- 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: Any

2.7.30.6 Source check

This setting influences the address check by the firewall. "Loose" does not expect a return route, so any source address is accepted when the device is contacted. Thus the device can be accessed directly, as before. 'Strict', on the other hand, expects an explicit route if no IDS alarms are to be triggered.

Telnet path: /Setup/TCP-IP/Network-List

Possible values:

- Loose
- Strict

Default: Loose

2.7.30.7 Type

Use this item to choose the type of the network (Intranet or DMZ) or disable it.

Telnet path: /Setup/TCP-IP/Network-List

Possible values:

- Disabled
- Intranet
- DMZ

Default: Intranet

2.7.30.8 Routing tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received on this network are marked internally with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules. This tag also has an influence on the routes propagated by IP and on the hosts and groups visible to the NetBIOS proxy.

Telnet path: /Setup/TCP-IP/Network-List

Possible values:

- Maximum 65,535

Default: 0

2.7.30.9 Comment

You can enter a comment here.

Telnet path: /Setup/TCP-IP/Network-List

Possible values:

- Max. 64 characters

Default: Blank

2.8 IP router

This menu contains the settings for the IP router.

Telnet path: /Setup

2.8.1 Operating

Switches the IP router on or off.

Telnet path: /Setup/IP-Router

Possible values:

- Active
- Inactive

Default: Inactive

2.8.12 End WAN pool

Enter a range of IP addresses that should be assigned to users dialing into the device..

Each user is automatically assigned a free address from this range. As soon as a user disconnects from the device, the assigned address is freed up and is available for other users.

Telnet path: /Setup/IP-Router

Possible values:

- Valid IP address.

Default: 00.0.0

2.8.6 Send-ICMP-Redirect

This is where you can chose if ICMP redirects should be sent.

Telnet path: /Setup/IP-Router

Possible values:

- Active
- Inactive

Default: Active

2.8.14 Usage default timetable

Activates the time-dependent control of the default route. The default route is normally used to establish the connection to an Internet provider. The time control allows you to select various Internet providers depending on the time, for example to benefit from the most favorable provider at a certain time of day.

Telnet path: /Setup/IP-Router

Possible values:

- Active
- Inactive

Default: Inactive



To make use of this mechanism, a default route must have been specified in the routing table. The router specified in the default route is only used during those times that are not covered by the timed control table.

2.8.5 Proxy-ARP

This is where you can activate/deactivate the ARP mechanism . Use proxy ARP to integrate remote computers into your local network as if they were connected locally.

Telnet path: /Setup/IP-Router

Possible values:

- Active
- Inactive

Default: Inactive

2.8.11 Start-WAN-Pool

Enter a range of IP addresses that should be assigned to users dialing into the device..

Each user is automatically assigned a free address from this range. As soon as a user disconnects from the device, the assigned address is freed up and is available for other users.

Telnet path: /Setup/IP-Router

Possible values:

- Valid IP address.

Default: 00.0.0

2.8.22 WAN-Tag- Creation

WAN tag creation defines the source for the assignment of interface tags. Besides assignment via the firewall or direct assignment via the tag table, the interface tag can also be selected based on the effective routing table (static routing entries plus routes learned via RIP). The tag selected from this routing table is is for the route that matches both the remote site and the associated network. If the effective routing table contains more than one entry for a remote site with the same network, the smallest tag is used.

Telnet path: /Setup/IP-Router

Possible values:

- Manual: With this setting, the interface tags are determined solely by an entry in the tag table. The routing table has no significance in the assignment of interfaces tags.

- Auto: With this setting, the interface tags are determined initially by an entry in the tag table. If no matching entry is located there, the tag is determined based on the routing table.

Default: Manual:



The interface tags determined via the tag table and on the basis of the routing table can be overwritten with an appropriate entry in the firewall.

2.8.2 IP routing table

In this table you enter the remote sites which are to be used for accessing certain networks or stations.

Telnet path: /Setup/IP-Router

2.8.2.1 IP address

This is where you specify the destination address for this route. This can be an individual station that you wish to integrate into your network, or an entire network that you wish to couple with your own network.

Telnet path: /Setup/IP-Router/IP-Routing-Table

Possible values:

- Valid IP address.

Default: 00.0.0

2.8.2.2 IP netmask

Specify here the netmask associated with the IP addresses entered. If you only need to translate one single IP address, enter the netmask 255.255.255.255.

Telnet path: /Setup/IP-Router/IP-Routing-Table

Possible values:

- Valid IP address.

Default: 00.0.0

2.8.2.3 Peer or IP

Select the router that the packets for this route should be forwarded to.

Here you select the name of a remote site from the list of remote sites.

If this route is to lead to another station in the local network, simply enter the station's IP address.

Telnet path: /Setup/IP-Router/IP-Routing-Table

2.8.2.4 Distance

Enter the number of hops to this router. You do not normally need to set this value as it is managed by the router automatically.

Telnet path: /Setup/IP-Router/IP-Routing-Table

Possible values:

- 0 to 16

Default: 0

2.8.2.5.4 Masquerade

You can use IP masquerading to hide a logical network behind a single address (that of the router). If, for example, you have an Internet connection, you can use it to connect your entire network to the Internet. Almost all Internet providers usually have the remote device assign a dynamic IP address to your router when it establishes the connection. If your Internet provider has assigned fixed IP addresses, you can assign them

to the relevant connection in the IP parameter list. Select "Mask intranet and DMZ" if you wish to activate IP masquerading for all LAN interfaces. If you wish to assign fixed IP addresses to computers in the demilitarized zone (DMZ) and yet you still wish to activate IP masquerading for the computers on the other LAN interfaces (intranet), select "Intranet" (Mask intranet only).

Telnet path: /Setup/IP-Router/IP-Routing-Table

Possible values:

- No - IP masquerading switched off
- Yes - Intranet and DMZ masquerading (standard)
- Intranet - Intranet masquerading only

Default: No - IP masquerading switched off

2.8.2.6 Operating

Specify the switch status here. The route can be activated and either always propagated via RIP or only propagated via RIP when the destination network can be reached.

Telnet path: /Setup/IP-Router/IP-Routing-Table

Possible values:

- Yes: The route is activated and will always be propagated by RIP (sticky).
- Semi: The route can be activated and is propagated via RIP when the destination network can be reached (conditional).
- No: The route is off.

Default: Yes: The route is activated and will always be propagated by RIP (sticky)

2.8.2.7 Comment

This field is available for comments.

Telnet path: /Setup/IP-Router/IP-Routing-Table

Possible values:

- Max. 64 characters

2.8.2.8 Routing tag

If you specify a routing tag for this route, then the route will be used exclusively for packets given the same tag by the firewall or arriving from a network with the corresponding interface tag.

Telnet path: /Setup/IP-Router/IP-Routing-Table

Possible values:

- Maximum 65535

Default: 0



It follows that the use of routing tags only makes sense in combination with corresponding, decorative rules in the firewall or tagged networks.

2.8.7 Routing method

This menu contains the configuration of the routing methods used by your IP router.

Telnet path: /Setup/IP-Router

2.8.7.2 ICMP-Routing-Method

Specify if the router should transmit secure ICMP packets.

Telnet path: /Setup/IP-Router

Possible values:

- Normal
- Secured

Default: Normal**2.8.7.6 Route internal services**

This is where you select whether the internal services are to be directed via the router.

Telnet path: /Setup/IP-Router/Routing-Method**Possible values:**

- Yes: Packets for internal services are directed via the router.
- No: Packets are returned straight to the sender.

Default: No

You should treat the internal services VPN and PPTP specially since routing all packets without exception will result in performance loss. The device only forwards the initial packets sent by these services to the router while the connection is being established if you activate this option. Further packets are forwarded to the next port.

2.8.7.4 L2-L3 tagging

Specify what should happen with DiffServ layer 2 tags.

Telnet path: /Setup/IP-Router/Routing-Method**Possible values:**

- No - Ignore
- Yes - Copy to layer 3
- Auto - Copy automatically

Default: Ignore**2.8.7.5 L3-L2 tagging**

Specify if DiffServ layer 3 tags should be copied to layer 2.

Telnet path: /Setup/IP-Router**Possible values:**

- Active
- Inactive

Default: Inactive**2.8.7.1 Routing method**

Analysis of ToS or DiffServ fields.

Telnet path: /Setup/IP-Router**Possible values:**

- Normal: The TOS/DiffServ field is ignored.
- Type-of-service: The TOS/DiffServ field is regarded as a TOS field; the bits 'low delay' and 'high reliability' will be evaluated.
- DiffServ: The TOS/DiffServ field is regarded as a DiffServ field and evaluated as follows.
- CSx (including CS0 = BE): Normal transmission
- AFxx: Secure transmission

- EF: Preferred transmission

2.8.7.3 SYN/ACK speedup

Specify if TCP SYN and ACK packets should be given preferential treatment when forwarding.

Telnet path: /Setup/IP-Router/Routing-Method

Possible values:

- Active
- Inactive

Default: Active

2.8.8 RIP

This menu contains the RIP configuration for your IP router.

Telnet path: /Setup/IP-Router

2.8.8.2 R1 mask

This setting is only required if you selected RIP-1 as RIP support. It affects how network masks are formed for routes learned on the basis of RIP.

Telnet path: /Setup/IP-Router/RIP

Possible values:

- Class
- Address
- Class + address

Default: Class

2.8.8.4 WAN sites

Here you configure the WAN-side RIP support separately for each remote site.

Telnet path: /Setup/IP-Router/RIP

2.8.8.4.1 Peer

Name of the remote station from which WAN RIP packets are to be learned.

Telnet path: /Setup/IP-Router/RIP/WAN-Sites

Possible values:

- Select from the list of defined peers.

Default: Blank

Special values: Multiple remote sites can be configured in one entry by using * as a place holder. If for example multiple remote stations are to propagate their networks via WAN RIP, while the networks for all other users and branch offices are defined statically, the appropriate remote stations can be given names with the prefix "RIP_". To configure all of the remote stations, the WAN RIP table requires just a single entry for remote station "RIP_*".

2.8.8.4.10 RX filter

Here you define the filter to be used when receiving RIP packets.

Telnet path: /Setup/IP-Router/RIP/WAN-Sites

Possible values:

- Select from the list of defined RIP filters (max. 16 characters).

Default: Blank

2.8.8.4.11 TX filter

Here you define the filter to be used when sending RIP packets.

Telnet path: /Setup/IP-Router/RIP/WAN-Sites

Possible values:

- Select from the list of defined RIP filters (max. 16 characters).

Default: Blank

2.8.8.4.12 RIP send

Specify whether RIP is to be propagated on the WAN routes. The RIP type must be set for this.

LANconfig description: Send RIP to this remote device.

Telnet path: /Setup/IP-Router/RIP/WAN-Sites/RIP-Send

LANconfig path: IP router/WAN RIP

Possible values:

- No
- Yes

Possible LANconfig values:

- Off
- On

Default: No/Off

2.8.8.4.2 RIP type

The RIP type details the RIP version with which the local routes are propagated.

Telnet path: /Setup/IP-Router/RIP/WAN-Sites

Possible values:

- Off
- RIP-1
- RIP-1 compatible:
- RIP 2

Default: Off

2.8.8.4.3 RIP accept

The column RIP accept lists whether RIP from the WAN is to be accepted. The RIP type must be set for this.

Telnet path: /Setup/IP-Router/RIP/WAN-Sites

Possible values:

- On
- Off

Default: Off

2.8.8.4.4 Masquerade

The column Masquerade lists whether or not masquerading is performed on the connection and how it is carried out. This entry makes it possible to start WAN RIP even in an empty routing table.

Telnet path: /Setup/IP-Router/RIP/WAN-Sites

Possible values:

- Auto: The masquerade type is taken from the routing table. If there is no routing entry for the remote site, then masquerading is not performed.
- To: All connections are masqueraded.
- Intranet: IP masquerading is used for connections from the intranet, connections from the DMZ pass through transparently.

Default: On

2.8.8.4.5 Default routing tag

The column Default tag lists the valid "Default routing tag" for the WAN connection. All untagged routes are tagged with this tag when sent on the WAN.

Telnet path: /Setup/IP-Router/RIP/WAN-Sites

Possible values:

- Maximum 65,535

Default: 0

2.8.8.4.6 Routing tag list

The column Routing tags list details a comma-separated list of the tags that are accepted on the interface. If this list is empty, then all tags are accepted. If at least one tag is in the list, then only the tags in this list are accepted. When sending tagged routes on the WAN, only routes with valid tags are propagated.

All learned routes from the WAN are treated internally as untagged routes and propagated on the LAN with the default tag (0). In the WAN, they are propagated with the tag with which they were learned.

Telnet path: /Setup/IP-Router/RIP/WAN-Sites

Possible values:

- Comma-separated list with max. 33 characters

Default: Blank

2.8.8.4.7 Poisoned reverse

Poisoned reverse prevents the formation of routing loops. An update is sent back to the router that propagated the route to inform it that the network is unreachable at the associated interface.

However, this has a significant disadvantage over WAN connections: The central location transmits a high number of routes which would then suffer from route poisoning, so leading to a heavy load on the available bandwidth. For this reason, poisoned reverse can be manually activated for every LAN/WAN interface.

Telnet path: /Setup/IP-Router/RIP/WAN-Sites

Possible values:

- On
- Off

Default: Off

2.8.8.4.8 RFC2091

Other than in the LAN, WAN bandwidth limitations may make regular updates every 30 seconds undesirable. For this reason, RFC 2091 requires that routes are transmitted to the WAN once only when the connection is established. After this, updates only are transmitted (triggered updates).

Because updates are explicitly requested here, broadcasts or multicasts are not to be used for delivering RIP messages. Instead, the subsidiary device must be statically configured with the IP address of the next available router at the central location. Due to these requests, the central router knows which subsidiary routers it has received update requests from; it then sends any messages on route changes directly to the subsidiary device.

Telnet path: /Setup/IP-Router/RIP/WAN-Sites

Possible values:

- On
- Off

Default: Off



In a central gateway, the setting "RFC 2091" can always be off and the "Gateway" entry always set to 0.0.0.0 because the central gateway always considers the gateway as specified at the subsidiary.

2.8.8.4.9 Gateway

IP address of the nearest available router in the context of RFC 2091.

Telnet path: /Setup/IP-Router/RIP/WAN-Sites

Possible values:

- Valid IP address.

Default: 00.0.0

Special values: If 0.0.0.0 is entered, the gateway address is determined from PPP negotiation.



In a router at the central location, RFC 2091 can be switched off and the gateway can remain on 0.0.0.0 because the central location always observes the requests from the subsidiaries.



The LANCOM device automatically reverts to standard RIP if the gateway indicated does not support RFC 2091.



In a central gateway, the setting "RFC 2091" can always be off and the "Gateway" entry always set to 0.0.0.0 because the central gateway always considers the gateway as specified at the subsidiary.

2.8.8.5 LAN sites

This table is used to adjust RIP settings and to select the network that they apply to.

Telnet path: /Setup/IP-Router/RIP

2.8.8.5.1 Network name

Select here the name of the network to which the settings are to apply.

Telnet path: /Setup/IP-Router/RIP/LAN-Sites

Possible values:

- Intranet
- DMZ

Default: Blank

2.8.8.5.10 RX filter

Specify here the filter to be applied when receiving (RX) RIP packets.

Telnet path: /Setup/IP router/RIP/LAN-Sites/Rx-Filter

Possible values:

- Max. 16 alphanumerical characters

Default: Blank



You must first define the filter in the RIP filter list in order to use it here.

2.8.8.5.11 TX filter

Specify here the filter to be applied when sending (TX) RIP packets.

Telnet path: /Setup/IP router/RIP/LAN-Sites/Tx-Filter

Possible values:

- Max. 16 alphanumerical characters

Default: Blank



You must first define the filter in the RIP filter list in order to use it here.

2.8.8.5.12 RIP send

Specify here whether routes should be propagated in this network. The RIP type must also be set.

Telnet path: /Setup/IP router/RIP/LAN-Sites/RIP-Send

Possible values:

- No
- Yes

Default: No

2.8.8.5.2 RIP type

Specify whether the router should support IP-RIP or not. IP-RIP can be used to exchange routing information between individual stations automatically.

Telnet path: /Setup/IP-Router/RIP/LAN-Sites

Possible values:

- Off
- RIP-1
- RIP-1 compatible:
- RIP-2

Default: Off

2.8.8.5.3 RIP accept

Specify here whether routes from this network should be learned or not.

Telnet path: /Setup/IP-Router/RIP/LAN-Sites

Possible values:

- Active
- Inactive

Default: Inactive

2.8.8.5.4 Propagate

This option defines whether the associated network is to be propagated to other networks.

Telnet path: /Setup/IP-Router/RIP/LAN-Sites

Possible values:

- Active
- Inactive

Default: Inactive

2.8.8.5.5 Default routing tag

Enter a value here for the default routing tag that is valid for the selected interface. Routes that have the interface tag set will be propagated on this interface with the default routing tag. Routes learned by the interface that have this default routing tag set will be added to the RIP table with the interface tag. In addition, unmarked routes (i.e. routes with tag '0') will not be propagated on this interface unless the interface itself has the tag '0'.

Telnet path: /Setup/IP-Router/RIP/LAN-Sites

Possible values:

- 0 to 65535

Default: 0

2.8.8.5.6 Routing tag list

This field contains a comma-separated list of routing tags that are accepted by this interface. If this list is empty, then all routes are accepted irrespective of their routing tags. If the list contains at least one tag, then only the tags in this list are accepted. Similarly, when marked routes are being sent, only routes with permitted tags (i.e. those listed here) are forwarded. The routing tag list corresponds insofar to the WAN RIP list with the difference that any realization using standard routing is also taken into account. This means for example that, in the case of an interface tag '1' and the standard routing tag '0', the tag '0' has to be included in the routing tag list because it is internally changed to tag '1' when it is received. When transmitted, the internal tag '1' is converted into the external tag '0'. This measure is necessary in order for a virtualized router to be able to work together with other routers in the LAN that do not support tagged routes.

Telnet path: /Setup/IP-Router/RIP/LAN-Sites

Possible values:

- Max. 33 characters

Default: Blank

2.8.8.5.7 Poisoned reverse

Poisoned reverse prevents the formation of routing loops. An update is sent back to the router that propagated the route to inform it that the network is unreachable at the associated interface.

However, this has a significant disadvantage over WAN connections: The central location transmits a high number of routes which would then suffer from route poisoning, so leading to a heavy load on the available bandwidth. For this reason, poisoned reverse can be manually activated for every LAN/WAN interface.

Telnet path: /Setup/IP-Router/RIP/LAN-Sites

Possible values:

- Active
- Inactive

Default: Inactive

2.8.8.6 Parameter

The routing information protocol (RIP) regularly provides neighboring routers with updates on the available networks and the associated metrics (hops). RIP uses various timers to control the exchange of routing information.

Telnet path: /Setup/IP-Router/RIP

2.8.8.6.4 Flush

If a route in a router is not updated before the flush interval expires, then the route is deleted from the dynamic routing table.

Telnet path: /Setup/IP-Router/RIP/Parameter

Possible values:

- 0 to 99 as multiples of the update interval

Default: 10

2.8.8.6.2 Holddown

The holddown interval defines how many update intervals pass before a route from router A which is no longer being propagated is replaced by an inferior route from router B.

The LANCOM will only accept a route from the same router that propagated the original route until the hold-down interval expires. Within this period, the LANCOM device only accepts a route from another router if it is better than the former route.

Telnet path: /Setup/IP-Router/RIP/Parameter

Possible values:

- 0 to 99 as multiples of the update interval

Default: 4

2.8.8.6.3 Invalidate

The invalidate interval defines the number of update intervals before a route is marked as invalid (unavailable) when it stops being propagated by the router that originally reported it.

If the LANCOM device learns of an equivalent or better route from another router within this time period, then this will be used instead.

Telnet path: /Setup/IP-Router/RIP/Parameter

Possible values:

- 0 to 99 as multiples of the update interval

Default: 6

2.8.8.6.6 Max hopcount

In some scenarios it may be desirable to use a larger maximum hop count than that provided for by RIP (16). This value can be adapted with the parameter Max Hopcount.

Telnet path: /Setup/IP-Router/RIP/Parameter

Possible values:

- 16 to 99

Default: 16

2.8.8.6.7 Routes per frame

The number of routes that can be propagated in a single packet.

Telnet path: /Setup/IP-Router/RIP/Parameter

Possible values:

- 1 to 90

Default: 25

2.8.8.6.1 Update

The time between two regular updates. A random value of +/- 5 seconds is always added to this value.

Telnet path: /Setup/IP-Router/RIP/Parameter

Possible values:

- 0 to 99 seconds

Default: 30 seconds

2.8.8.6.5 Update delay

With a triggered update, changes to the metrics are immediately reported to the neighboring router. The system does not wait until the next regular update. An update delay stops faulty configurations from causing excessive update messages.

The update delay starts as soon as the routing table, or parts of it, are propagated. As long as this delay is running, new routing information is accepted and entered into the table but it is not reported any further. The router actively reports its current entries only after expiry of this delay.

The value set here sets the upper limit for the delay – the actual delay is a random value between one second and the value set here.

Telnet path: /Setup/IP-Router/RIP/Parameter

Possible values:

- 0 to 99 seconds

Default: 5

2.8.8.7 Filter

Routes learned from RIP can be filtered by their routing tag according to the settings for LAN and WAN RIP. Routes can additionally be filtered by specifying network addresses (e.g. "Only learn routes in the network 192.168.0.0/255.255.0.0"). First of all a central table is used to define the filters that can then be used by entries in the LAN and WAN RIP table.

Filters defined in the filter table can be referenced in the columns for RX filter and TX filter in the LAN RIP and WAN RIP tables. RX defines the networks from which routes can be learned or blocked, and TX defines the networks to which propagation should be allowed or blocked.

Telnet path: /Setup/IP-Router/RIP

2.8.8.7.1 Name

Name of the filter.

Telnet path: /Setup/IP-Router/RIP/Filter

Possible values:

- 18 characters



The hash symbol # can be used to combine multiple entries into a single filter. Taken together, the entries LAN#1 and LAN#2 make up a filter "LAN" that can be called from the RIP table.

2.8.8.7.2 Filter

Comma-separated list of networks that are to be accepted (+) or rejected (-).

Telnet path: /Setup/IP-Router/RIP/Filter

Possible values:

- 64 characters from ,+/-/0123456789.



The plus-sign for accepted networks is optional.



Filtering by routing tags is unaffected, i.e. if a tag for a route indicates that it is not to be learned or propagated, then this cannot be forced by means of the filter table.

2.8.8.8 Best routes

In large networks a destination network may be reachable via several gateways. If all these gateways propagate their routes using RIP the device will learn several routes to the same destination. The preferred routes are stored in the "Best Routes" table. This table contains the following entries:

- IP address
- IP netmask
- Rtg tag
- Gateway
- Distance
- Time
- Peer
- Port
- VLAN-ID
- Network name

Telnet path: /Setup/IP-Router/RIP/Best-Routes

2.8.8.9 All routes

In large networks a destination network may be reachable via several gateways. If all these gateways propagate their routes using RIP the device will learn several routes to the same destination. These routes are stored in the "All Routes" table. This table contains the following entries:

- IP address
- IP netmask
- Rtg tag
- Gateway
- Distance
- Time
- Peer
- Port
- VLAN-ID
- Network name

Telnet path: /Setup/IP-Router/RIP/All-Routes

2.8.9 1-N-NAT

This menu contains the configuration of 1-N-NAT for your IP router.

Telnet path: /Setup/IP-Router

2.8.9.7 Fragment aging seconds

If an IP packet cannot be fully desmasked because fragments are missing, this time in seconds determines when the incomplete fragments are dropped.

Telnet path: /Setup/IP-Router/1-N-NAT/

Possible values:

■ 1 to 255

Default: 5

2.8.9.6 Fragments

This setting controls the firewall's behavior regarding fragmented IP packets.

Telnet path: /Setup/IP-Router/1-N-NAT/

Possible values:

■ Filter: Fragments are always rejected (filtered).

■ Route: The fragments are demasked. However, the fragments must be received in their original order. In addition, this settings allows only the individual fragments to be checked by the firewall, and not the entire IP packet.

■ Reassemble: The fragments are stored temporarily until the IP packet can be reassembled in full. The fragments may be received in any order. The firewall also checks the reassembled IP packet.

Default: Reassemble

2.8.9.3 ICMP aging seconds

Specify here how long an IPSec connection is inactive before the corresponding entry in the masquerading table is deleted.

Telnet path: /Setup/IP-Router/1-N-NAT/

Possible values:

■ 0 to 65,535

Default: 10 seconds

2.8.9.10 ID spoofing

NAT replaces the packet IDs in the outbound packets (ID spoofing). This enables fragmented packets to be transmitted and it stops information on the internal network (packet IDs) from being leaked to the outside. If AH is being used, this procedure should be avoided as the packet IDs are required by AH. For AH to function properly, ID spoofing can be deactivated here.

Telnet path: /Setup/IP-Router/1-N-NAT/

Possible values:

■ Yes

■ No

Default: Yes

2.8.9.8 IPSec aging seconds

Specify here how long an IPSec connection is inactive before the corresponding entry in the masquerading table is deleted.

Telnet path: /Setup/IP-Router/1-N-NAT/

Possible values:

■ 0 to 65,535

Default: 2000

2.8.9.1 TCP aging seconds

Specify here how long an IPsec connection is inactive before the corresponding entry in the masquerading table is deleted.

Telnet path: /Setup/IP-Router/1-N-NAT/

Possible values:

■ 0 to 65,535

Default: 300 seconds

2.8.9.2 UDP aging seconds

Specify here how long an IPsec connection is inactive before the corresponding entry in the masquerading table is deleted.

Telnet path: /Setup/IP-Router/1-N-NAT/

Possible values:

■ 0 to 65,535

Default: 20 seconds

2.8.9.4 Service table

If you wish to make certain services or stations accessible from outside of your network (e.g. a web server), enter these services and stations in this table.

Telnet path: /Setup/IP-Router/1-N-NAT/

2.8.9.4.1 D-port from

Specify the port of the desired service here.

Telnet path: /Setup/IP-Router/1-N-NAT/Service-Table

Possible values:

■ Maximum 65,535

Default: 0

2.8.9.4.2 Intranet address

Enter the address of the computer in the intranet providing the service.

Telnet path: /Setup/IP-Router/1-N-NAT/Service-Table

Possible values:

■ Valid IP address.

Default: 00.0.0

2.8.9.4.3 D-port to

Specify the port of the desired service here.

Telnet path: /Setup/IP-Router/1-N-NAT/Service-Table

Possible values:

■ Maximum 65,535

Default: 0

2.8.9.4.4 Map port

Port used for forwarding the packet.

Telnet path: /Setup/IP-Router/1-N-NAT/Service-Table

Possible values:

■ Maximum 65,535

Default: 0

2.8.9.4.5 Active

You can set this entry temporarily inactive without having to delete it.

Telnet path: /Setup/IP-Router/1-N-NAT/Service-Table

Possible values:

- Active
- Inactive

Default: Active

2.8.9.4.6 Comment

This field is available for comments.

Telnet path: /Setup/IP-Router/1-N-NAT/Service-Table

Possible values:

- Max. 64 characters

Default: /

2.8.9.4.7 Peer

Remote site which is valid for this entry.

Telnet path: /Setup/IP-Router/1-N-NAT/Service-Table

Possible values:

- Select from the list of defined peers.

2.8.9.4.8 Protocol

Here you define which protocol the dataset applies to.

Telnet path: /Setup/IP-Router/1-N-NAT/Service-Table

Possible values:

- TCP
- UDP
- TCP+UDP

Default: TCP+UDP

2.8.9.4.9 WAN address

Here you define which WAN address the dataset applies to. Where more than one static IP address is available, specifying this address enables a targeted port forwarding to be achieved for this address. If the address 0.0.0.0 is specified, then the address assigned to the connection will continue to be used.

Telnet path: /Setup/IP-Router/1-N-NAT/Service-Table

Possible values:

- Valid IP address.

Default: 00.0.0

2.8.9.5 Table-1-N-NAT

The 1-N-NAT table shows the masked connections.

Telnet path: /Setup/IP-Router/1-N-NAT/

2.8.9.5.1 Intranet address

Shows the internal IP address of the station to which a masked connection has been stored.

Telnet path: /Setup/IP-Router/1-N-NAT/Table-1-N-NAT

Possible values:

- Valid IP address.

2.8.9.5.2 Source port

Source port of the masked connection.

Telnet path: /Setup/IP-Router/1-N-NAT/Table-1-N-NAT

2.8.9.5.3 Protocol

Protocol (UDP/TCP) used by the masked connection.

Telnet path: /Setup/IP-Router/1-N-NAT/Table-1-N-NAT

2.8.9.5.4 Timeout

Lease period for the masked connection in seconds (set under TCP aging, UDP aging or ICMP aging).

Telnet path: /Setup/IP-Router/1-N-NAT/Table-1-N-NAT

2.8.9.5.5 Handler

Handler required for masking, e.g. FTP

Telnet path: /Setup/IP-Router/1-N-NAT/Table-1-N-NAT

2.8.9.5.6 Remote address

Remote IP address that the masked connection was connected to.

Telnet path: /Setup/IP-Router/1-N-NAT/Table-1-N-NAT

Possible values:

- Valid IP address.

2.8.9.9 IPSec table

The IPSec table displays the masked IPSec connections, including some of the connection parameters.

Telnet path: /Setup/IP-Router/1-N-NAT/

2.8.9.9.1 Remote address

Address of the remote VPN gateway

Telnet path: /Setup/IP-Router/1-N-NAT/IPSec-Table

Possible values:

- Valid IP address.

2.8.9.9.10 Flags

Flags that describe the state of the connection:

0x01 Connection is inverse masqueraded

0x02 Connection waiting for SPI

0x04 Other connections waiting for SPI

0x08 Aggressive mode connection

0x10 NAT-Traversal connection

0x20 Session recovery

Telnet path: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.11 CO

Connect timeout. Runs straight after the entry is created. If no SA is negotiated within 30 seconds (i.e. no ESP packet is sent or received) the entry is deleted again

Telnet path: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.12 NL

Local notification timeout. This timer is started when an IKE notification is received from the local VPN gateway. The entry is deleted if no IKE or ESP packet is received from the remote site within 30 seconds

Telnet path: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.13 NR

Remote notification timeout. Corresponds to the local notification timeout, except that in this case the notification was received from the remote VPN gateway.

Telnet path: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.14 DP

DPD timeout: This timer is started when a DPD packet is received from one site. If no DPD packet is received from the other site within 30 seconds the entry is removed.

Telnet path: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.2 Local address

Address of the local VPN gateway (generally a VPN client in the local network)

Telnet path: /Setup/IP-Router/1-N-NAT/IPSec-Table

Possible values:

- Valid IP address.

2.8.9.9.3 Rc-hi

The most significant 32 bits of the IKE cookie of the remote VPN gateway

Telnet path: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.4 Rc-lo

The least significant 32 bits of the IKE cookie of the remote VPN gateway

Telnet path: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.5 Lc-hi

The most significant 32 bits of the IKE cookie of the local VPN gateway

Telnet path: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.6 Lc-lo

The least significant 32 bits of the IKE cookie of the local VPN gateway

Telnet path: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.7 Remote SPI

SPI used by the remote VPN gateway

Telnet path: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.8 Local SPI

SPI used by the local VPN gateway

Telnet path: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.9 Timeout

Timeout in seconds until the entry is deleted. The value is divided into IPsec aging seconds. The default value is 2000 seconds

Telnet path: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.10 Firewall

This menu contains the firewall configuration.

Telnet path: /Setup/IP-Router

2.8.10.10 Admin e-mail

If you wish to be notified of predefined events (DoS, IDS or when limits are exceeded) you must specify a valid e-mail address here.

Telnet path: /Setup/IP-Router/Firewall

Possible values:

- Max. 255 characters



For e-mail messaging, you have to enter the necessary settings into the main group "Log & Tace" in the subsection "SMTP".

2.8.10.11 Operating

You can switch the entire firewall on or off here. The firewall inspects and counts every single incoming and outgoing packet. Depending on the protocol in question, it temporarily opens the channels that are required by a local station for processing a request. Furthermore individual networks, peers, services or protocols can be preferred, limited or blocked.

Telnet path: /Setup/IP-Router/Firewall

Possible values:

- Active
- Inactive

Default: Active



Defined VPN rules continue to be observed even with the firewall switched off.

2.8.10.16 Authentication port

Hiding TCP or UDP ports will cause problems on masked connections where so-called 'authenticate' or 'ident' queries, as used by some mail and news servers to request additional information from users, are no longer rejected correctly. These servers then time out, resulting in considerable delays in the delivery of mail or news. In order to overcome this problem when stealth mode is switched on, stealth mode is deactivated temporarily for the port in question. The firewall recognizes that the internal station's wish to establish contact with a mail (SMTP, POP3, IMAP2) or news server (NNTP) and opens the port for 20 seconds. You can use this option to suppress the temporary deactivation of stealth mode for the authentication port.

Telnet path: /Setup/IP-Router/Firewall

Possible values:

- Active
- Inactive

Default: Inactive

2.8.10.9 DoS action

This is where you can specify what action should be taken with packets that activate or exceed the trigger. You can transfer the packets, drop them uncommented or reject them using ICMP reject (i.e. the sender is informed).

Telnet path: /Setup/IP-Router/Firewall

Possible values:

- Transmit
- Drop
- Reject

Default: Drop

2.8.10.13 IDS action

This is where you can specify what action should be taken with packets that activate or exceed the trigger. You can transfer the packets, drop them uncommented or reject them using ICMP reject (i.e. the sender is informed).

Telnet path: /Setup/IP-Router/Firewall

Possible values:

- Transmit
- Drop
- Reject

Default: Drop

2.8.10.8 Max. half-open connections

Denial-of-Service attacks take advantage of inherent weaknesses in the TCP/IP protocol in combination with poor implementations. Attacks which target these inherent weaknesses include SYN Flood and Smurf. Attacks which target erroneous implementations include those operating with erroneously fragmented packets (e.g. Teardrop) or with fake sender addresses (e.g. Land). Your device detects most of these attacks and reacts with appropriate countermeasures.

Telnet path: /Setup/IP-Router/Firewall

Possible values:

- 100 to 9999

Default: 100

2.8.10.14 Ping block

A controversial method of increasing security is to conceal the router by not responding to ping and trace-route requests (ping blocking). This is controversial because the failure to answer can also betray the existence of a device. If there truly is no device present, the previous router will respond to the relevant packets with 'undeliverable' as it is unable to deliver them. However, if the previous router no longer responds with a corresponding rejection, the packet is 'deliverable' and, regardless of the recipient's subsequent behavior, is most certainly present. It is not possible to simulate the behavior of the previous router without keeping your device offline or switching it off (and thus making it unreachable for the services you yourself request).

Telnet path: /Setup/IP-Router/Firewall

Possible values:

- Off
- Always
- WAN
- Default route

Default: Off

2.8.10.12 Port scan threshold

Intrusion detection system (IDS). Your device detects most unauthorized intrusion attempts and can respond with countermeasures that can be configured here.

Telnet path: /Setup/IP-Router/Firewall

Possible values:

- 50 to 9999

Default: 50

2.8.10.17 Deny session recover

The firewall opens appropriate channels for each session initiated and its associated connections (e.g. FTP with control and data connections) for a certain period. If there is no communication over the connection for a defined period of time (setting in the IP router masquerading), then the session is considered to be ended and the channels associated with the connections are closed. Selecting 'session recover' determines the behavior of the firewall when receiving packets which appear to belong to an earlier session. The packets are dropped or it is assumed that a session existed but that no communication took place for too long. In this case, an equivalent session can be reestablished. The latter behavior can in general be allowed or forbidden. Denial of a session can be restricted to the default route or to WAN sessions.

Telnet path: /Setup/IP-Router/Firewall

Possible values:

- Off - always permitted
- Always - always forbidden
- WAN - forbidden over WAN
- Default-route - forbidden on default route

Default: Default-route - forbidden on default route

2.8.10.15 Stealth mode

A controversial method of increasing security is to conceal the router by not conforming to standards and rejecting TCP and UDP requests, but by ignoring them (stealth mode). This is controversial because the failure to answer can also betray the existence of a device. If there truly is no device present, the previous router will respond to the relevant packets with 'undeliverable' as it is unable to deliver them. However, if the previous router no longer responds with a corresponding rejection, the packet is 'deliverable' and, regardless of the recipient's subsequent behavior, is most certainly present. It is not possible to simulate the behavior of the previous router without keeping your device offline or switching it off (and thus making it unreachable for the services you yourself request).

Telnet path: /Setup/IP-Router/Firewall

Possible values:

- Off
- Always
- WAN
- Default route

Default: Off

2.8.10.1 Objects

Elements/objects that are to be used in the firewall rules table are defined in the objects table. Objects can be:

- Individual computers (MAC or IP address, hostname)
- Complete networks
- Protocols
- Services (ports or port areas, e.g. HTTP, Mail&News, FTP, ...)

These elements can be combined and hierarchically structured in any way. For example, objects for the TCP and UDP protocols can be defined first. Building upon this, objects can subsequently be created, for example, for FTP (= TCP + ports 20 and 21), HTTP (= TCP + port 80) and DNS (= TCP, UDP + port 53). These can in turn be combined into one object that contains all the definitions of the individual objects.

Telnet path: /Setup/IP-Router/Firewall

2.8.10.1.1 Name

Specify here a unique name for this object.

Telnet path: /Setup/IP-Router/Firewall/Objects

Possible values:

- Max. 32 characters

Default: Blank

2.8.10.1.2 Description

Stations and services can be defined in the objects table.

Telnet path: /Setup/IP-Router/Firewall/Objects

Possible values:

- %L: Local network
- %H: Remote sites – name must be in DSL/ISDN/PPTP or VPN remote site list
- %D: Host name – please note information on host names
- %E: MAC address – 00:A0:57:01:02:03
- %A: IP address – %A10.0.0.1, 10.0.0.2; %A0 (all addresses)
- %M: Network mask – %M255.255.255.0
- %P: Protocol (TCP/UDP/ICMP, etc.) – %P6 (for TCP)
- %S: Service (port) – %S20-25 (for ports 20 to 25)

Default: Blank



For configuration from the console (Telnet or terminal application), the combined parameters (port, destination, source) must be enclosed with quotation marks ("). Host names can only be used if the LANCOM can resolve the names into IP addresses. To this end, the LANCOM device must have learned the names via DHCP or NetBIOS, or the assignment must be entered statically in the DNS or IP routing table. One entry in the IP routing table can assign a complete network to a host name.

2.8.10.2 Rules

The rules table links various pieces of information on a firewall rule. The rule contains the protocol to be filtered, the source, the destination and the firewall action to be executed. For every firewall rule there is also an on/off switch, a priority, the option to link with other rules, and activation of the rule for VPN connections.

LCOS uses a special syntax to define firewall rules. This syntax enables the representation of complex inter-relationships for the testing and handling of data packets in the firewall with just a few characters. The rules are defined in the rules table. Pre-defined objects can be stored in two further tables so that frequently used objects do not have to be entered into the syntax every time:

The firewall actions are stored in the action table

The object table holds the stations and services

The definition of firewall rules can contain entries in the object table for protocols, services, stations and the action table for firewall actions, and also direct definitions in the appropriate LCOS syntax (e.g. %P6 for TCP).

Telnet path: /Setup/IP-Router/Firewall



The objects from these tables can be used for rule definition, although this is not compulsory. They merely simplify the use of frequently used objects. For direct input of level parameters in the LCOS syntax, the same rules apply as specified in the following sections for protocols, source/destination and firewall actions.

2.8.10.2.1 Name

Specify here a unique name for this firewall rule.

Telnet path: /Setup/IP-Router/Firewall/Rules

Possible values:

- Max. 32 characters

Default: Blank

2.8.10.2.10 Active

Switches the rule on/off.

Telnet path: /Setup/IP-Router/Firewall/Rules

Possible values:

- Yes
- No

Default: Yes**2.8.10.2.11 VPN rule**

Activates the rule for creating VPN rules.

Telnet path: /Setup/IP-Router/Firewall/Rules**Possible values:**

- Yes
- No

Default: No**2.8.10.2.12 Stateful**

When this option is enabled, a check is performed as to whether a connection is being established correctly. Erroneous packets are discarded whilst the connection is being established. If this option is disabled, all packets for which this rule applies are accepted.

Furthermore, this option is enabled for the automatic protocol recognition for FTP, IRC, PPTP necessary to be able to open a port in the firewall for each data connection.

The test for portscans/SYN flooding is also enabled/disabled with this option. This can exclude particular, heavily-frequented servers from the test, meaning that limits for half-open connections (DOS) or port requests (IDS) do not have to be set so high that they effectively become useless.

Telnet path: /Setup/IP-Router/Firewall/Rules**Possible values:**

- Yes
- No

Default: Yes**2.8.10.2.13 Comment**

Comment for this entry.

Telnet path: /Setup/IP-Router/Firewall/Rules**Possible values:**

- Max. 64 characters

Default: Blank**2.8.10.2.14 Routing tag**

Routing tag for the rule.

Telnet path: /Setup/IP-Router/Firewall/Rules**Possible values:**

- 0 to 65535

Default: 0**2.8.10.2.2 Protocol**

Specification of the protocols for which this entry is to apply.

Telnet path: /Setup/IP-Router/Firewall/Rules**Possible values:**

- Direct entry in LCOS syntax as described in the object table.
- Link to an entry of the object table.

Default: Blank**2.8.10.2.3 Source**

Specification of the source stations for which this entry is to apply.

Telnet path: /Setup/IP-Router/Firewall/Rules

Possible values:

- Direct entry in LCOS syntax as described in the object table.
- Link to an entry of the object table.

Default: Blank**2.8.10.2.4 Destination**

Specification of the destination stations for which this entry is to apply.

Telnet path: /Setup/IP-Router/Firewall/Rules**Possible values:**

- Direct entry in LCOS syntax as described in the object table.
- Link to an entry of the object table.

Default: Blank**2.8.10.2.7 Action**

Action to be run if the firewall rule applies to a packet.

Telnet path: /Setup/IP-Router/Firewall/Rules**Possible values:**

- Direct entry in LCOS syntax as described in the action table.
- Link to an entry of the action table.

Default: Blank**2.8.10.2.8 Linked**

Links the rule to other rules.

Telnet path: /Setup/IP-Router/Firewall/Rules**Possible values:**

- Yes
- No

Default: No**2.8.10.2.9 Priority**

Priority of the rule.

Telnet path: /Setup/IP-Router/Firewall/Rules**Possible values:**

- 0 to 255

Default: Blank**2.8.10.3 Filter list**

The filter list is generated from the rules in the firewall. The filters it contains are static and can only be changed when firewall rules are added, edited or deleted..

Telnet path: /Setup/IP-Router/Firewall**2.8.10.3.1 Index**

Index for this entry in the list.

Telnet path: /Setup/IP-Router/Firewall/Filter-List**2.8.10.3.10 D-End**

Finish address of range of destination IP addresses whose data packets are processed by this entry.

Telnet path: /Setup/IP-Router/Firewall/Filter-List**2.8.10.3.11 Action**

Action performed for the data packets processed by this entry.

Telnet path: /Setup/IP-Router/Firewall/Filter-List

2.8.10.3.13 Source MAC

Source MAC address for data packets processed by this entry.

Telnet path: /Setup/IP-Router/Firewall/Filter-List

2.8.10.3.14 Destination MAC

Destination MAC address for data packets processed by this entry.

Telnet path: /Setup/IP-Router/Firewall/Filter-List

2.8.10.3.15 Linked

Indicates whether further firewall rules are applied after this action.

Telnet path: /Setup/IP-Router/Firewall/Filter-List

2.8.10.3.16 Priority

Priority for this entry.

Telnet path: /Setup/IP-Router/Firewall/Filter-List

2.8.10.3.17 Routing tag

This routing tag is added to data packets processed by this entry.

Telnet path: /Setup/IP-Router/Firewall/Filter-List

2.8.10.3.2 Protocol

TCP protocol for data packets processed by this entry.

Telnet path: /Setup/IP-Router/Firewall/Filter-List

2.8.10.3.3 Source address

Source IP address for data packets processed by this entry.

Telnet path: /Setup/IP-Router/Firewall/Filter-List

Possible values:

- Valid IP address.

2.8.10.3.4 Source netmask

Source IP netmask for data packets processed by this entry.

Telnet path: /Setup/IP-Router/Firewall/Filter-List

Possible values:

- Valid IP address.

2.8.10.3.5 S-St. (source start)

Start address of range of source IP addresses whose data packets are processed by this entry.

Telnet path: /Setup/IP-Router/Firewall/Filter-List

2.8.10.3.6 S-End (source end)

End address of the range of source IP addresses whose data packets are processed by this entry.

Telnet path: /Setup/IP-Router/Firewall/Filter-List

2.8.10.3.7 Destination address

Destination IP address for data packets processed by this entry.

Telnet path: /Setup/IP-Router/Firewall/Filter-List

Possible values:

- Valid IP address.

2.8.10.3.8 Destination netmask

Destination IP netmask for data packets processed by this entry.

Telnet path: /Setup/IP-Router/Firewall/Filter-List

Possible values:

- Valid IP address.

2.8.10.3.9 D-St.

Start address of range of destination IP addresses whose data packets are processed by this entry.

Telnet path: /Setup/IP-Router/Firewall/Filter-List

2.8.10.4 Actions

A firewall action comprises of a condition, a limit, a packet action and other measures.

As with the elements of the object table, firewall actions can be given a name and be combined with each other in any way recursively. The maximum recursion depth is limited to 16. They can also be entered into the actions field of the rules table directly.

Telnet path: /Setup/IP-Router/Firewall

2.8.10.4.1 Name

Specify a unique name for this action.

Telnet path: /Setup/IP-Router/Firewall/Actions

Possible values:

- Max. 32 characters

Default: Blank

2.8.10.4.2 Description

In the actions table, firewall actions are combined as any combination of conditions, limits, packet actions and other measures.

Telnet path: /Setup/IP-Router/Firewall/Actions

Possible values:

- 0

2.8.10.5 Connection list

Established connections are entered into the connection list if the checked packet is accepted by the filter list. The connection list records the source and destination, the protocol, and the port that a connection is currently allowed to use. The list also indicates how long the entry remains in the list and which firewall rule generated the entry. This list is highly dynamic and always "on the move".

Telnet path: /Setup/IP-Router/Firewall

2.8.10.5.1 Source address

IP address of the station that established a connection.

Telnet path: /Setup/IP-Router/Firewall/Connection-List

Possible values:

- Valid IP address.

2.8.10.5.10 Destination route

Destination route to which a connection was established.

Telnet path: /Setup/IP-Router/Firewall/Connection-List

2.8.10.5.11 Routing tag

Connection routing tag.

Telnet path: /Setup/IP-Router/Firewall/Connection-List

2.8.10.5.2 Destination address

Destination IP address to which a connection was established.

Telnet path: /Setup/IP-Router/Firewall/Connection-List

Possible values:

- Valid IP address.

2.8.10.5.3 Protocol

Protocol allowed on this connection.

Telnet path: /Setup/IP-Router/Firewall/Connection-List

2.8.10.5.4 Source port

Source port of the station that established a connection.

Telnet path: /Setup/IP-Router/Firewall/Connection-List

2.8.10.5.5 Destination port

Destination port to which a connection was established.

Telnet path: /Setup/IP-Router/Firewall/Connection-List

2.8.10.5.6 Timeout

Lease for this entry in the table.

Telnet path: /Setup/IP-Router/Firewall/Connection-List

2.8.10.5.7 Flags

The flags are used to store information on the connection state and other (internal) information to a bit field.

The states can have the following values: New, establish, open, closing, closed, rejected (corresponding to the TCP flags: SYN, SYN ACK, ACK, FIN, FIN ACK and RST).

UDP connections know the states, open and closing (the latter only if the UDP connection is linked by a stateful control channel. This is the case with H.323, for example).

Telnet path: /Setup/IP-Router/Firewall/Connection-List

Possible values:

- 00000001 TCP: SYN sent
- 00000002 TCP: SYN/ACK received
- 00000004 TCP: Wait for ACK from server
- 00000008 all: Connection open
- 00000010 TCP: FIN received
- 00000020 TCP: FIN sent
- 00000040 TCP: RST sent or received
- 00000080 TCP: Session being restored
- 00000100 FTP: Passive FTP connection being established
- 00000400 H.323: Associated T.120 connection
- 00000800: Connection via loopback interface
- 00001000: Check linked rules
- 00002000: Rule is linked
- 00010000: Destination is on "local route"
- 00020000: Destination is on default route
- 00040000: Destination is on VPN route
- 00080000: No physical connection established
- 00100000: Source is on default route
- 00200000: Source is on VPN route
- 00800000: No route to destination
- 01000000: Contains global action with condition

2.8.10.5.8 Filter rule

Shows the filter rule that generated the entry.

Telnet path: /Setup/IP-Router/Firewall/Connection-List

2.8.10.5.9 Src-Port

Source route used to establish this connection.

Telnet path: /Setup/IP-Router/Firewall/Connection-List

2.8.10.6 Host block list

The port blocking list contains those stations that are blocked for a certain time due to a firewall event. This list is dynamic and new entries can be added continuously by corresponding firewall events; entries disappear automatically after the blocking time expires.

Telnet path: /Setup/IP-Router/Firewall

2.8.10.6.1 Source address

Source IP address that is blocked by this entry.

Telnet path: /Setup/IP-Router/Firewall/Host-Block-List

Possible values:

- Valid IP address.

2.8.10.6.2 Timeout

Lease for this entry in the table.

Telnet path: /Setup/IP-Router/Firewall/Host-Block-List

2.8.10.6.3 Filter rule

Shows the filter rule that generated the entry.

Telnet path: /Setup/IP-Router/Firewall/Host-Block-List

2.8.10.7 Port-Block-List

The port blocking list contains those protocols and services that are blocked for a certain time due to a firewall event. This list is dynamic and new entries can be added continuously by corresponding firewall events; entries disappear automatically after the blocking time expires.

Telnet path: /Setup/IP-Router/Firewall

2.8.10.7.1 Destination address

Destination IP address that is blocked by this entry.

Telnet path: /Setup/IP-Router/Firewall/Port-Block-List

Possible values:

- Valid IP address.

2.8.10.7.2 Protocol

Protocol that is blocked by this entry.

Telnet path: /Setup/IP-Router/Firewall/Port-Block-List

2.8.10.7.3 Destination port

Destination port blocked by this entry.

Telnet path: /Setup/IP-Router/Firewall/Port-Block-List

2.8.10.7.4 Timeout

Lease for this entry in the table.

Telnet path: /Setup/IP-Router/Firewall/Port-Block-List

2.8.10.7.5 Filter rule

Shows the filter rule that generated the entry.

Telnet path: /Setup/IP-Router/Firewall/Port-Block-List

2.8.10.19 Open port list

The port blocking list contains protocols and services that a firewall event has permitted for a certain time. This list is dynamic and new entries can be added continuously by corresponding firewall events; entries disappear automatically after the blocking time expires.

Telnet path: /Setup/IP-Router/Firewall

2.8.10.19.1 Source address

Source IP address that can be used by the open ports and protocols in this entry.

Telnet path: /Setup/IP-Router/Firewall/Open-Port-List

Possible values:

- Valid IP address.

2.8.10.19.2 Destination address

Destination IP address to which a connection may be established using the open ports and protocols in this entry.

Telnet path: /Setup/IP-Router/Firewall/Open-Port-List

Possible values:

- Valid IP address.

2.8.10.19.3 Protocol

Protocol opened by this entry.

Telnet path: /Setup/IP-Router/Firewall/Open-Port-List

2.8.10.19.5 Destination port

Destination port opened by this entry.

Telnet path: /Setup/IP-Router/Firewall/Open-Port-List

2.8.10.19.6 Timeout

Lease for this entry in the table.

Telnet path: /Setup/IP-Router/Firewall/Open-Port-List

2.8.10.19.8 Filter rule

Shows the filter rule that generated the entry.

Telnet path: /Setup/IP-Router/Firewall/Open-Port-List

2.8.10.19.9 Source route

Source route used to establish this connection.

Telnet path: /Setup/IP-Router/Firewall/Open-Port-List

2.8.10.20 Applications

This menu contains the configuration of individual firewall applications.

Telnet path: /Setup/IP-Router/Firewall

2.8.10.20.10 Application action

When an IRC session is identified on any port, the countermeasures configured here are taken.

Telnet path: /Setup/IP-Router/Firewall/Applications

Possible values:

- Transmit
- Drop
- Reject

Default: Reject

2.8.10.20.1 FTP

This menu contains the configuration of FTP for your firewall.

Telnet path: /Setup/IP-Router/Firewall/Applications

2.8.10.20.1.2 Active FTP block

When an FTP session is identified on any port, the countermeasures configured here are taken. 'Block active FTP' specifies whether and on what routes active FTP should be given special treatment.

Telnet path: /Setup/IP-Router/Firewall/Applications/FTP

Possible values:

- No
- Always
- WAN
- Default route

Default: No

2.8.10.20.1.1 FTP block

When an FTP session is identified on any port, the countermeasures configured here are taken. 'FTP block' specifies whether and on what routes any type of FTP should be given special treatment.

Telnet path: /Setup/IP-Router/Firewall/Applications/FTP

Possible values:

- Off
- Always
- WAN
- default route

Default: No

2.8.10.20.1.5 FXP block

When an FTP session is identified on any port, the countermeasures configured here are taken. 'FXP block' specifies whether site-to-site transfers (FXP) should be given special treatment.

Telnet path: /Setup/IP-Router/Firewall/Applications/FTP

Possible values:

- No
- Always
- WAN
- Default route

Default: Default route

2.8.10.20.1.4 Check host IP

When an FTP session is identified on any port, the countermeasures configured here are taken. 'Check host IP' specifies whether and on what routes the address transmitted in the FTP command should be checked against the source address of the FTP client. If it does not match, the countermeasures configured below will be taken. This check will of course be skipped if a site-to-site transfer is to take place and is permitted es.

Telnet path: /Setup/IP-Router/Firewall/Applications/FTP

Possible values:

- No
- Always
- WAN
- Default route

Default: Default route

2.8.10.20.1.3 Minimum port

When an FTP session is identified on any port, the countermeasures configured here are taken. 'Minimum port number' specifies the smallest permitted port for active FTP.

Telnet path: /Setup/IP-Router/Firewall/Applications/FTP

Possible values:

■ 1024 to 9999

Default: 1024

2.8.10.20.2 IRC

This menu contains the configuration of IRC for your firewall.

Telnet path: /Setup/IP-Router/Firewall/Applications

2.8.10.20.2.2 DDC block

When an IRC session is identified on any port, the countermeasures configured here are taken. 'Block DDC' specifies whether and on what routes Direct-Data-Connect (private chats and file transfers) should be given special treatment.

Telnet path: /Setup/IP-Router/Firewall/Applications/IRC

Possible values:

■ No

■ Always

■ WAN

■ Default route

Default: No

2.8.10.20.2.4 Check host IP

When an IRC session is identified on any port, the countermeasures configured here are taken. 'Check-Host-IP' indicates whether and on what routes the address transmitted in the DDC command should be checked against the source address of the IRC client.

Telnet path: /Setup/IP-Router/Firewall/Applications/IRC

Possible values:

■ No

■ Always

■ WAN

■ Default route

Default: Default route

2.8.10.20.2.1 IRC block

When an IRC session is identified on any port, the countermeasures configured here are taken. 'Block IRC' specifies whether and on what routes any type of IRC should be given special treatment.

Telnet path: /Setup/IP-Router/Firewall/Applications/IRC

Possible values:

■ No

■ Always

■ WAN

■ Default route

Default: No

2.8.10.20.2.3 Minimum port

When an IRC session is identified on any port, the countermeasures configured here are taken. 'Minimum port number' specifies the smallest permitted port for DDC.

Telnet path: /Setup/IP-Router/Firewall/Applications/IRC

Possible values:

- 1024 to 9999

Default: 1024

2.8.13 Default time list

Time-dependent control allows you to specify different destinations for the default route depending on the day of the week and time.

Telnet path: /Setup/IP-Router

2.8.13.1 Index

Index for this entry in the list.

Telnet path: /Setup/IP-Router/Default-Time-List

2.8.13.2 Days

Specify the days when this entry should be used.

Telnet path: /Setup/IP-Router/Default-Time-List

Possible values:

- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday
- Sunday
- Holiday

Default: No days are marked

2.8.13.3 Start

Used to specify the time period during which this entry should be used.

Telnet path: /Setup/IP-Router/Default-Time-List

Possible values:

- 00:00 to 23:59

Default: 0

2.8.13.4 Stop

Used to specify the time period during which this entry should be used.

Telnet path: /Setup/IP-Router/Default-Time-List

Possible values:

- 00:00 to 23:59

Default: 0.999305556

2.8.13.5 Peer

The remote site specified here will become the default route after this entry becomes valid when the defined time period is reached. Here you select the name of a remote site from the list of remote sites.

Telnet path: /Setup/IP-Router/Default-Time-List

Possible values:

- Select from the list of defined peers.

2.8.19 N-N-NAT

The rules in the N:N- NAT table regulate the IP addresses to which source addresses or entire IP networks are translated. These rules must be specified explicitly for each remote site because translation takes place after routing. The remote site reaches the stations or networks at their translated IP address as specified.

Telnet path: /Setup/IP-Router

2.8.19.1 Index

Unique index for the entry

Telnet path: /Setup/IP-Router/N-N-NAT

Possible values:

- Max. 4 characters

Default: Blank

2.8.19.2 Source address

IP address of the computer or network that is to receive an alternative IP address.

Telnet path: /Setup/IP-Router/N-N-NAT

Possible values:

- Valid IP address.

Default: 00.0.0

2.8.19.3 Src-Mask

Netmask of the source range.

Telnet path: /Setup/IP-Router/N-N-NAT

Possible values:

- Valid IP address.

Default: 00.0.0

2.8.19.4 Destination station

Name of the remote device that can be used to access the remote network.

Telnet path: /Setup/IP-Router/N-N-NAT

Possible values:

- Select from the list of defined peers.

Default: Blank

2.8.19.5 New network address

IP addresses or address range to be used for translation.

Telnet path: /Setup/IP-Router/N-N-NAT

Possible values:

- Valid IP address.

Default: 00.0.0



For the new network address, the same netmask is taken as used by the source address. The following applies with the assignment of source and mapping addresses:

- When translating individual addresses, source and mapping can be assigned in any way.
- When entire address ranges are translated, the computer-related part of the IP address is used directly and only the network-related part of the mapping address is appended. When assigning 10.0.0.0/255.255.255.0 to 192.168.1.0, the server in the LAN with the IP address 10.1.1.99 is necessarily assigned with the mapping address 192.168.1.99



The address range for translation must be at least as large as the source address range.



Please note that the N:N mapping function is only effective when the firewall is activated.

2.8.20 Load balancer

This menu contains the configuration of load balancing for your IP router.

Telnet path: /Setup/IP-Router

2.8.20.1 Operating

This is where you can set parameters for load balancing. Load balancing can be used if your provider does not offer true channel bundling. At least one virtual connection must be specified in the load balancing table for this. The maximum number of remote sites that can be bundled depends on how many DSL ports are available for the type of device used.

Telnet path: /Setup/IP-Router/Load-balancer

Possible values:

- Active
- Inactive

Default: Inactive

2.8.20.2 Bundle peers

If your Internet provider offers true channel bundling, it is possible for multiple connections to be combined with the help of load balancing.

Telnet path: /Setup/IP-Router/Load-balancer

2.8.20.2.1 Peer

Unique name for a virtual load-balancing remote site. This remote site can then be used in the routing table.

Telnet path: /Setup/IP-Router/Load-balancer/Bundle-Peers

Possible values:

- Select from the list of defined peers.

Default: Blank

2.8.20.2.2 Bundle peer 1

Name of a previously configured remote site to which the others are to be bundled.

Telnet path: /Setup/IP-Router/Load-balancer/Bundle-Peers

Possible values:

- Max. 16 characters

Default: Blank

2.8.20.2.3 Bundle peer 2

Name of a previously configured remote site to which the others are to be bundled.

Telnet path: /Setup/IP-Router/Load-balancer/Bundle-Peers

Possible values:

■ Max. 16 characters

Default: Blank

2.8.20.2.4 Bundle peer 3

Name of a previously configured remote site to which the others are to be bundled.

Telnet path: /Setup/IP-Router/Load-balancer/Bundle-Peers

Possible values:

■ Max. 16 characters

Default: Blank

2.8.20.2.5 Bundle peer 4

Name of a previously configured remote site to which the others are to be bundled.

Telnet path: /Setup/IP-Router/Load-balancer/Bundle-Peers

Possible values:

■ Max. 16 characters

Default: Blank

2.8.21 VRRP

This menu contains the configuration of VRRP for your IP router.

Telnet path: /Setup/IP-Router

2.8.21.1 Operating

VRRP – Virtual Router Redundancy Protocol – enables multiple physical routers to appear as a single "virtual" router. Of the existing physical routers, one is always the "master". The master is the only router that establishes a data connection to the Internet, for example, and transfers data. Only when the master fails, for example as a result of a power outage or if its Internet connection is dropped, will the other routers become active. They will then negotiate with the VRRP protocol to determine which router should assume the role of master. The new master completely takes over the tasks that were carried out by the previous master.

Telnet path: Setup/IP-Router/VRRP

Possible values:

■ Active

■ Inactive

Default: Inactive

2.8.21.4 Advert.-Interval

The advertising interval shows how many seconds until a virtual router is propagated again. All routers in virtual router system must be configured with the same value.

Telnet path: Setup/IP-Router/VRRP

Possible values:

■ 0 to 999 seconds

Default: 1 seconds

2.8.21.5 Internal-Services

The Internal services checkbox controls how the router should behave when it is addressed via a virtual router address. In the default 'on' position, the router reacts to DNS and NETBIOS services exactly as if it had been addressed via its actual address. This only occurs when the device itself is the master of the virtual router. The 'off' setting results in RFC-compliant behavior, i.e. relevant packets are rejected.

Telnet path: Setup/IP-Router/VRRP

Possible values:

- Yes
- No

Default: Yes

2.8.21.3 Reconnect-Delay

The router will no longer be propagated if the backup connection could not be established. The reconnect delay specifies after how many minutes such a router should in this case attempt to establish its main or backup connection. While the attempt is being made, the router will not be propagated.

Telnet path: Setup/IP-Router/VRRP

Possible values:

- 0 to 999 minutes

Default: 30 minutes

2.8.21.2 VRRP-List

In the VRRP list you can define and configure virtual routers.

Telnet path: Setup/IP-Router/VRRP

2.8.21.2.1 Router ID

Unique ID for the virtual router.

Telnet path: /Setup/IP-Router/VRRP/VRRP-List

Possible values:

- 0 to 255

Default: 1

2.8.21.2.2 virt.-Adresse

IP address for the virtual router. All routers on which the virtual router is set up must assign this router the same IP address.

Telnet path: /Setup/IP-Router/VRRP/VRRP-List

Possible values:

- Valid IP address.

Default: 00.0.0

2.8.21.2.3 Prio

Main priority for the virtual router. Values between 0 and 255 are permitted. Priority is proportional to the value entered. The values 0 and 255 have special meanings. '0' turns the virtual router off. '255' is only accepted when the virtual router address is identical to the address of the interface that is connected to the router. If this is not the case, the router will be reported by all other routers in their event logs.

Telnet path: /Setup/IP-Router/VRRP/VRRP-List

Possible values:

- 0 to 255

Default: 0

2.8.21.2.4 B-Prio

Backup priority for the virtual router. Values between 0 and 255 are permitted. Priority is proportional to the value entered. The values 0 and 255 have special meanings. 0 disables the virtual router in the event of backup. Checks are conducted regularly in order to determine whether the standard connection can be reestablished. The interval is determined by the Reconnect-Delay parameter. '255' is only accepted when the virtual router address is identical to the address of the interface that is connected to the router. If this is not the case, the router will be reported by all other routers in their event logs. When the backup connection cannot be established in backup mode, then the virtual router switches completely to the standby mode and attempts to reestablish the standard or backup connection at regular intervals.

Telnet path: /Setup/IP-Router/VRRP/VRRP-List

Possible values:

- 0 to 255

Default: 0

2.8.21.2.5 Peer

The entry for the name of the remote site is optional. If a peer name is entered here it will be controlled by VRRP. If, for example, the peer loses its Internet connection backup mode kicks in. If no peer is entered, VRRP can be used to cover a hardware outage. The remote site can still also be assigned to other virtual routers.

Telnet path: /Setup/IP-Router/VRRP/VRRP-List

Possible values:

- Select from the list of defined peers.

Default: Blank

2.8.21.2.6 Comment

This is where you can insert a comment to describe the virtual router.

Telnet path: /Setup/IP-Router/VRRP/VRRP-List

Possible values:

- Max. 64 characters

Default: Blank

2.8.23 Tag-Table

The tag table enables inbound data packets to be directly assigned with an interface tag that depends on the remote site.

Telnet path: /Setup/IP-Router

2.8.23.1 Peer

Name of the remote site whose packets are to be given interface tags when received.

Telnet path: /Setup/IP-Router/Tag-Table

Possible values:

- Select from the list of defined peers.

Default: Blank

Special values: Multiple remote sites can be configured in one entry by using * as a place holder. If, for example, several remote sites (RAS users) of a company are to be tagged, all appropriate remote sites can be given a name with the prefix "Company1_". To configure all of the remote sites, just one entry with remote site "Company1_*" can be included in the tag table.

2.8.23.2 Rtg-tag

This interface tag is assigned to the inbound packets of the remote site.

Telnet path: /Setup/IP-Router/Tag-Table

Possible values:

■ 0 to 65535

Default: 0

2.8.23.3 Start-WAN-Pool

The start WAN pool represents the beginning of the address pool for the remote site or group of remote sites (when using placeholders to specify remote site). When RAS users dial in, the remote site is assigned an address from the address pool defined here.

Telnet path: /Setup/IP-Router/Tag-Table

Possible values:

■ Valid IP address

Default: 00.0.0

2.8.23.4 End-WAN-Pool

The end WAN pool represents the end of the address pool for the remote site or group of remote sites (when using placeholders to specify remote site). When RAS users dial in, the remote site is assigned an address from the address pool defined here.

Telnet path: /Setup/IP-Router/Tag-Table

Possible values:

■ Valid IP address

Default: 00.0.0

Special values: If the pool is empty (start and end addresses are 0.0.0.0), the global pool is used.

2.9 SNMP

This menu contains the configuration of SNMP.

Telnet path: /Setup

2.9.3 Administrator

Name of the device administrator. For display purposes only.

Telnet path: /Setup/SNMP

Possible values:

■ Max. 255 characters

Default: Blank

2.9.11 Comment- 1

Comment on this device. For display purposes only.

Telnet path: /Setup/SNMP

Possible values:

■ Max. 255 characters

Default: Blank

2.9.12 Comment- 2

Comment on this device. For display purposes only.

Telnet path: /Setup/SNMP

Possible values:

■ Max. 255 characters

Default: Blank

2.9.13 Comment-3

Comment on this device. For display purposes only.

Telnet path: /Setup/SNMP

Possible values:

■ Max. 255 characters

Default: Blank

2.9.14 Comment-4

Comment on this device. For display purposes only.

Telnet path: /Setup/SNMP

Possible values:

■ Max. 255 characters

Default: Blank

2.9.16 Comment-5

Comment on this device. For display purposes only.

Telnet path: /Setup/SNMP

Possible values:

■ Max. 255 alphanumerical characters

Default: Blank

2.9.17 Comment-6

Comment on this device. For display purposes only.

Telnet path: /Setup/SNMP

Possible values:

■ Max. 255 alphanumerical characters

Default: Blank

2.9.17 Comment-7

Comment on this device. For display purposes only.

Telnet path: /Setup/SNMP

Possible values:

■ Max. 255 alphanumerical characters

Default: Blank

2.9.17 Comment-8

Comment on this device. For display purposes only.

Telnet path: /Setup/SNMP

Possible values:

■ Max. 255 alphanumerical characters

Default: Blank

2.9.6 Delete monitor

This action allows registered SNMP agents to be removed from the monitor list. The command is specified together with the IP address and the port of the SNMP agent. All three values can be replaced with the wild-card *, in which case the device ascertains the values from the packets received from the SNMP agent.

Telnet path: /Setup/SNMP

Possible values:

- <IP address|*>:<Port|*>

Default: Blank

2.9.10 Password required for SNMP read-access

This option allows you to specify that a password is required to read SNMP messages using an SNMP agent (e.g. LANmonitor). If this option is activated, the device password (or username:password) must be used as community.

Telnet path: /Setup/SNMP

Possible values:

- Yes
- No

Default: No

2.9.15 Read-only community

Entering a read-only community also enables authentication by TACACS+ to be deactivated for LANmonitor. The read-only community defined here is then entered into LANmonitor as a user name.

Telnet path: /Setup/SNMP

Possible values: Max. 31 alphanumerical characters

Default: Blank

2.9.5 Register monitor

This action allows SNMP agents to log in to the device in order to receive subsequent SNMP traps. The command is specified together with the IP address, the port and the MAC address of the SNMP agent. All three values can be replaced with the wildcard *, in which case the device ascertains the values from the packets received from the SNMP agent.

Telnet path: /Setup/SNMP

Possible values:

- <IP address|*>:<Port|*> <MAC address|*> <W>

Default: Blank

Special values: <W> at the end of the command is necessary if registration is to be effected over a wireless LAN connection.



A LANmonitor need not be explicitly logged in to the device. LANmonitor automatically transmits the login information to the device when scanning for new devices.

2.9.4 Location

Location information for this device. For display purposes only.

Telnet path: /Setup/SNMP

Possible values:

- Max. 255 characters

Default: Blank

2.9.1 Send traps

When serious errors occur, for example when an unauthorized attempt is made to access the device, it can send an error message to one or more SNMP managers automatically. Activate the option and, in the IP traps table, enter the IP addresses of those computers where the SNMP managers are installed.

Telnet path: /Setup/SNMP

Possible values:

- Yes

- No

Default: No

2.9.20 Full host MIB

Please select whether a full host MIB is used for the device.

Telnet path: /Setup/SNMP/Full-Host-MIB

Possible values:

- No
- Yes

Default: No

2.9.2 IP-Traps

You can enter SNMP managers here.

Telnet path: /Setup/SNMP

2.9.2.1 Trap-IP

Enter the IP address of the computer where an SNMP manager is installed.

Telnet path: /Setup/SNMP/IP-Traps

Possible values:

- Valid IP address.

Default: Blank

2.9.2.3 Loopback address

This is where you can configure an optional sender address to be used instead of the one otherwise automatically selected for the destination address.

Telnet path: /Setup/SNMP/IP-Traps

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LB0 to LBF for the 16 loopback addresses
- Any valid IP address

Default: Blank



If the list of IP networks or loopback addresses contains an entry named 'DMZ', the associated IP address will be used.

2.9.2.4 Version

Indicates SNMP version that should be used for the traps sent to this receiver.

Telnet path: /Setup/SNMP/IP-Traps

Possible values:

- SNMPv1
- SNMPv2

Default: SNMPv2

2.9.7 Monitor table

The monitor table shows all SNMP agents registered with the device.

Telnet path: /Setup/SNMP

2.9.7.1 IP address

IP address of the remote station from where an SNMP agent accesses the device.

Telnet path: /Setup/SNMP/Monitor-Table

Possible values:

- Valid IP address.

2.9.7.2 Port

Port used by the remote device to access the local device with an SNMP agent.

Telnet path: /Setup/SNMP/Monitor-Table

2.9.7.3 Timeout

Timeout in minutes until the remote device is removed from the monitor table.

Telnet path: /Setup/SNMP/Monitor-Table

2.9.7.4 MAC address

MAC address of the remote station from where an SNMP agent accesses the device.

Telnet path: /Setup/SNMP/Monitor-Table

2.9.7.5 Peer

Name of the remote station from where an SNMP agent accesses the device.

Telnet path: /Setup/SNMP/Monitor-Table

Possible values:

- Select from the list of defined peers.

2.9.7.6 Loopback address

Loopback address of the remote station from where an SNMP agent accesses the device.

Telnet path: /Setup/SNMP/Monitor-Table

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LB0 to LBF for the 16 loopback addresses
- Any valid IP address

2.9.7.7 VLAN-ID

ID of the VLAN used by the remote device to access the local device with an SNMP agent.

Telnet path: /Setup/SNMP/Monitor-Table

2.9.7.8 LAN-Ifc

LAN Ifc used by the remote device to access the local device with an SNMP agent.

Telnet path: /Setup/SNMP/Monitor-Table

2.9.7.9 Ethernet port

Ethernet port used by the remote device to access the local device with an SNMP agent.

Telnet path: /Setup/SNMP/Monitor-Table

2.10 DHCP

This menu contains the DHCP settings.

Telnet path: /Setup

2.10.7 Default-Lease-Time-Minutes

When a client requests an address without asking for a specific lease period, the address will be assigned the value set here as lease.

Telnet path: Setup/DHCP

Possible values:

■ Max. 10 characters

Default: 500

2.10.6 Max.-Lease-Time-Minutes

When a client requests an IP address from a DHCP server, it can also ask for a lease period for the address. This value governs the maximum length of lease that the client may request.

Telnet path: Setup/DHCP

Possible values:

■ Max. 10 characters

Default: 6000

2.10.19 User class identifier

The DHCP client in the device can supplement the transmitted DHCP requests with additional information to simplify the recognition of request within the network. The vendor class identifier (DHCP option 60) shows the device type, e.g. 'LANCOM L-54ag'. The vendor class ID is always transmitted. The user class ID (DHCP option 77) specifies a user-defined string. The user class ID is only transmitted when the user has configured a value.

Telnet path: Setup/DHCP

Possible values:

■ Max. 63 characters

Default: Blank

2.10.8 DHCP table

The DHCP table provides an overview of the IP addresses used in the IP networks. The DHCP table is purely a status table where no parameters can be configured.

Telnet path: Setup/DHCP

2.10.8.1 IP address

IP address used by the client.

Telnet path: Setup/DHCP/DHCP-Table

Possible values:

- Valid IP address.

2.10.8.10 LAN-Ifc

The LAN interface that this entry refers to.

Telnet path: /Setup/DHCP/DHCP-Table/LAN-Ifc

2.10.8.2 MAC-Address

The client's MAC address.

Telnet path: Setup/DHCP/DHCP-Table

2.10.8.3 Timeout

Lease for the address assignment in minutes.

Telnet path: Setup/DHCP/DHCP-Table

2.10.8.4 Hostname

Name of the client, if it was possible to determine this.

Telnet path: Setup/DHCP/DHCP-Table

2.10.8.5 Type

The 'Type' field indicates how the address was assigned. This field may contain the following values:

New: The client made the request for the first time. The DHCP checks that the address to be assigned to the client is unique.

Unknown: When the server checked if the address was unique, it was found that the address had already been assigned to another client. Unfortunately, the DHCP server does not have any way of obtaining further information about this client.

Stat: A client has informed the DHCP server that it has a fixed IP address. This address may not be used for any other clients in the network.

Dyn.: The DHCP server has assigned an address to the client.

Telnet path: Setup/DHCP/DHCP-Table

2.10.8.7 Ethernet port

Physical interface connecting the client to the device.

Telnet path: Setup/DHCP/DHCP-Table

2.10.8.8 VLAN-ID

The VLAN ID used by the client.

Telnet path: Setup/DHCP/DHCP-Table

2.10.8.9 Network name

Name of the IP network where the client is located.

Telnet path: Setup/DHCP/DHCP-Table

2.10.9 Hosts

The bootstrap protocol (BOOTP) can be used to communicate a certain IP address and other parameters to a workstation when it boots up. For this, the workstation's MAC address is entered in the hosts table.

Telnet path: Setup/DHCP

2.10.9.1 MAC-Address

Enter the MAC address of the workstation to which an IP address is to be assigned.

Telnet path: Setup/DHCP/Hosts

Possible values:

- Valid MAC address

Default: 000000000000

2.10.9.2 IP address

Enter the client IP address that is to be assigned to the client.

Telnet path: Setup/DHCP/Hosts

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.10.9.3 Hostname

Enter the name that is to be used to identify the station. If the station does not communicate its name, the device will use the name entered here.

Telnet path: Setup/DHCP/Hosts

Possible values:

- Max. 30 characters

Default: Blank

2.10.9.4 Image alias

If the client uses the BOOTP protocol, you can select a boot image that the client should use to load its operating system from.

Telnet path: Setup/DHCP/Hosts

Possible values:

- Max. 16 characters

Default: Blank



You must enter the server providing the boot image and the name of the file on the server in the boot image table.

2.10.9.5 Network name

Enter the name of a configured IP network here. Only if a requesting client is located in this IP network will it be assigned the relevant IP address defined for the MAC address.

Telnet path: Setup/DHCP/Hosts

Possible values:

■ Max. 16 characters

Default: Blank

Special values: Blank: The IP address will be assigned if the IP address defined in this field belongs to the range of addresses for the IP network where the requesting client is located.



If the requesting client is located in an IP network for which there is no corresponding entry in the hosts table, the client will be assigned an IP address from the address pool of the appropriate IP network.

2.10.10 Alias list

The alias list defines the names for the boot images that are used to reference the images in the hosts table.

Telnet path: Setup/DHCP

2.10.10.1 Image alias

Enter any name you wish for this boot image. This name is used when you assign a boot image to a particular client in the station list.

Telnet path: Setup/DHCP/Alias-List

Possible values:

■ Max. 16 characters

Default: Blank

2.10.10.2 Image file

Enter the name of the file on the server containing the boot image.

Telnet path: Setup/DHCP/Alias-List

Possible values:

■ Max. 60 characters

Default: Blank

2.10.10.3 Image server

Enter the IP address of the server that provides the boot image.

Telnet path: Setup/DHCP/Alias-List

Possible values:

■ Valid IP address.

Default: 0.0.0.0

2.10.18 Ports

The port table is where the DHCP server is enabled for the appropriate logical interface of the device.

Telnet path: Setup/DHCP

2.10.18.2 Port

Select the logical interface for which the DHCP server should be enabled or disabled.

Telnet path: Setup/DHCP/Ports

Possible values:

- Select from the list of logical devices in this device, e.g. LAN-1, WLAN-1, P2P-1-1 etc.

2.10.18.3 Enable-DHCP

Enables or disables the DHCP server for the selected logical interface.

Telnet path: Setup/DHCP/Ports

Possible values:

- Yes
- No

Default: Yes

2.10.20 Network list

If multiple DHCP servers are active in a network, the stations "divide" themselves equally between them. However, the DNS server in devices can only properly resolve the name of the station which was assigned the address information by the DHCP server. In order for the DNS server to be able to resolve the names of other DHCP servers, these can be operated in a cluster. In this operating mode, the DHCP server monitors all DHCP negotiations in the network. It additionally supplements its table with the stations which are registered at the other DHCP servers in the cluster.

A DHCP server's operation in the cluster can be activated or deactivated for each individual ARF network with the associated DHCP settings.

Telnet path: Setup/DHCP/Network-list

2.10.21.2 Network-name

The name of the network which the DHCP server settings apply to.

Telnet path: Setup/DHCP/Network-list

Possible values:

- Max. 16 characters

Default: Blank

2.10.20.10 NBNS backup

IP address of the backup NBNS name server. The workstation will use this NBNS server if the first NBNS name server fails

Telnet path: Setup/DHCP/Network-list

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.10.20.11 Operating

DHCP server operating mode in this network. Depending on the operating mode, the DHCP server can enable/disable itself. The DHCP statistics show whether the DHCP server is enabled.

Telnet path: Setup/DHCP/Network-list

Possible values:

- No: DHCP server is permanently switched off.
- Yes: DHCP server is permanently switched on. When this value is entered the server configuration (validity of the address pool) is checked. If the configuration is correct then the device starts operating as a DHCP server in the network. Errors in the configuration (e.g. invalid pool limits) will cause the DHCP server to be deactivated. Only use this setting if you are certain that no other DHCP server is active in the LAN.
- Automatic: With this setting, the device regularly searches the local network for other DHCP servers. The LAN-Rx/Tx LED flashes briefly when this search is in progress. If another DHCP server is discovered the device switches its own DHCP server off. If the LANCOM is not configured with an IP address, then it switches into DHCP client mode and queries the LAN DHCP server for an IP address. This prevents unconfigured devices introduced to the network from assigning addresses unintentionally. If no other DHCP server is discovered the device switches its own DHCP server on. If another DHCP server is activated later, then the DHCP server in the LANCOM will be disabled.
- 'Relay requests': The DHCP server is active and receives requests from DHCP clients in the LAN. The device does not respond to requests, but forwards them to a central DHCP server elsewhere in the network (DHCP relay agent mode).
- 'Client mode': The DHCP server is disabled, the device behaves as a DHCP client and obtains its address from another DHCP server in the LAN. Only use this setting if you are certain that another DHCP server is in the LAN and actively assigning IP addresses.

Default: No



Only use the setting "Yes" if you are certain that no other DHCP server is active in the LAN. Only use the "client mode" setting if you are certain that another DHCP server is in the LAN and actively assigning IP addresses.

2.10.20.12 Broadcast bit

This setting decides whether the broadcast bit from clients is to be checked. If the bit is not checked then all DHCP messages are sent as broadcasts.

Telnet path: Setup/DHCP/Network-list

Possible values:

- Yes
- No

Default: No

2.10.20.13 Master server

This is where the IP address for the upstream DHCP server is entered where DHCP requests are forwarded when the mode 'Relay requests' is selected for the network.

Telnet path: Setup/DHCP/Network-list

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.10.20.14 Cache

This option allows the responses from the superordinate DHCP server to be stored in the LANCOM Wireless. Subsequent requests can then be answered by the LANCOM Wireless itself. This option is useful if the superordinate DHCP server can only be reached via a connection which incurs costs.

Telnet path: Setup/DHCP/Network-list

Possible values:

- Yes
- No

Default: No

2.10.20.15 Adaption

This option allows the responses from the superordinate DHCP server to be adapted to the local network. When activated, the LANCOM Wireless adapts the responses from the superordinate DHCP server by replacing the following entries with its own address (or locally configured addresses):

- Gateway
- Network mask
- Broadcast address
- DNS server
- NBNS server
- Server ID

This option is worthwhile if the superordinate DHCP server does not permit the separate configuration for DHCP clients in another network.

Telnet path: Setup/DHCP/Network-list**Possible values:**

- Yes
- No

Default: No

2.10.20.16 Cluster

This setting defines whether the DHCP server for this ARF network is to be operated separately or in the cluster.

Telnet path: Setup/DHCP/Network-list**Possible values:**

- Yes: With cluster mode activated, the DHCP server monitors all of the ongoing DHCP negotiations in the network, and it additionally supplements its table with the stations which are registered at the other DHCP servers in the cluster. These stations are flagged as "cache" in the DHCP table.
- No: The DHCP server manages information only for the stations connected to it.

Default:

No



If the lease time for the information supplied by DHCP expires, the station requests a renewal from the DHCP server which supplied the original information. If the original DHCP server does not respond, the station then emits its rebinding request as a broadcast to all available DHCP servers. DHCP servers in a cluster ignore renew requests, which forces a rebinding. The resulting broadcast is used by all of the DHCP servers to update their entries for the station. The only DHCP server to answer the rebind request is the one with which the station was originally registered. If a station repeats its rebind request, the all DHCP servers in the cluster assume that the original DHCP server is no longer active in the cluster, and they respond to the request. The responses received by the station will have the same IP address, but the gateway and DNS server addresses may differ. From these responses, the station selects a new DHCP server to connect with, and it updates its gateway and DNS server (and other relevant parameters) accordingly.

2.10.20.17 2nd master server

This is where the IP address for an alternative DHCP server is entered where DHCP requests are forwarded when the mode 'Relay requests' is selected for the network.

Telnet path: /Setup/DHCP/Network-list/2nd-Master-Server**Possible values:**

- Valid IP address.

Default: 0.0.0.0

2.10.20.18 3rd master server

This is where the IP address for an alternative DHCP server is entered where DHCP requests are forwarded when the mode 'Relay requests' is selected for the network.

Telnet path: /Setup/DHCP/Network-list/2nd-Master-Server

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.10.20.19 4th master server

This is where the IP address for an alternative DHCP server is entered where DHCP requests are forwarded when the mode 'Relay requests' is selected for the network.

Telnet path: /Setup/DHCP/Network-list/2nd-Master-Server

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.10.20.2 Start address pool

The first IP address in the pool available to the clients. If no address is entered here the DHCP server takes the first available IP address from the network (as determined by network address and netmask).

Telnet path: Setup/DHCP/Network-list

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.10.20.3 End address pool

The last IP address in the pool available to the clients. If no address is entered here the DHCP server takes the last available IP address from the network (as determined by network address and netmask).

Telnet path: Setup/DHCP/Network-list

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.10.20.4 Netmask

Corresponding netmask for the address pool available to the clients. If no address is entered here the DHCP server uses the netmask from the corresponding network.

Telnet path: Setup/DHCP/Network-list

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.10.20.5 Broadcast address

As a rule, broadcast packets in a local network have an address which results from the valid IP addresses and the netmask. In special cases (e.g. when using subnets for a selection of workstations) it may be necessary to use a different broadcast address. In this case the broadcast address is entered into the DHCP module.

Telnet path: Setup/DHCP/Network-list

Possible values:

- Valid IP address.

Default: 0.0.0.0 (broadcast address is determined automatically).



We recommend that only experienced network specialists change the presetting for the broadcast address. Errors in the configuration can lead to the establishment of undesired and costly connections.

2.10.20.6 Gateway address

As standard, the DHCP server issues its own IP address as the gateway address to computers making requests. If necessary, the IP address of another gateway can also be transmitted if a corresponding address is entered here.

Telnet path: Setup/DHCP/Network-list

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.10.20.7 DNS default

IP address of the DNS name server that the requesting workstation should use.

Telnet path: Setup/DHCP/Network-list

Possible values:

- Valid IP address.

Default: 0.0.0.0



If no default or backup DNS server is defined, the device will assign the requesting workstation its own IP address in the relevant ARF network as (primary) DNS server.

2.10.20.8 DNS backup

IP address of the backup DNS server. The workstation will use this DNS server if the first DNS server fails

Telnet path: Setup/DHCP/Network-list

Possible values:

- Valid IP address.

Default: 00.0.0



If no default or backup DNS server is defined, the device will assign the requesting workstation its own IP address in the relevant ARF network as (primary) DNS server.

2.10.20.9 NBNS default

IP address of the NBNS name server that the requesting workstation should use.

Telnet path: Setup/DHCP/Network-list

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.10.21 Additional options

DHCP options can be used to send additional configuration parameters to the clients. The vendor class ID (DHCP option 60) shows e.g. the type of device. This table allows additional options for DHCP operations to be defined.

Telnet path: Setup/DHCP

2.10.21.1 Option number

Number of the option that should be sent to the DHCP client. The option number describes the transmitted information. For example "17" (root path) is the path to a boot image that a PC without its own hard disk uses to obtain its operating system via BOOTP.

Telnet path: Setup/DHCP/Additional-Options**Possible values:** Max. 3 characters**Default:** Blank

You can find a list of all DHCP options in RFC 2132 – "DHCP Options and BOOTP Vendor Extensions" of the Internet Engineering Task Force (IETF).

2.10.21.2 Network name

Name of the IP network where this DHCP option is to be used.

Telnet path: Setup/DHCP/Additional-Options**Possible values:**

- Select from the list of defined IP networks.

Default: Blank

Special values: Blank: If no network name is specified the DHCP option defined in this entry will be used in all IP networks.

2.10.21.3 Option Value

This field defines the contents of the DHCP option. IP addresses are normally specified using the conventional IPv4 notation, e.g. "123.123.123.100". Integer tapes are usually entered in normal decimal digits and string types as simple text. Multiple values in a single field are separated with commas, e.g. "123.123.123.100, 123.123.123.200".

Telnet path: Setup/DHCP/Additional-Options**Possible values:**

- Max. 128 characters



The maximum possible length value depends on the selected option number. RFC 2132 lists the maximum length allowed for each option.

2.10.21.4 Option-Type

Entry type.

Telnet path: Setup/DHCP/Additional-Options

This value depends on the respective option. For option "35" according to RFC 1232, e.g. the ARP cache time is defined as follows:

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

This description tells you that this the type "32-bit integer" is used for this option.

Possible values:

- String
- Integer8
- Integer16
- Integer32
- IP address

Default: String



You can find out the type of the option either from the corresponding RFC or from the manufacturer's documentation of their DHCP options.

2.11 Config

Contains the general configuration settings.

Telnet path: /Setup

2.11.9 Administrator EAZ-MSN

If the LANCAPI server is to receive incoming calls, enter your ISDN telephone number which is to receive the LANCAPI calls into the 'EAZ-MSNs' field. Multiple telephone numbers are separated by semicolons. If no telephone number is entered here, LANCAPI receives calls on any of its ISDN telephone numbers.

Telnet path: Setup/Config

Possible values:

- Max. 31 characters

Default: Blank

2.11.41 Admin gender

Enter the sex of the Admin.

Telnet path: /Setup/Config/Admin-Gender

Possible values:

- Unknown
- Male
- Female

Default: Unknown

2.11.42 Assert action

This parameter affects the behavior of the device when it checks the firmware code.

Telnet path: /Setup/Config/Assert-Action

Possible values:

- log_only
- reboot

Default: log_only

The settings for this parameter are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.11.16 Screen height

Specifies the maximum height of the screen in lines. Entering 0 here causes the device to determine optimum screen height automatically when you log in.

Telnet path: Setup/Config**Possible values:**

- Max. 10 characters

Default: 24**Special values:** 0

2.11.5 Config aging minutes

Specify here the number of minutes after which an inactive TCP configuration connection (e.g. via telnet) is automatically terminated.

Telnet path: Setup/Config**Possible values:**

- Max. 10 characters

Default: 15

2.11.60 CPU-load interval

You can select the time interval for averaging the CPU load. The CPU load displayed in LANmonitor, in the status area, in the display (if fitted), or by SNMP tools is a value which is averaged over the time interval set here. The status area under WEBconfig or CLI additionally display the CPU load values for all four of the optional averaging periods.

Meaned values for CPU load are available in the following time intervals:

Telnet path: Setup/Config**Possible values:**

- T1s (arithmetic mean)
- T5s (arithmetic mean)
- T60s (moving average)
- T300s (moving average)

Default: T60s

2.11.40 Crash message

Here you specify the message that appears in the bootlog when the device crashes.

Telnet path: /Setup/Config/Crash-Message**Possible values:**

- Maximum 32 alphanumerical characters

Default: LCOS-Watchdog

2.11.10 Display contrast

This item allows you to set the contrast for the display of the device.

Telnet path: /Setup/Config/Display-contrast

Possible values:

■ K1 (low contrast) to K8 (high contrast).

Default: K4

2.11.18 LED test

Activates the test mode for the LEDs to test LED function in different colors.

Telnet path: Setup/Config

Possible values:

■ Off: Switches all LEDs off

■ Red Switches all LEDs on that emit red.

■ Green: Switches all LEDs on that emit green.

■ Orange Switches all LEDs on that emit orange.

■ No_Test: Normal LED operating mode.

Default: No_Test:

2.11.39 License expiry e-mail

The license to use a product can be restricted to a set validity period. You will be reminded of the license expiry date 30 days, one week and one day before it actually expires by an e-mail to the address configured here.

Telnet path: Setup/Config//License-Expiry-Email

Possible values:

■ Valid e-mail address

Default: Blank

2.11.7 Login errors

In order to protect the configuration of your device against unauthorized access, the device can lock itself after repeated incorrect attempts to log in. Use this setting to specify the number of incorrect login attempts are allowed before the device is locked.

Telnet path: Setup/Config

Possible values:

■ Max. 10 characters

Default: 10

2.11.4 Maximum connections

The maximum number of simultaneous configuration connections to this device.

Telnet path: Setup/Config

Possible values:

■ Max. 10 characters

Default: 0

Special values: 0 switches the limit off.

2.11.33 Outband aging minutes

Specify here the number of minutes after which an inactive serial connection (e.g. via Hyper Terminal) is automatically terminated.

Telnet path: Setup/Config

Possible values:

■ Max. 10 characters

Default: 1

2.11.3 Password required for SNMP read access

If this option is activated and no password has been set, you will always be requested to set a password when you log in to the device.

Telnet path: Setup/Config

Possible values:

- Yes
- No

Default: No

2.11.17 Prompt

This value sets the prompt on the command line.

Telnet path: Setup/Config

Possible values:

- Max. 31 characters with the following variables:
- %f: Starts a [Test] if you previously entered the command 'flash no' on the command line. The command 'flash no' activates the test mode for the configuration changes outlined below. When test mode is enabled, the device saves the changes to the configuration in RAM only. As the device's RAM is deleted during a reboot, all of the configuration changes made in test mode are lost. The [Test] display alerts the administrator about this potential loss of changes to the configuration.
- %u: User name
- %n: Device name
- %p: Current path
- %t: Current time
- %o: Current operating time

Default: Blank

2.11.32 Reset button

The reset button offers two basic functions—boot (restart) and reset (to the factory settings)—which are called by pressing the button for different lengths of time.

It is not always possible to install a device under lock and key. There is consequently a risk that the configuration will be deleted by mistake if a co-worker presses the reset button too long. The behavior of the reset button can be controlled with this setting.

Telnet path: Setup/Config

Possible values:

- Ignore: The button is ignored.
- Boot only: With a suitable setting, the behavior of the reset button can be controlled; the button is then ignored or a press of the button prompts a restart only, however long it is held down.
- Reset-or-boot (standard setting): With this setting, the reset button fulfills different functions depending upon how long the key remains pressed:
 - Less than 5 seconds: Boot (restart), whereby the user-defined configuration is loaded from the configuration memory. If the user-defined configuration is empty, then the customer-specific standard settings (first memory space) are loaded instead. The loading of the customer-specific standard settings is visible when all LEDs on the device light up briefly in red. Similarly, the LANCOM factory settings are loaded if the first memory space is empty.
 - Longer than 5 seconds until the first time that all device LEDs light up: Configuration reset (deletes the configuration memory) followed by a restart. In this case the customer-specific standard settings (first memory space) are loaded instead. The loading of the customer-specific standard settings is visible when all LEDs on the device light up briefly in red. The LANCOM factory settings are loaded if the first memory space is empty.
 - Longer than 15 seconds until the second time that all device LEDs light up: Activating the rollout configuration and deleting the user-defined configuration. After restarting, the rollout configuration is started from the second memory space. The loading of the rollout configuration is visible when all

LEDs on the device light up twice briefly in red. The LANCOM factory settings are loaded if the second memory space is empty.



Further information about the different boot configurations are to be found in the reference manual.

Default: Reset-or-boot



After a reset, the LANCOM access point returns to managed mode, in which case the configuration cannot be directly accessed via the WLAN interface!



After resetting, the device starts completely unconfigured and all settings are lost. If possible be sure to backup the current device configuration before resetting.



The settings 'Ignore' or 'Boot only' makes it impossible to reset the configuration to the factory settings or to load the rollout configuration with a reset. If the password is lost for a device with this setting, there is no way to access the configuration! In this case the serial communications interface can be used to upload a new firmware version to the device—this resets the device to its factory settings, which results in the deletion of the former configuration. Instructions on firmware uploads via the serial configuration interface are available in the LCOS reference manual.

2.11.8 Lock minutes

In order to protect the configuration of your device against unauthorized access, the device can lock itself after repeated incorrect attempts to log in. Enter the period for which the lock is to be active for. Access to the device will only be possible after this period expires.

Telnet path: Setup/Config

Possible values:

■ Max. 10 characters

Default: 45

Special values: 0 switches the lock off.

2.11.6 Language

Terminal mode is available in English or German. Devices are set with English as the default console language.

Telnet path: Setup/Config

Possible values:

■ Deutsch

■ English

Default: English



Please ensure that the language you use to enter commands matches with that set for the console, otherwise scheduler commands will not be observed.

2.11.25 SSH port

This port is used for configuration connections via SSH.

Telnet path: Setup/Config

Possible values:

■ Max. 10 characters

Default: 22

2.11.23 Telnet port

This port is used for unencrypted configuration connections via Telnet.

Telnet path: Setup/Config

Possible values:

■ Max. 10 characters

Default: 23

2.11.24 Telnet SSL port

This port is used for encrypted configuration connections via telnet.

Telnet path: Setup/Config

Possible values:

■ Max. 10 characters

Default: 992

2.11.13 TFTP client

Default values for the device configuration, firmware and/or a script can be used if the latest configurations, firmware versions and scripts are always stored under the same name in the same location. In this case, the simple commands LoadConfig, LoadFirmware and LoadScript can be used to load the relevant files.

Telnet path: Setup/Config

2.11.13.5 Bytes per hashmark

Number of bytes used per hashmark.

Telnet path: /Setup/Config/TFTP-Client

Possible values:

■ Max. 6 numbers

Default: 8192

2.11.13.1 Configuration address

Default path for configuration files when the parameter -f is not specified for LoadConfig commands.

Telnet path: /Setup/Config/TFTP-Client

Possible values:

■ Path specified in the notation //Server/Directory/File name

Default: Blank

2.11.13.2 Configuration filename

Default name of the configuration file when the parameter -f is not specified for LoadConfig commands.

Telnet path: /Setup/Config/TFTP-Client

Possible values:

■ Max. 63 characters

Default: Blank

2.11.13.3 Firmware address

Default path for firmware files when the parameter -f is not specified for LoadFirmware.

Telnet path: /Setup/Config/TFTP-Client

Possible values:

■ Path specified in the notation //Server/Directory/File name

Default: Blank

2.11.13.4 Firmware filename

Default path for the firmware file when the parameter -f is not specified for LoadFirmware.

Telnet path: /Setup/Config/TFTP-Client

Possible values:

- Max. 63 characters

Default: Blank

2.11.13.6 Script address

Default path for scripts when the parameter -f is not specified for LoadScript.

Telnet path: /Setup/Config/TFTP-Client

Possible values:

- Path specified in the notation //Server/Directory/File name

Default: Blank

2.11.13.7 Script filename

Default path for the script when the parameter -f is not specified for LoadScript.

Telnet path: /Setup/Config/TFTP-Client

Possible values:

- Max. 63 characters

Default: Blank

2.11.15 Access table

Here you can set the access rights separately for each network and configuration protocol. You can also set limitations on the access to certain stations.

Telnet path: Setup/Config

2.11.15.1 Interface

The LAN interface that this entry refers to.

Telnet path: /Setup/Config/Access-Table

2.11.15.2 Telnet

Use this option to set the access rights for configuring the device via the TELNET protocol. This protocol is required for text-based configuration of the device with the Telnet console, which is independent of the operating system.

Telnet path: /Setup/Config/Access-Table

Possible values:

- VPN
- Yes
- Read
- No

Default: Yes

2.11.15.3 TFTP

Use this option to set the access rights for configuring the device via the TFTP protocol (Trivial File Transfer Protocol). This protocol is required, for example, for configuration using the LANconfig application.

Telnet path: /Setup/Config/Access-Table

Possible values:

- ☐ VPN
- ☐ Yes
- ☐ Read
- ☐ No

Default: Yes

2.11.15.4 HTTP

Use this option to set the access rights for configuring the device via the HTTP protocol (Hypertext Transfer Protocol). This protocol is required for configuring the device via the implemented web-based browser interface independent of the operating system.

Telnet path: /Setup/Config/Access-Table

Possible values:

- ☐ VPN
- ☐ Yes
- ☐ Read
- ☐ No

Default: Yes

2.11.15.5 SNMP

Use this option to set the access rights for configuring the device via the SNMP protocol (Simple Network Management Protocol). This protocol is required, for example, for configuring the device using the LANmonitor application.

Telnet path: /Setup/Config/Access-Table

Possible values:

- ☐ VPN
- ☐ Yes
- ☐ Read
- ☐ No

Default: Yes

2.11.15.6 HTTPS

Use this option to set the access rights for configuring the device via the HTTPS protocol (Hypertext Transfer Protocol Secure or HTTP via SSL). This protocol is required for configuring the device via the implemented web-browser interface independent of the operating system.

Telnet path: /Setup/Config/Access-Table

Possible values:

- ☐ VPN
- ☐ Yes
- ☐ Read
- ☐ No

Default: Yes

2.11.15.7 Telnet-SSL

Use this option to set the access rights for configuring the device via the TELNET protocol. This protocol is required for text-based configuration of the device with the Telnet console, which is independent of the operating system.

Telnet path: /Setup/Config/Access-Table

Possible values:

- VPN
- Yes
- Read
- No

Default: LAN: Yes, WAN:No

2.11.15.8 SSH

Use this option to set the access rights for configuring the device via the TELNET/SSH protocol. This protocol is required for configuring the device securely via the implemented Telnet console from text-based systems independent of the operating system.

Telnet path: /Setup/Config/Access-Table

Possible values:

- VPN
- Yes
- Read
- No

Default: Yes

2.11.20 Cron table

CRON jobs are used to carry out recurring tasks on a LANCOM device automatically at certain times. If the installation features a large number of active devices, all of which are subjected to the same CRON job at the same time (e.g. updating a configuration by script), unpleasant side effects can result if, for example, all devices try to establish a VPN connection at once. To avoid these effects, the CRON jobs can be set with a random delay time between 0 and 59 minutes.

Telnet path: Setup/Config

2.11.20.1 Index

Index for this entry.

Telnet path: /Setup/Config/Cron-Table

2.11.20.10 Owner

An administrator defined in the device can be designated as owner of the CRON job. If an owner is defined, then the CRON job commands will be executed with the rights of the owner.

Telnet path: /Setup/Config/Cron-Table

Possible values:

- Max. 16 characters

Default: Blank

2.11.20.11 Variation

This parameter specifies the maximum delay in minutes for the start of the CRON job after the set start time. The actual delay time is determined randomly and lies between 0 and the time entered here.

Telnet path: /Setup/Config/Cron-Table

Possible values:

- 0 to 65535 seconds

Default: 0

Special values: With the variation set to zero the CRON job will be executed at the set time.



Rules based on real-time can only be executed if the device has a time from a valid source, e.g. via NTP.

2.11.20.2 Minute

The value defines the point in time when a command is to be executed. With no value entered, it is not included in the controlling. A comma-separated list of values can be entered, or alternatively a range of minimum and maximum values.

Telnet path: /Setup/Config/Cron-Table

Possible values:

- Max. 50 characters

Default: Blank

2.11.20.3 Hour

The value defines the point in time when a command is to be executed. With no value entered, it is not included in the controlling. A comma-separated list of values can be entered, or alternatively a range of minimum and maximum values.

Telnet path: /Setup/Config/Cron-Table

Possible values:

- Max. 50 characters

Default: Blank

2.11.20.4 DayOfWeek

The value defines the point in time when a command is to be executed. With no value entered, it is not included in the controlling. A comma-separated list of values can be entered, or alternatively a range of minimum and maximum values.

Telnet path: /Setup/Config/Cron-Table

Possible values:

- 0: Sunday
- 1: Monday
- 2: Tuesday
- 3: Wednesday
- 4: Thursday
- 5: Friday
- 6: Saturday

Default: Blank

2.11.20.5 Day

The value defines the point in time when a command is to be executed. With no value entered, it is not included in the controlling. A comma-separated list of values can be entered, or alternatively a range of minimum and maximum values.

Telnet path: /Setup/Config/Cron-Table

Possible values:

- Max. 50 characters

Default: Blank

2.11.20.6 Month

The value defines the point in time when a command is to be executed. With no value entered, it is not included in the controlling. A comma-separated list of values can be entered, or alternatively a range of minimum and maximum values.

Telnet path: /Setup/Config/Cron-Table

Possible values:

- 0: Sunday
- 1: Monday
- 2: Tuesday
- 3: Wednesday
- 4: Thursday
- 5: Friday
- 6: Saturday

Default: Blank

2.11.20.7 Command

The command to be executed or a comma-separated list of commands. Any LANCOM command-line function can be executed.

Telnet path: /Setup/Config/Cron-Table

Possible values:

- Max. 100 characters

Default: Blank

2.11.20.8 Base

The time base field determines whether time control is based on real time or on the device's operating time.

Telnet path: /Setup/Config/Cron-Table

Possible values:

- Real-Time: These rules evaluate all time/date information. Rules based on real-time can only be executed if the device has a time from a valid source, e.g. via NTP.
- Operation-Time: These rules only evaluate the minutes and hours since the last time the device was started.

Default: Real time

2.11.20.9 Active

Activates or deactivates the entry.

Telnet path: /Setup/Config/Cron-Table

Possible values:

- Yes
- No

Default: Yes

2.11.21 Admins

Here you can create additional administrator user accounts.

Telnet path: Setup/Config

2.11.21.1 Administrator

Multiple administrators can be set up in the configuration of the device, each with different access rights. Up to 16 different administrators can be set up for a LANCOM device.

Telnet path: Setup/Config/Admins

Possible values:

- Max. 16 characters

Default: Blank



Besides these administrators set up in the configuration, there is also the "root" administrator with the main password for the device. This administrator always has full rights and cannot be deleted or renamed. To log in as root administrator, enter the user name "root" in the login window or leave this field empty. As soon as a password is set for the "root" administrator in the device's configuration, WEBconfig will display the button Login that starts the login window. After entering the correct user name and password, the WEBconfig main menu will appear. This menu only displays the options that are available to the administrator who is currently logged in. If more than one administrator is set up in the admin table, the main menu features an additional button 'Change administrator' which allows other users to log in (with different rights, if applicable).

2.11.21.2 Password

Password for this entry.

Telnet path: Setup/Config/Admins

Possible values:

- Max. 16 characters

Default: Blank

2.11.21.3 Function rights

Each administrator also has "function rights" that determine personal access to certain functions such as the Setup Wizards.

Telnet path: Setup/Config/Admins

Possible values:

- The different function rights are represented by the following hexadecimal values:
- 0x00000001: The user can run the Basic Settings Wizard
- 0x00000002: The user can run the Security Wizard
- 0x00000004: The user can run the Internet Wizard
- 0x00000008: The user can run the Wizard for selecting Internet providers
- 0x00000010: The user can run the RAS Wizard
- 0x00000020: The user can run the LAN-LAN Coupling Wizard
- 0x00000040: The user can set the date and time (also applies for Telnet and TFTP)
- 0x00000080: The user can search for additional devices
- 0x00000100: The user can run the WLAN Link test (also applies for Telnet)

- 0x00000200: The user can run the a/b Wizard
- 0x00000400: The user can run the WTP Assignment Wizard
- 0x00000800: The user can run the Public Spot Wizard
- 0x00001000: The user can run the WLAN Wizard
- 0x00002000: The user can run the Rollout Wizard
- 0x00004000: The user can run the Dynamic DNS Wizard
- 0x00008000: The user can run the VoIP Call Manager Wizard
- 0x00010000: The user can run the WLC Profile Wizard
- 0x00020000: The user can use the integrated Telnet or SSH client

Default: Blank

2.11.21.4 Active

Activates or deactivates the function

Telnet path: Setup/Config/Admins

Possible values:

- Yes
- No

Default: Yes

2.11.21.5 Access rights

Access to the internal functions can be configured for each interface separately:

- ISDN administration access
- LAN
- Wireless LAN (WLAN)
- WAN (e.g. ISDN, DSL or ADSL)

Access to the network configuration can be further restricted so that, for example, configurations can only be edited from certain IP addresses or LANCAPAPI clients. Furthermore, the following internal functions can be switched on/off separately:

- LANconfig (TFTP)
- WEBconfig (HTTP, HTTPS)
- SNMP
- Terminal/Telnet

For devices supporting VPN, it is also possible to restrict the use of internal functions that operate over WAN interfaces to be restricted to VPN connections only.

Telnet path: Setup/Config/Admins

Possible values:

- None
- Admin-RO limit
- Admin-RW limit
- Admin-RO
- Admin-RW
- Supervisor

Default: Blank

2.11.26 SSH authentication methods

Here you specify the authentication method to be used for SSH.

Telnet path: Setup/Config

2.11.26.1 Interface

The authentication methods permitted for SSH access can be set separately for LAN, WAN and WLAN.

Telnet path: Setup/Config/SSH-Authentication-Methods

Possible values:

- LAN
- WAN
- WLAN

2.11.26.2 Methods

The SSH protocol generally allows two different authentication mechanisms: Username and password, using a public key, or interactively via the keyboard.

Telnet path: Setup/Config/SSH-Authentication-Methods

Possible values:

- Public-Key: Only allows authentication with a digital certificate.
- Keyboard-Interactive: Only allows authentication via the keyboard.
- Password: Only allows authentication with a password.
- Password+Keyboard-Interactive: Allows authentication with password or interactively via the keyboard.
- Password+Public-Key: Allows authentication using password or using digital certificate.
- Keyboard-Interactive+Public Key: Only allows authentication via the keyboard or via digital certificate.
- All: Allows authentication using any method.

Default: All

2.11.27 Predefined Admins

Here you will find the predefined administrator account for the device. This administrator account is used when no user name is defined when logging in.

Telnet path: Setup/Config/Predef.-Admins

2.11.27.1 Name

Enter the name of the predefined administrator account here.

Telnet path: Setup/Config/Predef.-Admins/Name

Possible values:

- Maximum 16 characters

Default: Blank

2.11.30 Update client

This menu contains the settings for the Update Client.

Telnet path: Setup/Config



The settings for the update client are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.11.30.1 Operating

Activates or deactivates the update client.

Telnet path: /Setup/Config/Update-Client

Possible values:

- No
- Yes

Default: No



The settings for the update client are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.11.30.4 Response-Timeout

Timeout in seconds for the update client to respond.

Telnet path: /Setup/Config/Update-Client

Possible values:

- Max. 10 numeric characters in the range 0 – 4289999999

Default: 3



The settings for the update client are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.11.30.7 Last firmware update

Date and time when the firmware was last updated.

Telnet path: /Setup/Config/Update-Client



The settings for the update client are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.11.30.8 Last config update

Date and time when the configuration was last updated.

Telnet path: /Setup/Config/Update-Client



The settings for the update client are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.11.30.2 Server name

This parameter specifies the server address that the device uses for the update client.

Telnet path: /Setup/Config/Update-Client

Possible values:

- Maximum 64 alphanumerical characters

Default: Blank



The settings for the update client are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.11.30.3 Server port

This parameter specifies the server address that the device uses for the update client.

Telnet path: /Setup/Config/Update-Client

Possible values:

■ Max. 5 numeric characters in the range 1 – 65535

Default: 12501



The settings for the update client are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.11.30.5 Retry failure

After this time in seconds, the device reports an error if the update server is not responding to requests.

Telnet path: /Setup/Config/Update-Client

Possible values:

■ Max. 10 numeric characters in the range 0 – 4289999999

Default: 60



The settings for the update client are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.11.30.6 Retry OK

Time in seconds for the update client, after which the device starts a new attempt to update.

Telnet path: /Setup/Config/Update-Client

Possible values:

■ Max. 10 numeric characters in the range 0 – 4289999999

Default: 86400



The settings for the update client are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.11.31 Anti-Theft-Protection

After being stolen, the device can theoretically be operated at another location by unauthorized persons. Password-protected device configurations do not stop third parties from operating RAS access, LAN connectivity or VPN connections that are set up in the device: A thief could gain access to a protected network. The device's operation can be protected in such a way that it will cease to function if there is an interruption to the power supply, or if the device is switched on in another location.

GPS location verification

GPS location verification enables a geographical position to be defined within the device. After being switched on the device automatically activates the GPS module and checks if it is located at the "correct" position. The router module only switches on if the check is positive. After location verification has been carried out the GPS module is switched off again, unless it was activated manually. ISDN location verification can prevent the misuse of a router: Each time it is switched on, the router carries out a check by making an ISDN telephone call to itself to ensure that it is installed at the intended location. Only after successful location verification is the router module activated.

ISDN location verification

The device must be reachable from the public ISDN telephone network. The device needs two free B channels for the duration of the check. If just one channel is free, e.g. one channel at a point-to-multipoint connection with two B channels is being used for a telephone call, then the device cannot make a call to itself via ISDN.

Telnet path: Setup/Config

2.11.31.3 Outgoing calling number

This number is called for ISDN location verification.

Telnet path: Setup/Config/Anti-Theft-Protection

Possible values:

■ Max. 14 characters

Default: Blank

2.11.31.8 Deviation

Deviation from the intended position in meters

Telnet path: Setup/Config/Anti-Theft-Protection

Possible values:

■ 50

2.11.31.10 Latitude

Latitude of the location where the device is to operate.

Telnet path: Setup/Config/Anti-Theft-Protection

Possible values:

■ Blank

2.11.31.4 Checked calling number

This call number is expected as outgoing call number for ISDN location verification.

Telnet path: Setup/Config/Anti-Theft-Protection

Possible values:

■ Max. 14 characters

Default: Blank

2.11.31.12 Get GPS position

This option allows the device to determine the geographical coordinates of its current location. Once the configuration is written back to the device, the current longitude and latitude are entered automatically, assuming that location verification is activated and a valid GPS position is available. Subsequently this option is automatically deactivated again.

Telnet path: Setup/Config/Anti-Theft-Protection

Possible values:

■ Yes

■ No

2.11.31.1 Enabled

Activate location verification with the 'Enabled' option. ISDN location verification can prevent the misuse of a router. Each time it is switched on, the router carries out a check by making an ISDN telephone call to itself to ensure that it is installed at the intended location. Only after successful location verification is the router module activated. Prerequisites for successful ISDN location verification: The device must be reachable from the public ISDN telephone network. The device needs two free B channels for the duration of the check. If just one channel is free, e.g. one channel at a point-to-multipoint connection with two B channels is being used for a telephone call, then the device cannot make a call to itself via ISDN.

Telnet path: Setup/Config/Anti-Theft-Protection

2.11.31.7 ISDN interface

The interface that this entry refers to.

Telnet path: Setup/Config/Anti-Theft-Protection

Possible values:

- S0-1
- S0-2

2.11.31.9 Longitude

Longitude of the location where the device is to operate.

Telnet path: Setup/Config/Anti-Theft-Protection

Possible values:

- Blank

2.11.31.6 Method

Select the method for the location check.

Telnet path: Setup/Config/Anti-Theft-Protection

Possible values:

- Basic call: 'Self call' for a check via ISDN by means of a return call.
- Facility: Call forwarding check via ISDN by requesting the call number from the exchange. No call-back is necessary in this case.
- GPS: GPS verification for a check on the geographical coordinates.



For a location check by GPS an appropriate GPS antenna must be connected to the AUX connector on the device. Additionally, a SIM card for mobile telephone operation has to be inserted and the device must be logged on to a mobile phone network. For ISDN location verification to function, the device must be reachable from the public ISDN telephone network. The device needs two free B channels for the duration of the check. If just one channel is free, e.g. one channel at a point-to-multipoint connection with two B channels is being used for a telephone call, then the device cannot make a call to itself via ISDN.

2.11.31.2 Called number

This call number is used as outgoing calling number when a call is made for ISDN location verification.

Telnet path: Setup/Config/Anti-Theft-Protection

Possible values:

- Max. 14 characters

Default: Blank

2.11.35 Monitor trace

This menu contains the settings for monitor tracing.

Telnet path: Setup/Config

2.11.35.1 Tracemask1

This parameter is for support purposes only.

Telnet path: /Setup/Config/Monitortrace

2.11.35.2 Tracemask2

This parameter is for support purposes only.

Telnet path: /Setup/Config/Monitortrace

2.11.43 Function keys

The function keys enable the user to save frequently used command sequences and to call them easily from the command line. In the appropriate table, commands are assigned to function keys F1 to F12 as they are entered in the command line.

Telnet path: Setup/Config

2.11.43.1 Key

Name of function key.

Telnet path: Setup\Config\Function-Keys

Possible values:

- Selection from function keys F1 to F12.

Default: F1

2.11.43.2 Mapping

Description of the command/shortcut to be run on calling the function key in the command line.

Telnet path: Setup\Config\Function-Keys

Possible values:

- All commands/shortcuts possible in the command line

Default: Blank

Special values: The caret symbol ^ is used to represent special control commands with ASCII values below 32. ^a

^A stands for Ctrl-A (ASCII 1)

^Z stands for Ctrl-Z (ASCII 26)

^[stands for Escape (ASCII 27)

^M stands for Return/Enter This character is useful if you enter a command with the function key and wish to send it immediately.

^^ A double caret symbol stands for the caret symbol itself.



If a caret symbol is entered in a dialog field or editor followed directly by another character, the operating system may possibly interpret this sequence as another special character. By entering caret + A the Windows operating system outputs an Å. To enter the caret character itself, enter a space in front of the subsequent characters. Sequence ^A is then formed from caret symbol + space + A.

2.11.50 LL2M

The menu contains the settings for LANCOM layer-2 management.

Telnet path: Setup/Config

2.11.50.1 Operating

Enables/disables the LL2M server. An LL2M client can contact an enabled LL2M server for the duration of the time limit following device boot/power-on.

Telnet path: /Setup/Config/LL2M

Possible values:

- Yes
- No

Default: Yes

2.11.50.2 Time limit

Defines the period in seconds during which an enabled LL2M server can be contacted by an LL2M client after device boot/power-on. The LL2M server is disabled automatically after expiry of the time limit.

Telnet path: /Setup/Config/LL2M

Possible values:

- 0 to 4294967295

Default: 0

Special values: 0 disables the time limit. The LL2M server stays permanently enabled in this state.

2.12 WLAN

This menu contains the settings for wireless LAN networks

Telnet path: /Setup

2.12.114 Aggregate retry limit

This parameter specifies how many times a set of packets to be sent by the hardware may be repeated until it is deferred while other packets waiting to be sent are transmitted. Restricting the number of repeat attempts to a small amount, e.g. in VoIP environments, limits the maximum delay for VoIP packets

Telnet path: /Setup/WLAN/Aggregate-Retry-Limit

Possible values:

- 0 to 255

Default: 255



The absolute value set under 'Hard-Retries' for transmission attempts remains unaffected by the setting here.

2.12.38 ARP handling

A station in the LAN attempting to establish a connection to a WLAN station which is in power-save mode will often fail or only succeed after a considerable delay. The reason is that the delivery of broadcasts (such as ARP requests) to stations in power-save mode cannot be guaranteed by the base station.

If you activate ARP handling, the base station responds to ARP requests on behalf of the stations associated with it, thus providing greater reliability in these cases.

Telnet path: /Setup/WLAN

Possible values:

- On

■ Off

Default: On



As of LCOS version 8.00, this switch activates a similar treatment for IPv6 neighbor solicitations.

2.12.48 Use full channel set

When 5 GHz and DFS are used, this parameter allows the use of channels 120, 124, 128 which are otherwise blocked for 'weather radar'.

Telnet path: /Setup/WLAN/Use-Full-Channelset

Possible values:

■ Yes

■ No

Default: No



Please note that activating this option constitutes a breach of ETSI regulations since no approval for these channels has been granted for LCOS.

2.12.44 Allow illegal association without authentication

The ability of the device to associate with a WLAN without authentication is enabled or disabled with this parameter.

Telnet path: /Setup/WLAN

Possible values:

■ Yes

■ No

Default: No

2.12.115 Omit global crypto sequence check

This is where you set the value for the crypto sequence check.

Telnet path: /Setup/WLAN

Possible values:

■ Auto

■ Yes

■ No

Default: Auto

Special values: Auto: LCOS contains a list of relevant devices. In the 'Auto' setting, the global sequence check is disabled. For other devices not included in this list, the global sequence check has to be disabled manually.

2.12.3 Spare heap

The heap reserve specifies how many blocks in the LAN heap can be reserved for direct communication (Telnet) with the device. If the number of blocks in the heap falls below the specified value, received packets are rejected immediately (except for TCP packets sent directly to the device).

Telnet path: /Setup/WLAN

Possible values:

■ Max. 3 numbers

Default: 10

2.12.13 IAPP announce interval

This is the interval (in seconds) with which the access points broadcast their SSIDs.

Telnet path: /Setup/WLAN

Possible values:

- Max. 10 numbers

Default: 120

2.12.14 IAPP handover timeout

If the handover is successful, the new access point informs the former access point that a certain client is now associated with another access point. This information enables the former access point to delete the client from its station table. This stops packets being (unnecessarily) forwarded to the client. For this time space (in milliseconds) the new access point waits before contacting the former access point again. After trying five times the new access point stops these attempts.

Telnet path: /Setup/WLAN

Possible values:

- Max. 10 numbers

Default: 1000

2.12.60 IAPP-IP network

Here you select the ARF network which is to be used as the IAPP-IP network.

Telnet path: /Setup/WLAN

Possible values:

- Select from the list of ARF networks defined in the device
- Maximum 16 alphanumerical characters

Default: Blank

Special values: Blank: If no IAPP-IP network is defined, IAPP announcements are transmitted on all of the defined ARF networks.

2.12.12 IAPP protocol

Access points use the Access Point Protocol (IAPP) to exchange information about their associated clients. This information is used in particular when clients roam between different access points. The new access point informs the former one of the handover, so that the former access point can delete the client from its station table.

Telnet path: /Setup/WLAN

Possible values:

- Yes
- No

Default: Yes

2.12.47 Idle timeout

This is the time in seconds during which the access point cannot receive any packets after a client is disconnected.

Telnet path: /Setup/WLAN/Idle-Timeout

Possible values:

- Max. 10 numerical characters

Default: 3600 seconds

2.12.26 Inter-SSID traffic

Depending on the application, it may be required that the WLAN clients connected to an access point can—or expressly cannot—communicate with other clients. Communications between clients in different SSIDs can be allowed or stopped with this option. For models with multiple WLAN modules, this setting applies globally to all WLANs and all modules.

Telnet path: /Setup/WLAN

Possible values:

■ Yes

■ No

Default: Yes



Communications between clients in a logical WLAN is controlled separately by the logical WLAN settings (Inter-Station-Traffic). If the Inter-SSID-Traffic is activated and the Inter-Station-Traffic deactivated, a client in one logical WLAN can communicate with clients in another logical WLAN. This option can be prevented with the VLAN settings or protocol filter.

2.12.100 Card reinitialize cycle

In this interval (in seconds) the internal WLAN cards in older access points are reinitialized in order for point-to-point connections to remain active. This function is handled by the "alive test" in newer models.

Telnet path: /Setup/WLAN

Possible values:

■ Max. 10 numbers

Default: 0

Special values: 0: Deactivates this function.

2.12.36 Country

The device needs to be set with the country where it is operating in order for the WLAN to use the parameters approved for the location.

Telnet path: /Setup/WLAN

Possible values:

■ Select from the list of countries.

Default: Unknown

Special values: Unknown: Only settings that are approved worldwide are permitted.

2.12.41 Mail address

Information about events in the WLAN is sent to this e-mail address.

Telnet path: /Setup/WLAN

Possible values:

■ Valid e-mail address

Default: Blank



An SMTP account must be set up to make use of the e-mail function.

2.12.46 Indoor only operation

If indoor-only operation is activated, the 5-GHz-band channels are limited to the 5.15 - 5.25 GHz spectrum (channels 36-48) in ETSI countries. Radar detection (DFS) is switched off and the mandatory interruption after 24 hours is no longer in effect. This mode reduces the risk of interruption due to false radar detections. In the 2.4-GHz band in France, the channels 8 to 13 are also permitted, meaning that more channels are available.

Telnet path: /Setup/WLAN

Possible values:

■ On

■ Off

Default: Off



Indoor operation may only be activated if the base station and all other stations are operated within an enclosed space.



Indoor operation may only be activated if the base station and all other stations are operated within an enclosed space.

2.12.108 Radar load threshold

This value indicates the percentage utilization of the wireless module at which the accuracy of radar detection is reduced.

Telnet path: /Setup/WLAN

Possible values:

■ Max. 3 numeric characters in the range 0 – 100

Default: 40

2.12.101 Noise calibration cycle

WLAN cards fitted with the Atheros chipset measure noise levels on the medium in this interval (in seconds).

Telnet path: /Setup/WLAN

Possible values:

■ Max. 10 numbers

Default: 0

Special values: 0: Deactivates this function.

2.12.105 Thermal recalibration cycle

In this interval (in seconds) WLAN cards fitted with the Atheros chipset adjust their transmission power to compensate for thermal variations.

Telnet path: /Setup/WLAN

Possible values:

■ Max. 10 numbers

Default: 20

Special values: 0: Deactivates this function.



Please note that deactivating the thermal recalibration cycle for these cards means that they cannot react to changes in temperature.

2.12.103 Trace MAC

The output of trace messages for the WLAN-Data-Trace can be set for a certain client. The corresponding MAC address is entered here.

Telnet path: /Setup/WLAN

Possible values:

■ Max. 12 hexadecimal characters

Default: 000000000000

Special values: 000000000000: Deactivates this function and outputs trace messages for all clients.

2.12.116 Trace packets

Similar to Trace MAC and Trace level, the output from WLAN DATA traces can be restricted by the type of packet sent or received, e.g. management (authenticate, association, action, probe-request/response), control (e.g. powersave poll), EAPOL (802.1x negotiation, WPA key handshake).

Telnet path: /Setup/WLAN

Possible values:

- One or more values from Management, Control, Data, EAPOL, All

Default: All

2.12.110 Trace level

The output of trace messages for the WLAN data trace can be restricted to contain certain content only. The messages are entered in the form of a bit mask for this.

Telnet path: /Setup/WLAN

Possible values:

- 0 to 255.
- 0: Reports that a packet has been received/sent
- 1: Adds the physical parameters for the packets (data rate, signal strength...)
- 2: Adds the MAC header
- 3: Adds the Layer-3 header (e.g. IP/IPX)
- 4: Adds the Layer-4 header (TCP, UDP...)
- 5: Adds the TCP/UDP payload

Default: 255

2.12.27 Supervise stations

In particular for public WLAN access points (public spots), the charging of usage fees requires the recognition of stations that are no longer active. Monitoring involves the access point regularly sending packets to logged-in stations. If the stations do not answer these packets, then the charging systems recognizes the station as no longer active.

Telnet path: /Setup/WLAN

Possible values:

- On
- Off

Default: Off

2.12.8 Access mode

You can limit the data traffic between the wireless LAN and its local network by excluding certain stations from transferring data, or you can approve specific stations only.

Telnet path: /Setup/WLAN

Possible values:

- Filter out data from listed stations, transfer all other
- transfer data from the listed stations, authenticate all other via RADIUS or filter them out

Default: Filter out data from listed stations, transfer all other

2.12.7 Access list

You can limit the data traffic between the wireless LAN and its local network by excluding certain stations from transferring data, or you can approve specific stations only.

Telnet path: /Setup/WLAN

2.12.7.1 MAC address

Enter the MAC address of a station.

Telnet path: Setup/WLAN/Access-List

Possible values:

- Valid MAC address

Default: Blank



Every network card has its own MAC address that is unique in the world. The address is a 12-character hexadecimal number (e.g. 00A057010203). This address can generally be found printed on the network card.

2.12.7.2 Name

You can enter any name you wish and a comment for any station.

This enables you to assign MAC addresses more easily to specific stations or users.

Telnet path: Setup/WLAN/Access-List

Possible values:

■ Max. 64 characters

Default: Blank

2.12.7.3 Comment

Comment on this entry

Telnet path: Setup/WLAN/Access-List

Possible values:

■ Max. 64 characters

Default: Blank

2.12.7.4 WPA passphrase

Here you may enter a separate passphrase for each physical address (MAC address) that is used in a 802.11i/WPA/AES-PSK-secured network. If no separate passphrase is specified for this MAC address, the passphrases stored in the '802.11i/WEP' area will be used for each logical wireless LAN network.

Telnet path: Setup/WLAN/Access-List

Possible values:

■ ASCII character string with a length of 8 to 63 characters

Default: Blank



This field has no significance for networks secured by WEP.



The passphrases should consist of a random string at least 22 characters long, corresponding to a cryptographic strength of 128 bits.

2.12.7.5 Tx limit

Bandwidth restriction for registering WLAN clients.

A client communicates its own settings to the base station when logging in. The base station uses these values to set the minimum bandwidth.

Telnet path: Setup/WLAN/Access-List

Possible values:

■ 0 to 4294967296 (2^{32})

Default: 0

Special values: 0: No limit



The significance of the Rx and Tx values depends on the device's operating mode. In this case, as an access point, Rx stands for "Send data" and Tx stands for "Receive data".

2.12.7.6 Rx limit

Bandwidth restriction for registering WLAN clients.

A client communicates its own settings to the base station when logging in. The base station uses these values to set the minimum bandwidth.

Telnet path: Setup/WLAN/Access-List

Possible values:

■ 0 to 4294967296 (2^{32})

Default: 0

Special values: 0: No limit



The significance of the Rx and Tx values depends on the device's operating mode. In this case, as an access point, Rx stands for "Send data" and Tx stands for "Receive data".

2.12.7.7 VLAN-ID

This VLAN ID is assigned to packets that are received from the client with the MAC address entered here.

Telnet path: Setup/WLAN/Access-List

Possible values:

■ 0 to 4096

Default: 0

2.12.29 RADIUS access check

This menu contains the settings for the RADIUS access checking

Telnet path: /Setup/WLAN

2.12.29.7 Response lifetime

This value defines the lifetime for an entry stored on the device for a MAC check that was rejected by the RADIUS server.

If a RADIUS server is used to check the MAC addresses of wireless clients, the device forwards all requests from wireless clients to the RADIUS server. If a MAC address is listed in the RADIUS server as blocked, then the reject response from the RADIUS server is stored in the device for the time set here. If the device receives repeated requests from blocked MAC addresses, the requests are not forwarded to the RADIUS server.

Telnet path: /Setup/WLAN/RADIUS-Access-Check

Possible values:

■ Max. 10 numeric characters ranging from 0 to 4294967295 ($2^{32}-1$)

Default: 15



Recently cached MAC address entries can be viewed in the table '1.3.48 RADIUS-Cache '.

2.12.29.2 Authentication port

Port for communication with the RADIUS server during authentication

Telnet path: /Setup/WLAN/RADIUS-Access-Check

Possible values:

■ Valid port specification

Default: 1812

2.12.29.5 Backup authentication port

Port for communication with the backup RADIUS server during authentication

Telnet path:/Setup/WLAN/RADIUS-Access-Check

Possible values:

- Valid port specification

Default: 1812

2.12.29.12 Backup loopback address

This is where you can configure an optional sender address to be used instead of the one otherwise automatically selected for the destination address.

If you have configured loopback addresses, you can specify them here as sender address.

Telnet path:/Setup/WLAN/RADIUS-Access-Check

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LBO... LBF for the 16 loopback addresses
- Any valid IP address

Default: Blank

2.12.29.14 Backup protocol

Protocol for communication between the backup RADIUS server and the clients.

Telnet path:/Setup/WLAN/RADIUS-Access-Check/Backup-Protocol

Possible values:

- RADIUS
- RADSEC

Default: RADIUS

2.12.29.6 Backup secret

Password used to access the backup RADIUS server

Telnet path:/Setup/WLAN/RADIUS-Access-Check

Possible values:

- Max. 64 characters

Default: Blank

2.12.29.4 Backup server IP address

IP address of the backup RADIUS server that checks the authorization of WLAN clients using the MAC address (authentication).

Telnet path:/Setup/WLAN/RADIUS-Access-Check

Possible values:

- Valid IP address.

Default: Blank

2.12.29.11 Loopback address

This is where you can configure an optional sender address to be used instead of the one otherwise automatically selected for the destination address.

If you have configured loopback addresses, you can specify them here as sender address.

Telnet path: /Setup/WLAN/RADIUS-Access-Check

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LBO to LBF for the 16 loopback addresses
- Any valid IP address

Default: Blank



If there is an interface named "DMZ", then its address is used.

2.12.29.8 Password source

Here you specify whether the device uses the shared secret or the MAC address as the password during authentication at the RADIUS server.

Telnet path: /Setup/WLAN/RADIUS-Access-Check

Possible values:

- Secret
- MAC address

Default: Secret

2.12.29.13 Protocol

Protocol for communication between the RADIUS server and the clients.

Telnet path: /Setup/WLAN/RADIUS-Access-Check

Possible values:

- RADSEC
- RADIUS

Default: RADIUS

2.12.29.9 Recheck cycle

If you select a value greater than zero, the device checks your MAC address not only at login but also during the connection in the specified cycle in seconds. If you specify zero, the MAC address is only checked at login. Cyclical rechecking enables the device to recognize, for example, a change in bandwidth limits for a MAC address. In this case the client remains logged on and the connection remains intact.

Telnet path: /Setup/WLAN/RADIUS-Access-Check

Possible values:

- Max. 10 numeric characters ranging from 0 – 4294967295 ($2^{32}-1$)

Default: 0

2.12.29.3 Secret

Password used to access the RADIUS server

Telnet path: /Setup/WLAN/RADIUS-Access-Check

Possible values:

- Max. 64 characters

Default: Blank

2.12.29.1 Server address

IP address of the RADIUS server that checks the authorization of WLAN clients using the MAC address (authentication).

Telnet path: /Setup/WLAN/RADIUS-Access-Check

Possible values:

- Valid IP address.

Default: Blank



To use the RADIUS functionality for WLAN clients, the option "Transfer data from the listed stations, authenticate all others via RADIUS or filter them out" must be selected for the "Filter stations" parameter. The general values for retry and timeout must also be configured in the RADIUS section.



WLAN clients must be entered as follows on the RADIUS server: The user name is the MAC address in the format AABBCC-DDDEFF. The password for all users is identical to the key (shared secret) for the RADIUS server.

2.12.29.10 Provide server database

Activate this option if the MAC address list is provided by a RADIUS server.

Telnet path: /Setup/WLAN/RADIUS-Access-Check

Possible values:

- No
- Yes

Default: Yes

2.12.45 RADIUS accounting

The accounting function in the LANCOM can be used to check the budgets of associated wireless LAN clients, among other things. Wireless Internet Service Providers (WISPs) use this option as a part of their accounting procedure. Accounting periods generally switch at the end of the month. A suitable action will cause the accounting session to be restarted at this time. Existing WLAN connections remain intact. A cron job can be used to automate a restart.

Telnet path: /Setup/WLAN

2.12.45.2 Accounting port

Port for communication with the RADIUS server during accounting

Telnet path: /Setup/WLAN/RADIUS-Accounting

Possible values:

- Valid port specification

Default: 1813

2.12.45.9 Excluded VLAN

Here you enter the ID of the VLAN that the device is to exclude from RADIUS accounting. The RADIUS server then receives no information about the traffic in that VLAN.

Telnet path: /Setup/WLAN/RADIUS-Accounting

Possible values:

- Max. 4 numeric characters in the range 0 – 9999
- 0 deactivates this function.

Default: 0

2.12.45.5 Backup authentication port

Port for communication with the backup RADIUS server during accounting

Telnet path: /Setup/WLAN/RADIUS-Accounting

Possible values:

- Valid port specification

Default: 1813

2.12.45.11 Backup loopback address

This is where you can configure an optional sender address to be used instead of the one otherwise automatically selected for the destination address.

If you have configured loopback addresses, you can specify them here as sender address.

Telnet path: /Setup/WLAN/RADIUS-Accounting

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LBO... LBF for the 16 loopback addresses
- Any valid IP address

Default: Blank

2.12.45.13 Backup protocol

Protocol for communication between the backup RADIUS server and the clients.

Telnet path: /Setup/WLAN/RADIUS-Accounting/Backup-Protocol

Possible values:

- RADIUS
- RADSEC

Default: RADIUS

2.12.45.6 Backup secret

Password used to access the backup RADIUS server

Telnet path: /Setup/WLAN/RADIUS-Accounting

Possible values:

- Max. 64 characters

Default: Blank

2.12.45.4 Backup server IP address

IP address of the backup RADIUS server used to perform accounting for WLAN clients.

Telnet path: /Setup/WLAN/RADIUS-Accounting

Possible values:

- Valid IP address.

Default: Blank

2.12.45.7 Client bridge handling

This item configures the device settings for RADIUS accounting when the device operates in client bridge mode.

Telnet path: /Setup/WLAN/RADIUS-Accounting

Possible values:

- All traffic: The device logs all traffic at the accounting server.
- Bridge traffic only: The device reports only the traffic generated by the client bridge itself to the accounting server.
- Client traffic only: The device reports only the traffic generated by the other stations in the client bridge to the accounting server.
- Separate accounting: In this mode, the device opens two separate sessions with the RADIUS server. One is used by the device to report the traffic of the bridge itself, and the other is used to report the traffic generated by the stations connected to the bridge.

Default: All traffic

2.12.45.8 Interim update period

This value sets the time interval in seconds after which the device sends an interim update to the accounting server.

Telnet path: /Setup/WLAN/RADIUS-Accounting

Possible values:

- Max. 10 numeric characters in the range 0 – 4289999999

Default: 0

2.12.45.10 Loopback address

This is where you can configure an optional sender address to be used instead of the one otherwise automatically selected for the destination address.

If you have configured loopback addresses, you can specify them here as sender address.

Telnet path: /Setup/WLAN/RADIUS-Accounting

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LB0 to LBF for the 16 loopback addresses
- Any valid IP address

Default: Blank



If there is an interface named "DMZ", then its address is used.

2.12.45.14 Restart accounting

This feature allows the device to end all running wireless LAN accounting sessions by sending an 'accounting stop' to the RADIUS server. This is helpful, for example, at the end of a billing period.

Telnet path: /Setup/WLAN/RADIUS-Accounting/Restart-Accounting

2.12.45.12 Protocol

Protocol for communication between the RADIUS server and the clients.

Telnet path: /Setup/WLAN/RADIUS-Accounting

Possible values:

- RADSEC
- RADIUS

Default: RADIUS

2.12.45.3 Secret

Password used to access the RADIUS server

Telnet path: /Setup/WLAN/RADIUS-Accounting

Possible values:

- Max. 64 characters

Default: Blank

2.12.45.1 Server address

IP address of the RADIUS server used to perform accounting for WLAN clients.

Telnet path: /Setup/WLAN/RADIUS-Accounting

Possible values:

- Valid IP address.

Default: Blank



The general values for retry and timeout must also be configured in the RADIUS section.



WLAN clients must be entered as follows on the RADIUS server: The user name is the MAC address in the format AABBCC-DDDEEFF. The password for all users is identical to the key (shared secret) for the RADIUS server.

2.12.50 Signal averaging

This menu contains the settings for signal averaging.

Telnet path: /Setup/WLAN



The settings for signal averaging are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.12.50.1 Method

Method for signal averaging.

Telnet path: /Setup/WLAN/Signal-Averaging

Possible values:

- Standard
- Filtered

Default: Standard



The settings for signal averaging are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.12.50.2 Standard parameters

This menu contains the configuration of the default parameters for signal averaging.

Telnet path: /Setup/WLAN/Signal-Averaging



The settings for signal averaging are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.12.50.2.1 Factor

Factor for the signal averaging.

Telnet path: /Setup/WLAN/Signal-Averaging/Standard-Parameters

Possible values:

■ Max. 3 numerical characters

Default: 4



The settings for signal averaging are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.12.50.3 Filtered parameters

This menu contains the configuration of the filtered parameters for signal averaging.

Telnet path: /Setup/WLAN/Signal-Averaging



The settings for signal averaging are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.12.50.3.1 Ct

Ct value for signal averaging.

Telnet path: /Setup/WLAN/Signal-Averaging/Filtered-Parameters

Possible values:

■ Max. 10 numerical characters

Default: 0



The settings for signal averaging are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.12.50.3.2 Coefficients

In this table the coefficients for filtering the parameters are defined.

Telnet path: /Setup/WLAN/Signal-Averaging/Filtered-Parameters



The settings for signal averaging are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.12.50.3.2.1 Index

Index of the table entry.

Telnet path: /Setup/WLAN/Signal-Averaging/Filtered-Parameters/Coefficients

Possible values:

- 1 to 24



The settings for signal averaging are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.12.50.3.2.2 Value

Value of the coefficient used for signal averaging.

Telnet path: /Setup/WLAN/Signal-Averaging/Filtered-Parameters/Coefficients

Possible values:

- Max. 11 numerical characters

Default: 0



The settings for signal averaging are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.12.107 Radar pattern thresholds

This table is used to define threshold values to be used when the radar detection is activated.

Telnet path: /Setup/WLAN



These settings are relevant for devices that operate according to ETSI EN 301 893 version 1.3. These settings have no meaning for devices compliant with ETSI EN 301 893 version 1.5 and later.

2.12.107.1 Pattern pps

Select one of the predefined radar patterns here to enter or change the threshold value for the radar pattern recognition.

Telnet path: /Setup/WLAN/Radar-Pattern-Thresholds

Possible values:

- 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 Threshold

The value entered here describes the accuracy with which the corresponding radar pattern is detected.

Telnet path: /Setup/WLAN/Radar-Pattern-Thresholds

Possible values:

- Max. 10 numeric characters in the range 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



Changing these default values may cause the device to operate in violation of the standard ETSI EN 301 893 version 1.3.

2.12.109 Noise offsets

This table is used to define the correction factors which adjust the displayed signal values.

Telnet path: /Setup/WLAN

2.12.109.1 Band

The noise-offset value is applied to the frequency band selected here.

Telnet path: /Setup/WLAN/Noise-Offsets

Possible values:

- Choose from the frequency bands supported by the device, e.g. 2.4 GHz or 5 GHz.

Default: 2.4 GHz

2.12.109.2 Channel

The noise-offset value is applied to the channel selected here.

Telnet path: /Setup/WLAN/Noise-Offsets

Possible values:

- Max. 5 numerical characters

Default: Blank

2.12.109.3 Interface

The noise-offset value is applied to the WLAN interface selected here.

Telnet path: /Setup/WLAN/Noise-Offsets

Possible values:

- Depend on the hardware capabilities, e.g. WLAN-1 or WLAN-2

Default: WLAN-1

2.12.109.4 Value

This numeric value is added to the current noise value.

Telnet path: /Setup/WLAN/Noise-Offsets

Possible values:

- Max. 3 numeric characters in the range 0 – 127

Default: 0

2.12.111 Noise immunity level

The settings for noise-immunity (Adaptive Noise Immunity - ANI) can be adjusted here.

Telnet path: /Setup/WLAN/Noise-Immunity



Under most conditions the settings for noise immunity are controlled automatically by the WLAN module driver according to the radio-field conditions. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.12.111.3 CCK weak signal detection threshold

This item sets the threshold value to be used for detecting weak CCK signals.

Telnet path: /Setup/WLAN/Noise-Immunity/CCK-Weak-Signal-Detection-Threshold

Possible values

- Numerical characters from 0 to 255

Default: 255



Under most conditions the settings for noise immunity are controlled automatically by the WLAN module driver according to the radio-field conditions. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.12.111.4 Fir step level

This item sets the value to be used for the fir step.

Telnet path: /Setup/WLAN/Noise-Immunity/Fir-Step

Possible values:

- Numerical characters from 0 to 255

Default: 255



Under most conditions the settings for noise immunity are controlled automatically by the WLAN module driver according to the radio-field conditions. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.12.111.2 OFDM weak signal detection

This item sets the threshold value to be used for detecting weak OFDM signals.

Telnet path: /Setup/WLAN/Noise-Immunity/OFDM-Weak-Signal-Detection

Possible values:

■ Numerical characters from 0 to 255

Default: 255



Under most conditions the settings for noise immunity are controlled automatically by the WLAN module driver according to the radio-field conditions. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.12.111.1 Noise immunity level

This item sets the threshold value to be used for noise immunity.

Telnet path: /Setup/WLAN/Noise-Immunity/Noise-Immunity-Level

Possible values:

■ Numerical characters from 0 to 255

Default: 255



Under most conditions the settings for noise immunity are controlled automatically by the WLAN module driver according to the radio-field conditions. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.12.111.5 Spurious immunity level

This item sets the threshold value to be used for spurious immunity.

Telnet path: /Setup/WLAN/Noise-Immunity/Spurious-Immunity-Level

Possible values

■ Numerical characters from 0 to 255

Default: 255



Under most conditions the settings for noise immunity are controlled automatically by the WLAN module driver according to the radio-field conditions. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.13 LANCAPI

LANCAPI from LANCOM Systems is a specialized version of the widespread ISDN CAPI interface. CAPI stands for Common ISDN Application Programming Interface and it links ISDN adapters and communications software. This software in turn provides the computer with office-communications functions such as a fax or answering machine.

Telnet path: /Setup

2.13.3 UDP port

You can change the UDP port number of the LANCAPI server here.

Telnet path: /Setup/LANCAPI/UDP-Port

Possible values: Max. 5 characters

Default: 75 (any private telephony service)

2.13.1 Access list

This table is for specifying addresses or address ranges that should have access to the server. If this table is empty, all users automatically have access.

Telnet path: Setup/LANCAPI/Access-List

2.13.1.1 IP address

An IP address that is to be granted access is entered here.

Telnet path: /Setup/LANCAPI/Priority-List/IP-Address

Possible values: Max. 15 characters

Default: Blank

2.13.1.2 IP netmask

Enter the associated netmask here.

If you wish to authorize just a single workstation with the previously specified IP address, enter **255.255.255.255** here. If you wish to authorize a whole IP network, enter the corresponding netmask.

Telnet path: /Setup/LANCAPI/Priority-List/IP-Netmask

Possible values: Max. 15 characters

Default: Blank

2.13.1.3 Routing tag

If you specify a routing tag for this access rule, the only packets that will be accepted have received the same tag in the firewall or they are from a network with the corresponding interface tag. If the routing tag is 0, access attempts from suitable IP addresses are accepted every time.

Telnet path: /Setup/LANCAPI/Access-List/Rtg-Tag

Possible values: Max. 5 characters

Default: Blank



It follows that the use of routing tags only makes sense in combination with the appropriate accompanying rules in the firewall or tagged networks.

2.13.6 Interface list

This list contains an entry for each device of your device. For each interface you can define whether it should be available for LANCAPI clients and which telephone numbers are to be used.

Telnet path: /Setup/LANCAPI

2.13.6.1 Ifc

This describes the interface (e.g. S0-1).

Telnet path: /Setup/LANCAPI/Interface-List

2.13.6.2 Operating

You can specify if and how this interface should be **available for LANCAP clients**. You can specify that, via this interface:

- All/yes
- None/no
- Dial-in only or
- Dial only

calls should be allowed.

Telnet path: /Setup/LANCAP/Interface-List

2.13.6.3 EAZ MSN(s)

If the LANCAP server should receive incoming calls, enter your ISDN telephone number which is to receive the LANCAP calls into the 'EAZ-MSNs' field. Multiple telephone numbers are separated by semicolons. If no telephone number is entered here, LANCAP receives calls at any of its ISDN telephone numbers.

Telnet path: /Setup/LANCAP/Interface-List

2.13.6.5 Force out MSN

If an outgoing call is not set with your own number, then this option determines that the number of this interface is set as your own number. Only activate this option if your PBX system does not allow outgoing calls without being set with your own number.

Telnet path: /Setup/LANCAP/Interface-List

Possible values:

- Yes
- No

Default: No

2.13.6.6 Max connections

A maximum limit can be placed on the number of connections per S0 bus (max. 3 characters)

Telnet path: /Setup/LANCAP/Interface-List

2.13.7 Priority list

This table is used to define the priorities of the ISDN interfaces for outgoing calls made with the LANCAP.

Telnet path: /Setup/LANCAP/Priority-List

2.13.7.1 Interface

Select the ISDN interface here for which you wish to set a priority value.

Telnet path: /Setup/LANCAP/Priority-List/Ifc

Possible values:

- Choose from the device's ISDN interfaces, e.g. S0-1

2.13.7.2 Priority out

Here you select the priority of the ISDN interface to be used for outgoing calls made with the LANCAP.

Telnet path: /Setup/LANCAP/Priority-List/Prio-out

Possible values:

- P1 (high priority) to P3 (low priority)

Default: P3

2.14 Time

This menu contains the configuration of the device time settings.

Telnet path: /Setup

2.14.2 Current time

Display of current time.

Telnet path: /Setup/Time

2.14.5 Call attempts

Specify the maximum number of dial attempts by the device to the specified number for the purpose of time initialization.

Telnet path: /Setup/Time

Possible values:

- Max. 3 digits

Default: 3

2.14.1 Fetch method

Select here if and how the device synchronizes its internal real-time clock.

Telnet path: /Setup/Time

Possible values:

- None
- ISDN
- NTP

Default: NTP

2.14.11 Daylight saving time

The time change between local standard time and daylight-saving time can be set here manually or automatically. For automatic daylight saving time adjustment, enter the appropriate time region for the location of your device. If your device is located outside the specified time regions, the use of automatic time adjustment requires you to select 'User defined' and for you to enter the following values into the table for automatic time adjustment.

Telnet path: /Setup/Time

Possible values:

- Yes
- No
- Europe (EU)
- Russia
- USA
- Userdefined

Default: Europe (EU)

2.14.13 Get time

This command causes the device to fetch the current time from the specified time server.

Telnet path: /Setup/Time

2.14.3 Time call number

Enter here a phone number that the device can call to obtain time information from the ISDN. After being switched on, the device will immediately dial this number and then disconnect the connection immediately. This transmits the current time from the ISDN exchange.

Telnet path: /Setup/Time

Possible values:

■ Max. 39 characters

Default: Blank

2.14.10 Timezone

This item sets the timezone for the location of your device. The time zone is the difference between local time and Coordinated Universal Time (UTC) in hours. This is especially important for the Network Time Protocol (NTP)

Telnet path: /Setup/Time

Possible values:

- 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 DST clock changes

Here you configure the individual values for the automatic clock change between summer and winter time, assuming that the local daylight-saving time settings have been selected as 'User defined'.

Telnet path: /Setup/Time

2.14.12.1 Event

Defines the beginning and end of daylight saving time

Telnet path: /Setup/Time/DST-Clock-Changes

2.14.12.2 Index

First or last day of month for switching to daylight-saving time (summertime).

Telnet path: /Setup/Time/DST-Clock-Changes

2.14.12.3 Day

Defines on which recurring weekday of the month the time change is carried out.

Telnet path: /Setup/Time/DST-Clock-Changes

2.14.12.4 Month

The month in which the change is carried out.

Telnet path: /Setup/Time/DST-Clock-Changes

2.14.12.5 Hour

The hour at which the change is carried out.

Telnet path: /Setup/Time/DST-Clock-Changes

2.14.12.6 Minute

The minute at which the change is carried out.

Telnet path: /Setup/Time/DST-Clock-Changes

2.14.12.7 Time type

Time standard, such as UTC (Coordinated Universal Time).

Telnet path: /Setup/Time/DST-Clock-Changes

2.14.15 Holidays

This table contains the holidays that have been defined.

Telnet path: /Setup/Time/Holidays

2.14.15.1 Index

This describes the position of the entry in the table.

Telnet path: /Setup/Time/Holidays/Index

Possible values:

■ 0 to 9999

Default: Blank

2.14.15.2 Date

If you have created entries in the least-cost table or the timed control table that should apply on public holidays, enter the days here.

Telnet path: /Setup/Time/Holidays/Date

Possible values:

- Valid date

Default: Blank

2.14.16 Timeframe

Timeframes are used to define the periods when the content-filter profiles are valid. One profile may have several lines with different timeframes. Different lines in a timeframe should complement each other, i.e. if you specify WORKTIME you will probably wish to specify a timeframe called FREETIME to cover the time outside of working hours.

Telnet path: /Setup/Time

2.14.16.1 Name

Enter the name of the timeframe for referencing from the content-filter profile.

Telnet path: /Setup/Time/Timeframe

Possible values:

- Name of a timeframe
- Maximum 31 characters

Default: Blank

2.14.16.2 Start

Here you set the start time (time of day) when the selected profile becomes valid.

Telnet path: /Setup/Time/Timeframe

Possible values:

- Max. 5 characters
- Format HH:MM

Default: 00:00

2.14.16.3 Stop

Here you set the end time (time of day) when the selected profile becomes invalid.

Telnet path: /Setup/Time/Timeframe

Possible values:

- Max. 5 characters
- Format HH:MM

Default: 11:59 PM

2.14.16.4 Weekdays

Here you select the weekday on which the timeframe is to be valid.

Telnet path: /Setup/Time/Timeframe

Possible values:

- Monday
- Tuesday

- Wednesday
- Thursday
- Friday
- Saturday
- Sunday
- Public holiday

Default: Activated for Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, Holiday

2.15 LCR

This menu contains the configuration of the least-cost router.

Telnet path: /Setup

2.15.2 Lancapi usage

If this option is activated, all connections made by CAPI clients are controlled by least-cost routing.

Telnet path: /Setup/LCR

Possible values:

- Yes
- No

Default: No

2.15.1 Router usage

A router is an intelligent network component; comparable with a post office, it uses the logical target address of a packet to determine which network component should transmit the packet next; it knows the overall topology of the network. If this option is activated, all connections made by the router are controlled by least-cost routing.

Telnet path: /Setup/LCR

Possible values:

- Yes
- No

Default: No

2.15.4 Time list

In this table you can define the Call-by-Call numbers to be used for telephone calls depending on the time, day and area code.

Telnet path: /Setup/LCR

2.15.4.1 Index

Index for this entry in the table.

Telnet path: /Setup/LCR/Time-List

Possible values:

- Max. 10 characters

Default: 0

2.15.4.2 Prefix

Enter the prefix (e.g. area code) or the first few digits of a group of prefixes to which the entry will apply. If, for example, you enter 030 for Berlin, all calls with this prefix will be redirected as indicated here. Optionally

you may wish to enter only 03 and then all calls to any place that begins with the prefix 03 will be redirected accordingly.

Telnet path: /Setup/LCR/Time-List

Possible values:

- Max. 10 characters

Default: Blank

2.15.4.3 Days

The days on which this entry should apply. You can create multiple entries for a given prefix, each applying to different periods or different days.

Telnet path: /Setup/LCR/Time-List

Possible values:

- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday
- Sunday
- Public holiday

Default: Blank

2.15.4.4 Start

The start of the period during which this entry should apply.

Telnet path: /Setup/LCR/Time-List

Possible values:

- Max. 5 characters

Default: Blank

2.15.4.5 Stop

The end of the period during which this entry should apply.

Telnet path: /Setup/LCR/Time-List

Possible values:

- Max. 5 characters

Default: Blank

2.15.4.6 Number list

Enter here the prefix for the call-by-call provider to be used for calls matching this entry.

Multiple prefixes can be separated by semi-colons. If no connection can be established with the first prefix, the following prefixes will be tried in sequence.

Leave this field empty if calls that match this entry are not to be re-directed.

Telnet path: /Setup/LCR/Time-List

Possible values:

- Max. 29 characters

Default: Blank

2.15.4.7 Fallback

Automatic fallback: If no connection can be established on any of the supplied call-by-call numbers, the least-cost router will connect to your regular telephone service provider. Switch this option off if you do not want this to happen.

Telnet path: /Setup/LCR/Time-List

Possible values:

- Yes
- No

Default: No

2.16 NetBIOS

This menu contains the configuration of the NetBIOS.

Telnet path: /Setup

2.16.9 Update

The device has to exchange routing information with other NetBIOS routers from time to time. To avoid unnecessary connections being established, select when this should occur.

Telnet path: /Setup/NetBIOS

Possible values:

- pBack
- Trig
- Time

Default: pBack

2.16.1 Operating

When this option is enabled, the router will also be able to forward NetBIOS packets directly to specific stations in remote networks. Without this option enabled, these packets often cause unnecessary connections, since the individual computers of NetBIOS-based networks (e.g. Microsoft Windows networks) continuously exchange status information.

Telnet path: /Setup/NetBIOS

Possible values:

- Yes
- No

Default: No

2.16.11 Lease time

The maximum time in minutes for which NetBIOS names remain valid.

A host registers with the device with a NetBIOS name. When this period expires, then the host must re-register with its name.

Telnet path: /Setup/NetBIOS

Possible values:

- Max. 10 numerical characters

Default: 500

2.16.2 Scope ID

The device appends this string to the NetBIOS name for all TCP/IP connections using NetBIOS.

Telnet path: /Setup/NetBIOS

Possible values:

- Max. 64 characters

Default: Blank

2.16.14 Support browsing

Windows uses the browser service or search service to discover the network environment. Since the browser service works with broadcasts, the network environment in routed networks is incomplete if no domains are used. Support of the search service closes this gap by propagating the master browser for each local workgroup to the remote side, or by using broadcasts in the LAN to propagate the master browsers located on the remote side. The list of master browsers known to the NetBIOS proxy can be viewed under /Status/TCP-IP/NetBIOS/Browser-List. Support of the search service only needs to be activated in workgroup networks. Domain networks operate without broadcasts, and the master browser is always the domain controller.

Telnet path: /Setup/NetBIOS/Support-Browsing

Possible values:

- Yes
- No

Default: Yes

2.16.10 WAN update minutes

If you have specified that routing information should be exchanged at particular intervals, enter this interval here in minutes.

Telnet path: /Setup/NetBIOS

Possible values:

- Max. 10 characters

Default: 60

2.16.8 Watchdogs

Some stations send watchdog packets from time to time to check whether other stations in the network can be reached. Watchdogs of this type can cause unnecessary connections to be established. Here you can specify whether the device should intercept watchdogs of this type and answer them itself to prevent these connections from being established.

Telnet path: /Setup/NetBIOS

Possible values:

- Spoof
- Route

Default: Spoof

2.16.4 Peers

Enter the name for the remote stations to which NetBIOS is to be transmitted over IP. These remote stations must also be entered in the IP routing table.

Telnet path: /Setup/NetBIOS

2.16.4.1 Name

Enter the name for the remote station here. This remote station must also be present in the routing table of the IP router.

Telnet path: /Setup/NetBIOS/Peers

Possible values:

- Max. 16 characters

Default: Blank

2.16.4.3 Type

Specify whether the remote station is also a router or an individual workstation with a dial-up remote-access connection.

Telnet path: /Setup/NetBIOS/Peers

Possible values:

- Workstation
- Router

Default: Router

2.16.5 Group list

This list displays all NetBIOS groups.

Telnet path: /Setup/NetBIOS

2.16.5.1 Group/Domain

Name of the workgroup communicated by NetBIOS.

Telnet path: /Setup/NetBIOS/Group-List

2.16.5.2 Type

NetBIOS defines a certain amount of server types, and these are displayed by hexadecimal numbers. The most important of these types are:

- Standard workstation 00
- Win PopUp service 03
- RAS server 06
- Domain master browser or PDC 1B
- Master browser 1D
- NetDDE service 1F
- File or printer service 20
- RAS client 21
- Network monitor agent BE
- Network monitor utility BF

Telnet path: /Setup/NetBIOS/Group-List

2.16.5.3 IP address

The station's IP address.

Telnet path: /Setup/NetBIOS/Group-List

Possible values:

- Valid IP address.

2.16.5.4 Peer

Name of the remote device that can be used to access this NetBIOS group.

Telnet path: /Setup/NetBIOS/Group-List

Possible values:

- Select from the list of defined peers.

2.16.5.5 Timeout

Period of validity (lease) of this entry in minutes.

Telnet path: /Setup/NetBIOS/Group-List

2.16.5.6 Flags

Flags as additional identifiers for the station or group.

Telnet path: /Setup/NetBIOS/Group-List

2.16.5.7 Network name

Name of the IP network where the client is located.

Telnet path: /Setup/NetBIOS/Group-List

2.16.5.8 Routing tag

Routing tag for this entry.

Telnet path: /Setup/NetBIOS/Group-List

2.16.6 Host List

This list displays all NetBIOS hosts.

Telnet path: /Setup/NetBIOS

2.16.6.1 Name

Name of the station communicated by NetBIOS.

Telnet path: /Setup/NetBIOS/Host-List

2.16.6.2 Type

NetBIOS defines a certain amount of server types, and these are displayed by hexadecimal numbers. The most important of these types are:

- Standard workstation 00
- Win PopUp service 03
- RAS server 06
- Domain master browser or PDC 1B
- Master browser 1D
- NetDDE service 1F
- File or printer service 20
- RAS client 21
- Network monitor agent BE
- Network monitor utility BF

Telnet path: /Setup/NetBIOS/Host-List

2.16.6.3 IP address

The station's IP address.

Telnet path: /Setup/NetBIOS/Host-List

Possible values:

- Valid IP address.

2.16.6.4 Peer

Name of the remote site that can be used to access this station.

Telnet path: /Setup/NetBIOS/Host-List

Possible values:

- Select from the list of defined peers.

2.16.6.5 Timeout

Period of validity (lease) of this entry in minutes.

Telnet path: /Setup/NetBIOS/Host-List

2.16.6.6 Flags

Flags as additional identifiers for the station or group.

Telnet path: /Setup/NetBIOS/Host-List

2.16.6.7 Network name

Name of the IP network where the client is located.

Telnet path: /Setup/NetBIOS/Host-List

2.16.6.8 Routing tag

Routing tag for this entry.

Telnet path: /Setup/NetBIOS/Host-List

2.16.7 Server list

This list displays all NetBIOS servers.

Telnet path: /Setup/NetBIOS

2.16.7.1 Host

Displays the host's NetBIOS name

Telnet path: /Setup/NetBIOS/Server-List

2.16.7.10 Flags

Displays the NetBIOS flags detected for the NetBIOS host.

Telnet path: /Setup/NetBIOS/Server-List

2.16.7.11 Network name

Displays the IP network where the NetBIOS host is located.

Telnet path: /Setup/NetBIOS/Server-List

2.16.7.12 Routing tag

Routing tag for the connection to the NetBIOS host.

Telnet path: /Setup/NetBIOS/Server-List

2.16.7.2 Group/Domain

Displays the workgroup/domain where the NetBIOS host is located.

Telnet path: /Setup/NetBIOS/Server-List

2.16.7.4 IP address

Displays the IP address of the NetBIOS host.

Telnet path: /Setup/NetBIOS/Server-List

2.16.7.5 OS ver.

Displays the NetBIOS host's operating system.

Telnet path: /Setup/NetBIOS/Server-List

2.16.7.6 SMB version

Displays the SMB version of the NetBIOS host.

Telnet path: /Setup/NetBIOS/Server-List

2.16.7.7 Server type

Displays the NetBIOS host's server type.

Telnet path: /Setup/NetBIOS/Server-List

2.16.7.8 Peer

Remote device over which the NetBIOS host can be reached.

Telnet path: /Setup/NetBIOS/Server-List

Possible values:

- Select from the list of defined peers.

2.16.7.9 Timeout

Displays the time in minutes until the NetBIOS information is updated.

Telnet path: /Setup/NetBIOS/Server-List

2.16.12 Networks

This table is used to adjust NetBIOS settings and to select the network that they apply to.

Telnet path: /Setup/NetBIOS

2.16.12.1 Network name

Select here the name of the network to which the settings are to apply.

Telnet path: /Setup/NetBIOS/Networks

Possible values:

■ Max. 16 characters

Default: Blank

2.16.12.2 Operating

Select here whether or not the NetBIOS proxy is to be used for the selected network.

Telnet path: /Setup/NetBIOS/Networks

Possible values:

■ Yes

■ No

Default: No

2.16.12.3 NT domain

Enter the name of the workgroup used by the computers in your network. If several workgroups exist within your network, entering one name is sufficient.

Telnet path: /Setup/NetBIOS/Networks

Possible values:

■ Max. 16 characters

Default: Blank

2.17 DNS

This menu contains the domain-name system (DNS) configuration.

Telnet path: /Setup

2.17.1 Operating

Activates or deactivates DNS.

Telnet path: /Setup/DNS/Operating

Possible values:

■ Yes

■ No

Default: Yes

2.17.3 DHCP usage

The DNS server can resolve the names of the stations that have requested an IP address by DHCP.

Use this switch to activate this option.

Telnet path: /Setup/DNS

Possible values:

■ Yes

■ No

Default: Yes

2.17.2 Domain

Device's own domain.

Telnet path: /Setup/DNS

Possible values:

■ Max. 64 characters

Default: Internal

2.17.12 Resolve domain

If this option is active, the device answers queries about its own domain with its own IP address.

Telnet path: /Setup/DNS

Possible values:

■ Yes

■ No

Default: Yes

2.17.7 Lease time

Some computers store the names and addresses of clients that they have queried from a DNS server in order to be able to access this information more quickly in the future.

Specify here how long this data may be stored before becoming invalid. After this time the computer in question must issue a new request for the information.

Telnet path: /Setup/DNS

Possible values:

■ Max. 10 characters

Default: 2000

2.17.4 NetBIOS usage

The DNS server can resolve the names of the clients that are known to the NetBIOS router.

Use this switch to activate this option.

Telnet path: /Setup/DNS

Possible values:

■ Yes

■ No

Default: Yes

2.17.5 DNS list

Enter the station names and the associated IP addresses here.

Telnet path: /Setup/DNS

2.17.5.1 Hostname

Enter the name of a station here.

For example, if you have a computer named myhost and your domain name is myhome.internal, then you should enter the station name here as myhost.myhome.intern.

Telnet path: /Setup/DNS/DNS-List

Possible values:

■ Max. 64 characters

Default: Blank

2.17.5.2 IP address

Enter the IP address of the station.

If a client needs to resolve the name of a station, it sends a request with that name to the DNS server. The server responds by communicating the IP address entered here.

Telnet path: /Setup/DNS/DNS-List

Possible values:

■ Valid IP address.

Default: 00.0.0

2.17.6 Filter list

Use the DNS filter to block access to certain stations or domains.

Telnet path: /Setup/DNS

2.17.6.1 Index

Index for the filter entries.

Telnet path: /Setup/DNS/Filter-List

Possible values:

■ Max. 4 characters

Default: Blank

2.17.6.2 Domain

Enter the name of a station or a domain that you want to block. The characters '*' and '?' can be used as wildcards.

Telnet path: /Setup/DNS/Filter-List

Possible values:

■ Max. 64 characters

Default: Blank

2.17.6.3 IP address

If you want this access restriction to only apply to a specific workstation or subnetwork, enter the IP address of the workstation or subnetwork here.

Telnet path: /Setup/DNS/Filter-List

Possible values:

■ Valid IP address.

Default: 00.0.0

2.17.6.4 Netmask

If you have entered the address of a subnetwork for access restriction, you must enter the associated subnet mask here.

Telnet path: /Setup/DNS/Filter-List

Possible values:

■ Valid IP address.

Default: 00.0.0



0

2.17.8 Dynamic DNS list

The Dyn DNS list records names that were registered via a register request. Windows does this when, for example, under Advanced TCP/IP Settings, "DNS", the network-connection options "Register this connection's addresses in DNS" and "Use this connection's DNS suffix in DNS registration" have been activated and the stations register in the domain.

Telnet path: /Setup/DNS

2.17.8.1 Hostname

Name of the station that registered via a register request.

Telnet path: /Setup/DNS/Dyn.-DNS-List

2.17.8.2 IP address

IP address of the station that registered via a register request.

Telnet path: /Setup/DNS/Dyn.-DNS-List

Possible values:

- Valid IP address.

2.17.8.3 Timeout

Lease period for this entry.

Telnet path: /Setup/DNS/Dyn.-DNS-List

2.17.9 DNS destinations

Requests for certain domains can be explicitly forwarded to particular remote sites.

Telnet path: /Setup/DNS

2.17.9.1 Domain name

Here you can enter the domain and assign it a dedicated remote device or a DNS server in order to resolve the name of a certain domain from another DNS server.

Telnet path: /Setup/DNS/DNS-Destinations

Possible values:

- Max. 64 characters

Default: Blank

2.17.9.2 Peer

Specify the remote station for DNS forwarding.

Telnet path: /Setup/DNS/DNS-Destinations

Possible values:

- Max. 31 characters

Default: Blank



0

2.17.10 Service location list

Here you configure if and to which station certain services are to be resolved.

Telnet path: /Setup/DNS

2.17.10.1 Service name

Specify here which service should be resolved by DNS, and how.

The service ID is the service that is to be resolved in accordance with RFC 2782.

By way of illustration, the following example lists several entries used to resolve SIP services: (Service-ID, station name, port)

■ _sips._tcp.myhome.intern . 0

■ _sip._tcp.myhome.intern myhost.myhome.intern 5060

■ _sip._udp.myhome.intern [self] 5060

Telnet path: /Setup/DNS/Service-Location-List

Possible values:

■ Max. 64 characters

Default: Blank

2.17.10.2 Hostname

The station name indicates which station provides the indicated service. For example, if you have a computer named myhost and your domain name is myhome.internal, then you should enter the station name here as myhost.myhome.intern. The station name '[self]' can be specified as the name if it is the device itself. A period '.' can be entered if this service is blocked and therefore should not be resolved. (In this case any definition in the following port field will be ignored).

Telnet path: /Setup/DNS/Service-Location-List

Possible values:

■ Max. 64 characters

Default: Blank

2.17.10.3 Port

The service port denotes the port number used for the defined service at the named client.

Telnet path: /Setup/DNS/Service-Location-List

Possible values:

■ Max. 10 characters

Default: 0

2.17.11 Dynamic SRV list

The dynamic SRV list stores service location records that the device uses itself. For example, the VoIP module enters itself here.

Telnet path: /Setup/DNS

2.17.11.1 Service name

Name of the service.

Telnet path: /Setup/DNS/Dynamic-SRV-List

2.17.11.2 Hostname

Name of the station providing this service.

Telnet path: /Setup/DNS/Dynamic-SRV-List

2.17.11.3 Port

Port used to register this service.

Telnet path: /Setup/DNS/Dynamic-SRV-List

2.17.13 Sub domains

Here a separate domain can be configured for each logical network.

Telnet path: /Setup/DNS

2.17.13.1 Network name

IP network for which a dedicated domain is to be defined.

Telnet path: /Setup/DNS/Sub-Domains

Possible values:

- Select from the list of defined IP networks.

Default: Blank

2.17.13.2 Sub-domain

Sub-domain that is to be used for the selected IP network.

Telnet path: /Setup/DNS/Sub-Domains

Possible values:

- Max. 64 characters

Default: Blank

2.18 Accounting

This menu contains the configuration of the Accounting.

Telnet path: /Setup

2.18.1 Operating

Turn accounting on or off.

Telnet path: /Setup/Accounting

Possible values:

- Yes
- No

2.18.10 Discriminator

This is where you can select the feature according to which accounting data are to be gathered. MAC address: The data are collected according to the client's MAC address. IP address: The data are collected according to the client's IP address. --> see information

Telnet path: /Setup/Accounting

Possible values:

- MAC address

- IP address



When varying IP addresses are in use, e.g. when using a DHCP server, the option 'IP address' can lead to inaccurate accounting data. In this case, it may not be possible to accurately assign the data to users. Conversely, with this setting, data can be separated from clients that are behind another router and therefore appear with the same MAC address as the router in the accounting list.

2.18.6 Delete accounting list

This option allows you to delete the parameters.

Telnet path: /Setup/Accounting

2.18.3 Sort by

Select here whether the data should be sorted in the accounting table according to connection times or data volume.

Telnet path: /Setup/Accounting

Possible values:

- Time
- Data

2.18.2 Save to flashrom

Turn accounting data in flash memory on or off. Accounting data saved to flash will not be lost even in the event of a power outage.

Telnet path: /Setup/Accounting

Possible values:

- Yes
- No

2.18.4 Current user

Displays an accounting list for all current users.

Telnet path: /Setup/Accounting

2.18.4.1 Username

Displays the username.

Telnet path: /Setup/Accounting/Current-User

2.18.4.3 Peer

Displays the name of the remote station.

Telnet path: /Setup/Accounting/Current-User

2.18.4.4 Connection type

Displays the connection type (e.g. DSL connection)

Telnet path: /Setup/Accounting/Current-User

2.18.4.5 Rx kbytes

The number of bytes received.

Telnet path: /Setup/Accounting/Current-User

2.18.4.6 Tx kbytes

The number of bytes sent.

Telnet path: /Setup/Accounting/Current-User

2.18.4.8 Total time

Shows the total time of the corresponding connection.

Telnet path: /Setup/Accounting/Current-User

2.18.4.9 Connection

Displays the number of connections.

Telnet path: /Setup/Accounting/Current-User

2.18.5 Accounting list

Information on connections between clients in the local network and various remote sites is saved in the accounting table with entries for the connection time and the transferred data volume. Using accounting snapshots, accounting data can be regularly saved at specific times for later evaluation.

Telnet path: /Setup/Accounting

2.18.5.1 Username

Displays the username.

Telnet path: /Setup/Accounting/Accounting-List

2.18.5.3 Peer

Displays the name of the remote station.

Telnet path: /Setup/Accounting/Accounting-List

2.18.5.4 Connection type

Displays the connection type (e.g. DSL connection)

Telnet path: /Setup/Accounting/Accounting-List

2.18.5.5 Rx kbytes

The number of bytes received.

Telnet path: /Setup/Accounting/Accounting-List

2.18.5.6 Tx kbytes

The number of bytes sent.

Telnet path: /Setup/Accounting/Accounting-List

2.18.5.8 Total time

Shows the total time of the corresponding connection.

Telnet path: /Setup/Accounting/Accounting-List

2.18.5.9 Connection

Displays the number of connections.

Telnet path: /Setup/Accounting/Accounting-List

2.18.8 Time snapshot

When configuring the snapshot, the interval is set at which the accounting data are temporarily saved into a snapshot.

Telnet path: /Setup/Accounting

2.18.8.1 Index

Displays the system's internal index.

Telnet path: /Setup/Accounting/Time-Snapshot

Default: 1

2.18.8.2 Operating

Turn intermediate storage of accounting data on or off.

Telnet path: /Setup/Accounting/Time-Snapshot

Possible values:

■ Yes

■ No

Default: No

2.18.8.3 Type

Here you can set the interval at which the snapshot will be generated.

Telnet path: /Setup/Accounting/Time-Snapshot

Possible values:

■ Daily

■ Weekly

■ Monthly

Default: Monthly

2.18.8.4 Day

The day of the month on which caching will be performed. Only relevant if the interval is 'monthly'.

Telnet path: /Setup/Accounting/Time-Snapshot

Possible values:

■ 0 to 31

Default: 1

2.18.8.5 DayOfWeek

The weekday on which caching will be performed. Only relevant if the interval is 'weekly'.

Telnet path: /Setup/Accounting/Time-Snapshot

Possible values:

■ 0 to 7

Default: Unknown

2.18.8.6 Hour

The hour of day at which caching will be performed.

Telnet path: /Setup/Accounting/Time-Snapshot

Possible values:

■ 0 to 23

Default: 0

2.18.8.7 Minute

The minute at which caching will be performed.

Telnet path: /Setup/Accounting/Time-Snapshot

Possible values:

■ 0 to 59

Default: 0

2.18.9 Last snapshot

Displays the last snapshot.

Telnet path: /Setup/Accounting

2.18.9.1 Username

Displays the username.

Telnet path: /Setup/Accounting/Last-Snapshot

2.18.9.3 Peer

Displays the name of the remote station.

Telnet path: /Setup/Accounting/Last-Snapshot

2.18.9.4 Connection type

Displays the connection type (e.g. DSL connection)

Telnet path: /Setup/Accounting/Last-Snapshot

2.18.9.5 Rx kbytes

The number of bytes received.

Telnet path: /Setup/Accounting/Last-Snapshot

2.18.9.6 Tx kbytes

The number of bytes sent.

Telnet path: /Setup/Accounting/Last-Snapshot

2.18.9.8 Total time

Shows the total time of the corresponding connection.

Telnet path: /Setup/Accounting/Last-Snapshot

2.18.9.9 Connection

Displays the number of connections.

Telnet path: /Setup/Accounting/Last-Snapshot

2.19 VPN

This menu contains the configuration of the Virtual Private Network (VPN).

Telnet path: /Setup

2.19.11 Aggressive mode IKE group default

This IKE group is used for aggressive-mode connections when the remote address cannot be identified by its IP address but by a subsequently transmitted ID.

Telnet path: /Setup/VPN

Possible values:

- MODP-768
- MODP-1024
- MODP-1536

Default: MODP-1024

2.19.10 Aggressive mode proposal list default

This IKE proposal list is used for aggressive-mode connections when the remote address cannot be identified by its IP address but by a subsequently transmitted ID.

Telnet path: /Setup/VPN

Possible values:

- Select from the list of defined IKE proposal lists.

Default: IKE_RSA_SIG

2.19.8 Operating

Switches the VPN module on or off.

Telnet path: /Setup/VPN

Possible values:

- Activated
- Deactivated

Default: Deactivated

2.19.22 Allow remote network selection

If simplified dial-in with certificates is activated for the device at headquarters, then the remote routers can suggest a network to be used for the connection during the IKE negotiation in phase 2. This network is ente-

red, for example, when setting up the VPN connection on the remote router. The device at headquarters accepts the suggested network when this option is activated. Moreover, the parameters used by the client during dial in must agree with the default values in the VPN router.

Telnet path: /Setup/VPN

Possible values:

- On
- Off

Default: Off



When configuring the dial-in remote sites, be sure to note that each remote site requests a specific network so that no network address conflicts arise.

2.19.25 Flexible ID comparison

This flexible method of identification comparison is activated or deactivated in the VPN configuration.

Telnet path: /Setup/VPN

Possible values:

- Yes
- No

Default: No



Flexible identity comparison is used when checking the (received) remote identity and also for selecting the certificate based on the local identity.

2.19.15 Legacy dyn. VPN (LCOS5.0x) support

Allows fallback from DynVPNv2 to DynVPNv1.

Telnet path: /Setup/VPN

Possible values:

- Yes
- No

Default: No

2.19.14 main mode IKE group default

This IKE group is used for main-mode connections when the remote address cannot be identified by its IP address but by a subsequently transmitted ID.

Telnet path: /Setup/VPN

Possible values:

- MODP-768
- MODP-1024
- MODP-1536

Default: MODP-1024

2.19.13 Main mode proposal list default

This IKE proposal list is used for main-mode connections when the remote address cannot be identified by its IP address but by a subsequently transmitted ID.

Telnet path: /Setup/VPN

Possible values:

- Select from the list of defined IKE proposal lists.

Default: IKE_PRESH_KEY

2.19.24 Max concurrent connections

This setting determines how many VPN connections the device can establish.

Telnet path: /Setup/VPN/Max-Concurrent-Connections

Possible values:

- The maximum value is limited by the relevant license.

Default: 0



With a value of 0, the device may take full advantage of the maximum number permitted by the license. Values above the license limits are ignored.

2.19.16 NAT-T operating

Enables the use of NAT-Traversal. NAT Traversal eliminates the problems that occur when establishing a VPN connection at the end points of the VPN tunnel.

Telnet path: /Setup/VPN

Possible values:

- On
- Off

Default: Off



NAT-T can only be used with VPN connections that use ESP (Encapsulating Security Payload) for authentication. Unlike AH (Authentication Header), ESP does not consider the IP header of the data packets when determining the hash value for authentication. The hash value calculated by the receiver is therefore also equivalent to the hash value entered in the packets.



If the LANCOM functions as a NAT router between the VPN end points, ensure that UDP ports 500 and 4500 are enabled in the firewall when you use NAT-T! This port is activated automatically if you use the firewall assistant in LANconfig.

2.19.26 NAT-T port for rekeying

This item sets whether the IKE packets are sent to port 500 (no) or the port 4500 (yes) during rekeying.

Telnet path: /Setup/VPN/NAT-T-Port-For-Rekeying

Possible values:

- Yes
- No

Default: No

2.19.20 Quick mode PFS group default

This IPSec group is used for simplified dial-in with certificates.

Telnet path: /Setup/VPN

Possible values:

- No PFS
- MODP-768
- MODP-1024
- MODP-1536

Default: MODP-1024

2.19.19 Quick mode proposal list default

This IPSec proposal list is used for simplified dial-in with certificates.

Telnet path: /Setup/VPN

Possible values:

- Select from the list of defined IPSec proposal lists.

Default: ESP_TN

2.19.21 Quick mode shorthold time default

This hold time is used for simplified dial-in with certificates.

Telnet path: /Setup/VPN

Possible values:

- 0 to 65535

Default: 0

2.19.23 Establish SAs collectively

Security Associations (SAs) are the basis for establishing a VPN tunnel between two networks. The establishment of Security Associations is normally initiated by an IP packet which is to be sent from a source network to a destination network.

The establishment of Security Associations is normally initiated by an IP packet which is to be sent from a source network to a destination network. This allows the setup of network relationships to be precise controlled according to the application.

Telnet path: /Setup/VPN

Possible values:

- Separately: Only the SA which corresponds explicitly to a packet waiting for transfer is to be established.
- Collectively: All SAs defined in the device will be established.
- Collectively with KeepAlive All of the defined SAs will be established for remote sites in the VPN connection list with a hold time set to '9999' (Keep Alive).

Default: Separately

2.19.27 SSL encapsulation allowed

Activate the 'SSL encaps' option in the general VPN settings to enable passive connection establishment to a VPN device from another VPN remote device using IPsec-over-HTTPS technology (LANCOM VPN device or LANCOM Advanced VPN client).

Telnet path: /Setup/VPN

Possible values:

- Yes, No

Default: No



The LANCOM Advanced VPN Client supports automatic fallback to IPsec over HTTPS. With this setting, the VPN client initially attempts to establish a connection without using the additional SSL encapsulation. If the connection cannot be made, the device then tries to connect with the additional SSL encapsulation.

2.19.17 Simple cert. RAS operating

Enables simplified dial-in with certificates. The simplification is that a shared configuration can be made for incoming connections, as long as the certificates of the remote peers are signed by the issuer of the root certificate in the device. In this case a configuration has to be made for each remote peer. You find the shared configuration necessary for this with the settings for default parameters. Individual remote peers can only be excluded from this function by having their certificates revoked in a CRL (Certificate Revocation List).

Telnet path: /Setup/VPN

Possible values:

- On
- Off

Default: Off

2.19.3 Isakmp

This menu contains the configuration of the Isakmp.

Telnet path: /Setup/VPN

2.19.3.4 Timer

This table contains values that affect the timing of IKE negotiations.

The values are passed to the IKE job with each full VPN configuration (setting up all VPN rules). Each time an IKE job is used it reads these values from its configuration. This means that the expiry timeout will be used immediately for every new negotiation (incl. rekeying of old connections). The retry limit is also used immediately, even during the ongoing repeats of negotiation packets.

Telnet path: /Setup/VPN/Isakmp

2.19.3.4.1 Retry limit

The retry limit specifies the maximum number of times that an IKE negotiation packet will be repeated if there is no response to it. The default value is '5'. The time interval between repeats currently cannot be configured and is 5, 7, 9, 11, 13... seconds. The overall time for IKE negotiation is also capped by the expiry limit.

Telnet path: /Setup/VPN/Isakmp/Timer

Possible values:

- Maximum 5 characters

Default: 5

2.19.3.4.2 Retry timer



These settings are included to maintain compatibility to earlier firmware versions. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

Telnet path: /Setup/VPN/Isakmp/Timer

2.19.3.4.3 Retr-Tim-Usec



These settings are included to maintain compatibility to earlier firmware versions. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

Telnet path: /Setup/VPN/Isakmp/Timer

2.19.3.4.4 Retr-Tim-Max



These settings are included to maintain compatibility to earlier firmware versions. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

Telnet path: /Setup/VPN/Isakmp/Timer

2.19.3.4.5 Exp-Tim

Maximum duration of the IKE negotiation phase in seconds.

Telnet path: /Setup/VPN/Isakmp/Timer

Possible values:

- 0 to 65535

Default: 30 seconds



These settings are included to maintain compatibility to earlier firmware versions. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.19.3.4.6 Index

The table contains only one line, so the index only has the value '1'.

Telnet path: /Setup/VPN/Isakmp/Timer

2.19.4 Proposals

This menu contains the configuration of the Proposals.

Telnet path: /Setup/VPN

2.19.4.9 IKE proposal lists

Here you can display and add IKE proposal lists.

Telnet path: /Setup/VPN/Proposals

2.19.4.9.1 IKE proposal lists

Name for the combination of IKE proposals

Telnet path: /Setup/VPN/Proposals/IKE-Proposal-Lists

Possible values:

- Max. 64 characters

Default: Blank

2.19.4.9.2 IKE-Proposal-1

Proposal to be used for this list.

Telnet path: /Setup/VPN/Proposals/IKE-Proposal-Lists

Possible values:

- Select from the defined IKE proposals

Default: Blank

2.19.4.9.3 IKE-Proposal-2

Proposal to be used for this list.

Telnet path: /Setup/VPN/Proposals/IKE-Proposal-Lists

Possible values:

- Select from the defined IKE proposals

Default: Blank

2.19.4.9.4 IKE-Proposal-3

Proposal to be used for this list.

Telnet path: /Setup/VPN/Proposals/IKE-Proposal-Lists

Possible values:

- Select from the defined IKE proposals

Default: Blank

2.19.4.9.5 IKE-Proposal-4

Proposal to be used for this list.

Telnet path: /Setup/VPN/Proposals/IKE-Proposal-Lists

Possible values:

- Select from the defined IKE proposals

Default: Blank

2.19.4.9.6 IKE-Proposal-5

Proposal to be used for this list.

Telnet path:/Setup/VPN/Proposals/IKE-Proposal-Lists

Possible values:

- Select from the defined IKE proposals

Default: Blank

2.19.4.9.7 IKE-Proposal-6

Proposal to be used for this list.

Telnet path:/Setup/VPN/Proposals/IKE-Proposal-Lists

Possible values:

- Select from the defined IKE proposals

Default: Blank

2.19.4.9.8 IKE-Proposal-7

Proposal to be used for this list.

Telnet path:/Setup/VPN/Proposals/IKE-Proposal-Lists

Possible values:

- Select from the defined IKE proposals

Default: Blank

2.19.4.9.9 IKE-Proposal-8

Proposal to be used for this list.

Telnet path:/Setup/VPN/Proposals/IKE-Proposal-Lists

Possible values:

- Select from the defined IKE proposals

Default: Blank

2.19.4.10 IPSEC proposal lists

Here you combine previously-defined proposals to form proposal lists.

Telnet path: /Setup/VPN/Proposals

2.19.4.10.1 IPSEC proposal lists

Name for the combination of IPSec proposals

Telnet path:/Setup/VPN/Proposals/IPSEC-Proposal-Lists

Possible values:

- Max. 64 characters

Default: Blank

2.19.4.10.2 IPSEC-Proposal-1

Proposal to be used for this list.

Telnet path:/Setup/VPN/Proposals/IPSEC-Proposal-Lists

Possible values:

- Select from the defined IPSec proposals

Default: Blank

2.19.4.10.3 IPSEC-Proposal-2

Proposal to be used for this list.

Telnet path:/Setup/VPN/Proposals/IPSEC-Proposal-Lists

Possible values:

- Select from the defined IPsec proposals

Default: Blank

2.19.4.10.4 IPSEC-Proposal-3

Proposal to be used for this list.

Telnet path: /Setup/VPN/Proposals/IPSEC-Proposal-Lists

Possible values:

- Select from the defined IPsec proposals

Default: Blank

2.19.4.10.5 IPSEC-Proposal-4

Proposal to be used for this list.

Telnet path: /Setup/VPN/Proposals/IPSEC-Proposal-Lists

Possible values:

- Select from the defined IPsec proposals

Default: Blank

2.19.4.10.6 IPSEC-Proposal-5

Proposal to be used for this list.

Telnet path: /Setup/VPN/Proposals/IPSEC-Proposal-Lists

Possible values:

- Select from the defined IPsec proposals

Default: Blank

2.19.4.10.7 IPSEC-Proposal-6

Proposal to be used for this list.

Telnet path: /Setup/VPN/Proposals/IPSEC-Proposal-Lists

Possible values:

- Select from the defined IPsec proposals

Default: Blank

2.19.4.10.8 IPSEC-Proposal-7

Proposal to be used for this list.

Telnet path: /Setup/VPN/Proposals/IPSEC-Proposal-Lists

Possible values:

- Select from the defined IPsec proposals

Default: Blank

2.19.4.10.9 IPSEC-Proposal-8

Proposal to be used for this list.

Telnet path: /Setup/VPN/Proposals/IPSEC-Proposal-Lists

Possible values:

- Select from the defined IPsec proposals

Default: Blank

2.19.4.11 IKE

In this table, you can define proposals for managing the SA negotiation.

Telnet path: /Setup/VPN/Proposals

2.19.4.11.1 Name

Name for the combinations of IKE parameters that should be used as the proposal.

Telnet path: /Setup/VPN/Proposals/IKE

Possible values:

- Max. 64 characters

Default: Blank



The Internet Key Exchange (IKE) is a protocol for authentication and key exchange.

2.19.4.11.2 IKE cryptographic algorithm

Encryption algorithm for this proposal

Telnet path: /Setup/VPN/Proposals/IKE

Possible values:

- AES
- Blowfish
- CAST128
- 3DES
- DES
- NIL

Default: AES-CBC

2.19.4.11.3 IKE cryptographic key length

Key length for this proposal

Telnet path: /Setup/VPN/Proposals/IKE

Possible values:

- 0 to 65535

Default: 128

2.19.4.11.4 IKE authentication algorithm

Hash algorithm for the encryption

Telnet path: /Setup/VPN/Proposals/IKE

Possible values:

- MD5
- SHA1

Default: MD5

2.19.4.11.5 IKE authentication mode

Authentication method for this proposal

Telnet path: /Setup/VPN/Proposals/IKE

Possible values:

- Preshared key: Symmetrical PSK requires the key to be known at both ends of the connection.
- RSA signature: Asymmetrical method with private and public keys, known from Rivest, Shamir Adleman.

Default: Preshared Key

2.19.4.11.6 Lifetime seconds

Validity of the connections negotiated with this proposal with respect to connection duration

Telnet path: /Setup/VPN/Proposals/IKE

Possible values:

- 0 to 65535

Default: 8000 seconds

Special values: 0: No limit on connection time

2.19.4.11.7 Lifetime KB

Validity of the connections negotiated with this proposal with respect to transmitted data volume.

Telnet path: /Setup/VPN/Proposals/IKE

Possible values:

- 0 to 65535

Default: 0 kBytes

Special values: 0: No limit on data volume

2.19.4.12 IPSEC

You can define the defaults for encryption, authentication or compression here.

Telnet path: /Setup/VPN/Proposals

2.19.4.12.1 Name

Name for the combinations of IPsec parameters that should be used as the proposal.

Telnet path: /Setup/VPN/Proposals/IPSEC

Possible values:

- Max. 64 characters

Default: Blank



IPsec stands for “IP Security Protocol” and was originally the name used by a working group of the IETF, the Internet Engineering Task Force. Over the years, this group has developed a framework for a secure IP protocol that today is generally referred to as IPsec.

2.19.4.12.2 Encapsulation mode

Connection mode selection

Telnet path: /Setup/VPN/Proposals/IPSEC

Possible values:

- Transport: In transport mode, the IP header of the original packet is left unchanged and the ESP header, encrypted data and both trailers are inserted. The IP header contains the unchanged IP address. Transport mode can therefore only be used between two end points, for the remote configuration of a router, for example. It cannot be used for the connectivity of networks via the Internet – this would require a new IP header with the public IP address of the recipient. In such cases, ESP can be used in tunnel mode.
- Tunnel: In tunnel mode, the entire packet including the original IP header is encrypted and authenticated and the ESP header and trailers are added at the entrance of the tunnel. A new IP header is added to this new packet, this time with the public IP address of the recipient at the end of the tunnel.

Default: Tunnel

2.19.4.12.3 ESP cryptographic algorithm

Encryption algorithm for this proposal

Telnet path: /Setup/VPN/Proposals/IPSEC

Possible values:

- AES
- Blowfish
- CAST128
- 3DES
- DES
- NIL

Default: AES-CBC

2.19.4.12.4 ESP cryptographic key length

Key length for this proposal

Telnet path: /Setup/VPN/Proposals/IPSEC

Possible values:

- 0 to 65535

Default: 128

2.19.4.12.5 ESP authentication algorithm

ESP authentication method for this proposal

Telnet path: /Setup/VPN/Proposals/IPSEC

Possible values:

- HMAC-MD5
- HMAC-SHA1
- No authentication

Default: HMAC-MD5

2.19.4.12.6 AH authentication algorithm

AH authentication method for this proposal

Telnet path: /Setup/VPN/Proposals/IPSEC

Possible values:

- HMAC-MD5
- HMAC-SHA1
- No AH

Default: No AH

2.19.4.12.7 IPCOMP algorithm

Compression method for this proposal

Telnet path: /Setup/VPN/Proposals/IPSEC

Possible values:

- No IPCOMP
- Deflate
- LZS

Default: No IPCOMP

2.19.4.12.8 Lifetime seconds

Validity of the connections negotiated with this proposal with respect to connection duration

Telnet path: /Setup/VPN/Proposals/IPSEC

Possible values:

- 0 to 65535

Default: 8000 seconds

Special values: 0: No limit on connection time

2.19.4.12.9 Lifetime KB

Validity of the connections negotiated with this proposal with respect to transmitted data volume.

Telnet path: /Setup/VPN/Proposals/IPSEC

Possible values:

- 0 to 65535

Default: 0 kBytes

Special values: 0: No limit on data volume

2.19.5 Certificate keys

This menu contains the configuration of the certificates and keys.

Telnet path: /Setup/VPN

2.19.5.3 IKE keys

Entered here are the shared key for preshared-key authentication and the identities for preshared-key- and RSA signature authentication.

Telnet path: /Setup/VPN/Certificates-and-Keys

2.19.5.3.1 Name

Name for the combination of identities and keys

Telnet path: /Setup/VPN/Certificates-and-Keys/IKE-Keys

Possible values:

■ Max. 64 characters

Default: Blank

2.19.5.3.2 Remote identity

Remote ID that the entered key is to be valid for.

Telnet path: /Setup/VPN/Certificates-and-Keys/IKE-Keys

Possible values:

■ Max. 64 characters

Default: Blank

2.19.5.3.3 Shared secret

Key/secret that should apply to this combination.

Telnet path: /Setup/VPN/Certificates-and-Keys/IKE-Keys

Possible values:

■ Max. 64 characters

Default: Blank

2.19.5.3.4 Shared secret file

[obsolete, not used: File with PSK]

Telnet path: /Setup/VPN/Certificates-and-Keys/IKE-Keys

2.19.5.3.5 Remote ID type

Type of remote ID that the entered key is to be valid for.

Telnet path: /Setup/VPN/Certificates-and-Keys/IKE-Keys

Possible values:

■ No identity

■ IP address

■ Domain name (FQDN)

■ E-mail address (FQUN)

■ ASN.1 distinguished name

Default: No identity

2.19.5.3.6 Local ID type

Type of local ID that the entered key is to be valid for.

Telnet path: /Setup/VPN/Certificates-and-Keys/IKE-Keys

Possible values:

■ No identity

■ IP address

■ Domain name (FQDN)

■ E-mail address (FQUN)

■ ASN.1 distinguished name

Default: No identity

2.19.5.3.7 Local identity

Local ID that the entered key is to be valid for.

Telnet path: /Setup/VPN/Certificates-and-Keys/IKE-Keys

Possible values:

- Max. 64 characters

Default: Blank

2.19.7 Layer

Define other parameters for the individual VPN connections here.

Telnet path: /Setup/VPN

2.19.7.1 Name

Name for the combination of connection parameters

Telnet path: /Setup/VPN/Layer

Possible values:

- Max. 64 characters

Default: Blank

2.19.7.3 PFS group

Perfect Forward Secrecy (PFS) is a security feature of encryption algorithms. The PFS group specifies the length of the Diffie-Hellman key used to encrypt the IKE negotiation.

Telnet path: /Setup/VPN/Layer

Possible values:

- No PFS
- MODP-768
- MODP-1024
- MODP-1536

Default: MODP-1024

2.19.7.4 IKE group

The IKE group specifies the length of the Diffie-Hellman key used to encrypt the IKE negotiation.

Telnet path: /Setup/VPN/Layer

Possible values:

- MODP-768
- MODP-1024
- MODP-1536

Default: MODP-1024

2.19.7.5 IKE proposal list

IKE proposal list for this connection.

Telnet path: /Setup/VPN/Layer

Possible values:

- Select from the list of defined IKE proposal lists.

Default: Blank

2.19.7.6 IPSEC proposal list

IKE key for this connection.

Telnet path: /Setup/VPN/Layer

Possible values:

- Select from the list of defined IKE keys.

Default: Blank

2.19.7.7 IKE key

IPsec proposal list for this connection.

Telnet path: /Setup/VPN/Layer

Possible values:

- Select from the list of defined IPsec proposal lists.

Default: Blank

2.19.9 VPN peers

In this table you define the VPN connections to be established by your device.

Telnet path: /Setup/VPN

2.19.9.1 Peer

Name of the VPN connection.

Telnet path: /Setup/VPN/VPN-Peers

Possible values:

- Select from the list of defined peers.

Default: Blank

2.19.9.10 DPD-inactivity timeout

Dead peer detection is used when VPN clients dial in to a VPN gateway or when 2 VPN gateways are connected. This is designed to ensure that a peer is logged out if there is an interruption to the VPN connection, for example when the Internet connection is interrupted briefly. If the line were not to be monitored, then the VPN gateway would continue to list the client or the other VPN gateway as logged-on. This would prevent the peer from dialing in again as, for example, the LANCOM Advanced VPN Client does not allow a simultaneous dial-in using the same serial number.

With dead-peer detection, the gateway and peer regularly exchange "keep alive" packets. If no replies are received, the gateway will log out the peer so that this ID can be registered anew once the VPN connection has been re-established. The DPD time for VPN clients is typically set to 60 seconds.

Telnet path: /Setup/VPN/VPN-Peers

Possible values:

- 0 to 9999 numerical characters

Default: 0



Without line monitoring, a user with the same "identity" (user name) would be prevented from dialing in because the associated user would still be in the list for the logged-in peer.

2.19.9.11 IKE configuration

When configuring VPN dial-in connections, there is as an alternative to fixed IP addresses for the remote sites that dial in, in that a pool of IP addresses can be made available to them. To this end, the "IKE-CFG" mode is additionally added to the entries in the connection list.

Telnet path: /Setup/VPN/VPN-Peers

Possible values:

- Off: If the IKE-CFG mode is switched off, no IP addresses will be assigned for the connection. Fixed IP addresses must be defined for both ends of the connection.
- Client: With this setting, the device functions as the client for this VPN connection and requests an IP address from the remote site (server). The device acts in a similar manner to a VPN client.
- Server: With this setting, the device functions as the server for this VPN connection. The assignment of an IP address to the client can take place in two ways:
 - If the remote site is entered in the routing table, the IP address defined here will be assigned to the client.
 - If the remote site is not entered in the routing table, an IP address which is available from the IP pool will be taken for the dial-in connections.

Default: Off



When set as server, the remote site must be configured as IKE-CFG client, and thus has to request an IP address from the server. To dial in with a LANCOM Advanced VPN Client, the option "Use IKE Config Mode" has to be activated in the connection profile.

2.19.9.12 XAUTH

Enables the use of XAUTH for the VPN remote site selected.

Telnet path: /Setup/VPN/VPN-Peers

Possible values:

- Client: In the XAUTH client operating mode, the device starts the initial phase of IKE negotiation (Main mode or Aggressive mode) and then waits for the authentication request from the XAUTH server. The XAUTH client responds to this request with the user name and password from the PPP table entry in which the PPP remote site corresponds to the VPN remote site defined here. There must therefore be a PPP remote site of the same name for the VPN remote site. The user name defined in the PPP table normally differs from the remote site name.
- Server: In the XAUTH server operating mode, the device (after successful negotiation of the initial IKE negotiation) starts authentication with a request to the XAUTH client, which then responds with its user name and password. The XAUTH server searches for the user name in the PPP table and, if a match is found, it checks the password. The user name for this entry in the PPP table is not used.
- Off: No XAUTH authentication is performed for the connection to this remote site.

Default: Off



If XAUTH authentication is enabled for a VPN remote site, the IKE-CFG option must be set to the same value.

2.19.9.13 SSL-Encaps.

With this option you activate IPsec-over-HTTPS technology when actively establishing a connection to this remote site.

Telnet path: /Setup/VPN/VPN-Peers

Possible values:

- Yes, No

Default: No



Please note that when the IPsec-over-HTTPS option is activated, the VPN connection can only be established when the remote site also supports this technology and when the remote site is set up to receive passive VPN connections that use IPsec over HTTPS.

2.19.9.15 Routing tag

Routing tags are used on the LANCOM in order to evaluate criteria relevant to the selection of the target route in addition to the IP address. The only routes in the routing table to be used are those with a matching routing tag. The routing tag for each VPN connection can be specified here. The routing tag is used to determine the route to the remote gateway.

Telnet path: /Setup/VPN/VPN-Peers

Possible values:

- 0 to 65535

Default: 0

2.19.9.2 Extranet address

If an IP address is specified here, the IP addresses of the local stations behind this IP address will be masked. This is only necessary for specialized scenarios.

Telnet path: /Setup/VPN/VPN-Peers

Possible values:

- Valid IP address.

Default: Blank

2.19.9.4 Layer

Combination of connection parameters (PFS, IKE and IPsec parameters) that should be used for this connection.

Telnet path: /Setup/VPN/VPN-Peers

Possible values:

- Select from the list of defined connection parameters.

Default: Blank

2.19.9.5 Dynamic

LANCOM Dynamic VPN is a technology which permits VPN tunnels to be connected even to remote sites that do not have a static IP address, but a dynamic one instead.

Telnet path: /Setup/VPN/VPN-Peers

Possible values:

- No dynamic VPN
- Dynamic VPN: A connection is established to transmit IP addresses
- Dynamic VPN: IP addresses are transmitted without establishing a connection if possible:
- Dynamic VPN: An ICMP packet is sent to the remote site to transmit the IP address
- Dynamic VPN: A UDP packet is sent to the remote site to transmit the IP address

Default: No dynamic VPN

2.19.9.6 Short-hold time

This value specifies the number of seconds that pass before a connection to this remote site is terminated if no data is being transferred.

Telnet path: /Setup/VPN/VPN-Peers

Possible values:

■ 0 to 9999

Default: 0

Special values: With the value 9999, connections are established immediately and without a time limit.

2.19.9.7 IKE exchange

Selects the IKE exchange mode

Telnet path: /Setup/VPN/VPN-Peers

Possible values:

■ Main mode

■ Aggressive mode

Default: Main mode



Main Mode exchanges significantly more unencrypted messages during the IKE handshake than the Aggressive Mode. This is why main mode is far more secure than the aggressive mode.

2.19.9.8 Remote gateway

DNS name or IP address of the remote gateway which is to be used to set up the VPN connection.

Telnet path: /Setup/VPN/VPN-Peers

Possible values:

■ Max. 64 characters

Default: Blank

2.19.9.9 Rule creation

On/off switch and type of rule creation

Telnet path: /Setup/VPN/VPN-Peers

Possible values:

■ Off: No VPN rule is created for the remote site.

■ Automatic: Automatically created VPN rules connect the local IP networks with the IP networks entered into the routing table for the remote site.

■ Manually: VPN rules are only created for the remote site for IP network relationships specified "Manually" in the firewall configuration.

Default: Automatic

2.19.12 Additional gateways

This table is used to specify a list of possible gateways for each remote site.

Telnet path: /Setup/VPN

2.19.12.1 Peer

Name of the VPN connection that works with the additional gateway defined here.

Telnet path: /Setup/VPN/Additional-Gateways

Possible values:

■ Select from the list of defined VPN connections.

Default: Blank

2.19.12.10 Begin with

Here you select the first gateway that is to be used for establishing the VPN connection.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

- First: Start with the first entry in the list.
- Random: Selects a random entry from the list.
- Last used: Selects the entry for the connection which was successfully used most recently.

Default: Last used

2.19.12.2 Remote gateway 1

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

- Max. 63 characters

Default: Blank

2.19.12.11 Routing tag 1

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

- 0 to 65535

Default: 0

2.19.12.3 Remote gateway 2

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

- Max. 63 characters

Default: Blank

2.19.12.12 Routing tag 2

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

- 0 to 65535

Default: 0

2.19.12.4 Remote gateway 3

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

- Max. 63 characters

Default: Blank

2.19.12.13 Routing tag 3

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ 0 to 65535

Default: 0

2.19.12.5 Remote gateway 4

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.14 Routing tag 4

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ 0 to 65535

Default: 0

2.19.12.6 Remote gateway 5

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.15 Routing tag 5

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ 0 to 65535

Default: 0

2.19.12.7 Remote gateway 6

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.16 Routing tag 6

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ 0 to 65535

Default: 0

2.19.12.8 Remote gateway 7

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.17 Routing tag 7

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ 0 to 65535

Default: 0

2.19.12.9 Remote gateway 8

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.18 Routing tag 8

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ 0 to 65535

Default: 0

2.19.12.19 Remote gateway 9

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ Max. 64 characters

Default: Blank

2.19.12.27 Routing tag 9

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ 0 to 65535

Default: 0

2.19.12.20 Remote gateway 10

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.28 Routing tag 10

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ 0 to 65535

Default: 0

2.19.12.21 Remote gateway 11

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.29 Routing tag 11

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ 0 to 65535

Default: 0

2.19.12.22 Remote gateway 12

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.30 Routing tag 12

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ 0 to 65535

Default: 0

2.19.12.23 Remote gateway 13

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.31 Routing tag 13

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ 0 to 65535

Default: 0

2.19.12.24 Remote gateway 14

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.32 Routing tag 14

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ 0 to 65535

Default: 0

2.19.12.25 Remote gateway 15

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.33 Routing tag 15

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional-Gateways

Possible values:

■ 0 to 65535

Default: 0

2.19.12.26 Remote gateway 16

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional-Gateways

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.34 Routing tag 16

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional-Gateways

Possible values:

■ 0 to 65535

Default: 0

2.19.12.35 Gateway-17

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional-Gateways/Gateway-17

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.36 Rtg-Tag-17

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional-Gateways/Rtg-Tag-17

Possible values:

■ 0 to 65535

Default: 0

2.19.12.37 Gateway-18

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional-Gateways/Gateway-18

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.38 Rtg-Tag-18

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways/Rtg-Tag-18

Possible values:

■ 0 to 65535

Default: 0

2.19.12.39 Gateway-19

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways/Gateway-19

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.40 Rtg-Tag-19

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways/Rtg-Tag-19

Possible values:

■ 0 to 65535

Default: 0

2.19.12.41 Gateway-20

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways/Gateway-20

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.42 Rtg-Tag-20

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways/Rtg-Tag-20

Possible values:

■ 0 to 65535

Default: 0

2.19.12.43 Gateway-21

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways/Gateway-21

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.44 Rtg-Tag-21

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways/Rtg-Tag-21

Possible values:

■ 0 to 65535

Default: 0

2.19.12.45 Gateway-22

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways/Gateway-22

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.46 Rtg-Tag-22

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways/Rtg-Tag-22

Possible values:

■ 0 to 65535

Default: 0

2.19.12.47 Gateway-23

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways/Gateway-23

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.48 Rtg-Tag-23

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways/Rtg-Tag-23

Possible values:

■ 0 to 65535

Default: 0

2.19.12.49 Gateway-24

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways/Gateway-24

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.50 Rtg-Tag-24

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways/Rtg-Tag-24

Possible values:

■ 0 to 65535

Default: 0

2.19.12.51 Gateway-25

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways/Gateway-25

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.52 Rtg-Tag-25

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways/Rtg-Tag-25

Possible values:

■ 0 to 65535

Default: 0

2.19.12.53 Gateway-26

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways/Gateway-26

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.54 Rtg-Tag-26

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways/Rtg-Tag-26

Possible values:

■ 0 to 65535

Default: 0

2.19.12.55 Gateway-27

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways/Gateway-27

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.56 Rtg-Tag-27

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways/Rtg-Tag- 27

Possible values:

■ 0 to 65535

Default: 0

2.19.12.57 Gateway-28

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways/Gateway- 28

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.58 Rtg-Tag-28

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways/Rtg-Tag- 28

Possible values:

■ 0 to 65535

Default: 0

2.19.12.59 Gateway-29

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways/Gateway- 29

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.60 Routing tag 29

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Certificate- Keys/Additional- Gateway- List/Rtg-Tag- 29

Possible values:

■ 0 to 65535

Default: 0

2.19.12.61 Gateway-30

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways/Gateway- 30

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.62 Rtg-Tag-30

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways/Rtg-Tag-30

Possible values:

■ 0 to 65535

Default: 0

2.19.12.63 Gateway-31

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways/Gateway-31

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.64 Rtg-Tag-31

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways/Rtg-Tag-31

Possible values:

■ 0 to 65535

Default: 0

2.19.12.65 Gateway-32

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Telnet path: /Setup/VPN/Additional- Gateways/Gateway-32

Possible values:

■ Max. 63 characters

Default: Blank

2.19.12.66 Rtg-Tag-32

Enter the routing tag for setting the route to the relevant gateway.

Telnet path: /Setup/VPN/Additional- Gateways/Rtg-Tag-32

Possible values:

■ 0 to 65535

Default: 0

2.20 LAN bridge

This menu contains the settings for the LAN bridge.

Telnet path: /Setup

2.20.12 Aging time

When a client requests an IP address from a DHCP server, it can also ask for a lease period for the address. This values governs the maximum length of lease that the client may request. When a client requests an address without asking for a specific lease period, the value set here will apply.

Telnet path: /Setup/LAN-Bridge

Possible values:

■ 1 to 99,999 minutes

Default: Max. validity 6,000 min., default validity: 500 min.

2.20.2 Bridge priority

This value sets the priority of the bridge in the LAN. This value influences which bridge the spanning tree protocol takes to be the root bridge. This is a 16-bit value (0 .. 65535), where higher values mean lower priority. You should only change the default value if you prefer a certain bridge. The selection process still works even if all the values are the same because, if the priorities are identical, the device uses the MAC address of the bridge to make the decision.

Telnet path: /Setup/LAN-Bridge/Bridge-Priority

Possible values:

■ Max. 5 numerical characters

Default: 32768



Even though an entire 16-bit parameter is available for configuring this parameter, special care should be taken where newer versions of the rapid or multiple spanning tree protocol are involved. The priority value should only be changed in increments of 4096, because the lower 12 bits are used for other purposes. This could mean that these values may be ignored by future firmware releases.

2.20.7 Forward delay

This value determines the time (in seconds) that passes before a port should change from 'listening' to 'learning' or from 'learning' to 'forwarding'. However, now that rapid spanning tree offers a method of determining when a port can be switched into the 'forwarding state' without a long wait, this setting in many cases no longer has any effect.

Telnet path: /Setup/LAN bridge/Forward-Delay

Possible values:

■ Max. 5 numerical characters

Default: 6

2.20.6 Hello time:

This parameter specifies the time interval in seconds in which the device operating as the root bridge sends information to the LAN.

Telnet path: /Setup/LAN-Bridge/Hello-Time

Possible values:

■ Max. 5 numerical characters

Default: 2

2.20.8 Isolated mode

This item allows connections to be switched on or off, such as those between layer-2 forwarding and the LAN interfaces.

Telnet path: /Setup/LAN-Bridge

Possible values:

■ Bridge or router (isolated mode)

Default: Bridge



Please note that other functions relating to the connection (e.g. spanning tree, packet filters) continue to function, independent of whether the interfaces are switched on or off.

2.20.5 Maximum age

This value defines the time (in seconds) after which a bridge drops messages received through Spanning Tree as 'outdated'. This defines how quickly the spanning-tree algorithm reacts to changes, for example due to failed bridges. This is a 16-bit value (0 .. 65535).

Telnet path: /Setup/LAN-Bridge/Max-Age

Possible values:

- Max. 5 numerical characters

Default: 20

2.20.1 Protocol version

Select the desired protocol here. Depending on the choice made here, the device uses either the classic protocol or the rapid protocol, as defined in the IEEE 802.1D-1998, chapter 8 and IEEE 802.1D-2004 chapter 17 respectively.

Telnet path: /Setup/LAN-Bridge/Protocol-Version

Possible values:

- Classic
- Rapid

Default: Classic

2.20.4 Encapsulation table

This table is used to add the encapsulation methods.

Telnet path: /Setup/LAN-Bridge

2.20.4.1 Protocol

A protocol is identified by its 16-bit protocol identifier carried in the Ethernet II/SNAP type field (often referred to as the Ethertype). The protocol type is written as a hexadecimal number from 0001 to ffff. Even if the table is empty, some protocols are implicitly assumed to be listed in this table as type SNAP (such as IPX and AppleTalk). This can be overridden by explicitly setting their protocol to Ethernet II.

Telnet path: /Setup/LAN-Bridge/Encapsulation-Table

2.20.4.2 Encapsulation

Here you can specify whether or not data packets are to be given an Ethernet header when being transmitted. Normally you should enter the option "Transparent". The "Ethernet" option should only be chosen if you wish to combine a layer for use with the bridge.

Telnet path: /Setup/LAN-Bridge/Encapsulation-Table

Possible values:

- Transparent
- Ethernet

Default: Transparent

2.20.10 Protocol table

You can add the protocols to be used over the LAN bridge here.

Telnet path: /Setup/LAN-Bridge

2.20.10.1 Name

This name should describe the rule. Note that this is also the content column (index column) of the table, i.e. the content of the table is a string.

Telnet path: /Setup/LAN-Bridge/Protocol-Table

Possible values:

- Max. 15 characters

Default: Blank

2.20.10.10 IP network

If the first field is set to a value unequal to 0.0.0.0, a packet will match this rule only if it is an IPv4 packet and either the packet's source or destination address are contained in the IP network defined by these two values.

Telnet path: /Setup/LAN-Bridge/Protocol-Table

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.20.10.11 IP netmask

If the first field is set to a value unequal to 0.0.0.0, a packet will match this rule only if it is an IPv4 packet and either the packet's source or destination address are contained in the IP network defined by these two values.

Telnet path: /Setup/LAN-Bridge/Protocol-Table

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.20.10.12 DHCP source MAC

This setting decides whether matching of the rule shall depend on a packet's source MAC address, i.e. whether it is the MAC address of a host that received its IP address via DHCP.

DHCP tracking on a particular (W)LAN interface only takes place when protocol filters for the interface have been defined with the parameter "IP allocated by DHCP" set to Yes or No. Additionally, a network can be specified for a filter rule. However, if a rule has the parameter "IP allocated by DHCP" set to Yes, then a given network could be ignored.

Telnet path: /Setup/LAN-Bridge/Protocol-Table

Possible values:

- Irrelevant
- No
- Yes

Default: Irrelevant

2.20.10.2 Protocol

The identifier of the protocol is entered here. The identifier is a 4-digit hexadecimal number that uniquely identifies each protocol. Common protocols include 0800, 0806 for IP and ARP (Internet), E0E0, 8137 for IPX (Novell Netware), F0F0 for NetBEUI (Windows networks), or 809B, 80F3 for AppleTalk (Apple networks). If you set the protocol field to zero, this rule affects all packets. Other protocols are referred to in the documentation.

Telnet path: /Setup/LAN-Bridge/Protocol-Table

Possible values:

- 4-digit hexadecimal number

Default: Blank

2.20.10.3 Sub-protocol

Enter the sub-protocol here. Common sub-protocols within the IP protocol (0800) include 1 ICMP, 6 TCP, 17 UDP, 50 ESP (IPsec). This field specifies the ARP frame type (ARP request/reply, RARP request/reply) for ARP packets. If this value is unequal to 0, the rule will only match if either the packet is an IPv4 packet and the IP protocol (UDP, TCP, ICMP,...) matches the given value, or if it is an ARP packet and the ARP type matches the given value. If the protocol field is set, but the sub-protocol field is set to 0, then the rule applies to all packets of the specified protocol (e.g. for all IP packets for protocol 0800). Note: Further information is to be found at www.iana.org under the section "Protocol Number Assignment Services", documents "Protocol Numbers" and "Port Numbers".

Telnet path: /Setup/LAN-Bridge/Protocol-Table

Possible values:

■ Maximum 65,535

Default: 0

2.20.10.4 Port

This specifies the range of port numbers for the TCP or UDP protocols. For example, UDP port 500 corresponds to the IKE used by IPsec.

If this value is not equal to 0, then the rule only applies when an IPv4 TCP or UDP packet arrives or when the source of the target TCP/UDP port is within the range defined by these two values.

If '0' is entered as the end port, the rule applies only for the start port. The port numbers of the receiving port and the target port are compared, and a rule applies if just one of these is within the defined range. If the protocol and the sub-protocol are set, but the port fields have the value 0, then the rule applies to all packets of the specified sub-protocol (e.g. for all packets for protocol 0800/6). Note: Further information is to be found at www.iana.org under the section "Protocol Number Assignment Services", documents "Protocol Numbers" and "Port Numbers".

Telnet path: /Setup/LAN-Bridge/Protocol-Table

Possible values:

■ Maximum 65,535

Default: 0

2.20.10.5 Port end

This specifies the range of port numbers for the TCP or UDP protocols. For example, UDP port 500 corresponds to the IKE used by IPsec.

If this value is not equal to 0, then the rule only applies when an IPv4 TCP or UDP packet arrives or when the source of the target TCP/UDP port is within the range defined by these two values.

If '0' is entered as the end port, the rule applies only for the start port. The port numbers of the receiving port and the target port are compared, and a rule applies if just one of these is within the defined range. If the protocol and the sub-protocol are set, but the port fields have the value 0, then the rule applies to all packets of the specified sub-protocol (e.g. for all packets for protocol 0800/6). Note: Further information is to be found at www.iana.org under the section "Protocol Number Assignment Services", documents "Protocol Numbers" and "Port Numbers".

Telnet path: /Setup/LAN-Bridge/Protocol-Table

Possible values:

■ Maximum 65,535

Default: 0

2.20.10.6 Interface list

This list contains the LAN interfaces for which the rule applies. The syntax of the interface list is specified in addenda/supplements/attachments.

The following pre-defined interface descriptors are used to specify the relevant interfaces in a comma-separated expression:

- 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' refers to the interface of the wireless LAN network and 'm' is the number of the P2P connection on this WLAN).

Numerically consecutive interface identifiers can be described by the following abbreviations: P2P-4~P2P-10. If no interface is specified here, the selected action will never be executed.

Telnet path: /Setup/LAN-Bridge/Protocol-Table

Possible values:

- All LAN interfaces
- DMZ interfaces
- Logical WLAN networks and the point-to-point bridges in the WLAN

Default: Blank

2.20.10.7 Action

This field defines the action to be taken on a packet if it matches the rule. A packet may be discarded (Drop), passed unchanged (Pass), or redirected to a different IP address. For redirection, the IP address that the packet is to be redirected to must be specified in the following field. The redirect feature is only available for packets that support TCP, UDP, or ICMP echo requests. The device will modify the destination MAC and IP address fields before forwarding the packet, and will put an entry in the Connection Table to allow back translation of possible answers.

Telnet path: /Setup/LAN-Bridge/Protocol-Table

Possible values:

- Pass
- Drop
- Redirect

Default: Drop packets

2.20.10.8 Redirect IP address

If the rule is a redirect rule, this field must be used to specify which IP address the appropriate packets are to be redirected to.

Telnet path: /Setup/LAN-Bridge/Protocol-Table

Possible values:

- Valid IP address.

Default: 0.0.0.0

2.20.10.9 Destination MAC address

The physical address (MAC) of a destination station in the wireless LAN is entered here. Every network card has its own MAC address that is unique in the world. The address is a 12-character hexadecimal number (e.g. 00A057010203). This address can generally be found printed on the network card. If you enter no MAC address (or zero), this rule affects all packets.

Telnet path: /Setup/LAN-Bridge/Protocol-Table

Possible values:

- 12-digit hexadecimal number

Default: Blank

2.20.11 Port

This table can be used to set further bridge parameters for each port.

Telnet path: /Setup/LAN-Bridge

2.20.11.2 Port

Selects the port for which the spanning tree parameters are to be set.

Telnet path: /Setup/LAN-Bridge/Port

Possible values:

- Select from the list of the device's logical interfaces, e.g. LAN-1, WLAN-1 or P2P-1-1

2.20.11.3 Active

This can be used to block a port completely, i.e. the port will always have the 'disabled' status.

Telnet path: /Setup/LAN-Bridge/Port

Possible values:

- Active
- Inactive

Default: Activated

2.20.11.5 Bridge group

Assigns the logical interface to a bridge group to enable bridging from/to this logical interface via the LAN bridge. If assigned to a common bridge group, several logical interfaces can be addressed at once and they appear to the LANCOM Wireless to be a single interface. This can then be used for Advanced Routing and Forwarding, for example.

Telnet path: /Setup/LAN-Bridge/Port

Possible values:

- BRG-1 bis BRG-8
- None

Default: BRG - 1

Special values: If the interface is removed from all bridge groups by setting 'none', then there is no communication between the LAN and WLAN via the LAN bridge (isolated mode). With this setting, LAN/WLAN data transfers over this interface are only possible via the router.



A requirement for data transfer from/to a logical interface via the LAN bridge is the deactivation of the global "isolated mode" which applies to the whole of the LAN bridge. Furthermore, the logical interface must be assigned to a bridge group. With the setting 'none', no transfers can be made via the LAN bridge.

2.20.11.6 DHCP limit

Number of clients which can be handled by DHCP. If the limit is exceeded, the oldest entry is dropped. This feature can be used in combination with the protocol filter table to limit access to just one logical interface.

Telnet path: /Setup/LAN-Bridge/Port

Possible values:

- 0 to 255

Default: 0

2.20.11.7 Point-to-point port

This item corresponds to the "adminPointToPointMAC" setting as defined in IEEE 802.1D. By default, the "point-to-point" setting for the LAN interface is derived from the technology and the concurrent status:

An Ethernet port is assumed to be a P2P port if it is operating in full-duplex mode.

A token ring port is assumed to be a P2P port if it is operating in full-duplex mode.

A WLAN SSID is never considered to be a P2P port.

A WLAN P2P connection is always assumed to be a P2P port.

However, this automatic setting can be revised if this is unsuitable for the required configuration. Interfaces in "point-to-point" mode have various specialized capabilities, such as the accelerated port status change for working with the rapid spanning tree protocol.

Telnet path: /Setup/LAN-Bridge/Port

Possible values:

- Automatic
- Yes
- No

Default: Automatic

2.20.13 Priority mapping

This table assigns a user priority to each IP packet due to be sent, based on a ToS/DSCP value as per 802.1D. An example of how user priority can be used concerns wireless LANs with activated QoS, where the packets are allocated to access categories (voice/video/best-effort/background).

Telnet path: /Setup/LAN- Bridge/ Priority- Mapping

2.20.13.1 Name

Enter a name for a combination of DSCP value and priority.

Telnet path: /Setup/LAN- Bridge/ Priority- Mapping/ Name

Possible values:

- Maximum 16 alphanumeric characters

Default: Blank

2.20.13.2 DSCP value

Enter the DSCP value that is used for this priority assignment.

Telnet path: /Setup/LAN- Bridge/ Priority- Mapping/ DSCP- Value

Possible values:

- Numerical characters from 0 to 255

Default: 0

2.20.13.3 Priority

Enter the priority that is used for this priority assignment.

Telnet path: /Setup/LAN- Bridge/ Priority- Mapping/ Priority

Possible values:

- Best effort
- Background

- Two
- Excellent effort
- Controlled latency
- Video
- Voice
- Network control

Default: Best effort

2.20.20 Spanning tree

This menu contains the settings for the spanning tree.

Telnet path: /Setup/LAN-Bridge

2.20.20.1 Operating

Here you can switch the Spanning-Tree support on and off. When Spanning Tree is turned off, the router does not send any Spanning Tree packets and passes received packets along instead of processing them itself.

Telnet path: /Setup/LAN-Bridge/Spanning-Tree

Possible values:

- Active
- Inactive

Default: Deactivated

2.20.20.2 Bridge priority

This value sets the priority of the bridge in the LAN. This can influence which bridge should preferably be made root bridge by the spanning tree protocol. This is a 16-bit value (0 .. 65535), where higher values mean lower priority. The default value should only be changed if a certain bridge is to be preferred. The selection process still works even if all the values are the same because, if the priorities are identical, the bridge's MAC address is used to make the decision. Even though an entire 16-bit parameter is available for configuring a parameter, special care should be taken where newer versions of the rapid or multiple spanning tree protocol are involved. The priority value should only be changed in increments of 4096, because the lower 12 bits are used for other purposes. This could mean that these values may be ignored by future firmware releases.

Telnet path: /Setup/LAN-Bridge/Spanning-Tree

Possible values:

- Maximum 65,535

Default: 32768

2.20.20.7 Forward delay

This value determines the time (in seconds) that passes before a port should change from 'listening' to 'learning' or from 'learning' to 'forwarding'. However, now that rapid spanning tree offers a method of determining when a port can be switched into the "forwarding state" without a long wait, this setting in many cases no longer has any effect. Do not change this value without detailed knowledge of spanning tree, since it may increase the risk of temporary loops in the network.

Telnet path: /Setup/LAN-Bridge/Spanning-Tree

Possible values:

- Max. 32768 seconds

Default: 6 seconds

2.20.20.6 Hello time

The Hello Time specifies the time interval (in seconds) for sending root-bridge information to the LAN. Note that the non-root bridge can adopt values from the root bridge. This value might be ignored depending on the topology of the network.

Telnet path: /Setup/LAN-Bridge/Spanning-Tree

Possible values:

■ Max. 32768 seconds

Default: 2 seconds

2.20.20.5 Maximum age

This value defines the time (in seconds) after which a bridge drops messages received through Spanning Tree as 'outdated'. This defines how quickly the spanning-tree algorithm reacts to changes, for example due to failed bridges.

Telnet path: /Setup/LAN-Bridge/Spanning-Tree

Possible values:

■ Max. 65535 seconds

Default: 20 seconds

2.20.20.14 Path cost computation

This item sets the protocol to be used for calculating the path cost. While the rapid spanning tree method uses the full 32-bit value range, the classic algorithm only works with a 16-bit value range. The rapid spanning tree method is only useful if it is supported by all bridges in the network and it is consistently configured.

Telnet path: /Setup/LAN-Bridge/Spanning-Tree

Possible values:

■ Classic

■ Rapid

Default: Classic

2.20.20.12 Protocol version

This item selects the spanning-tree protocol version to be used. Setting this switch to 'Classic' will engage the algorithm defined in IEEE 802.1D-1998 chapter 8, while setting it to 'Rapid' will engage the rapid spanning tree scheme defined by IEEE 802.1D-2004 chapter 17.

Telnet path: /Setup/LAN-Bridge/Spanning-Tree

Possible values:

■ Classic

■ Rapid

Default: Classic



Note the upward compatibility of this protocol. Rapid spanning tree will automatically fall back to classic spanning tree data elements and schemes if other bridges are detected that do not support rapid spanning tree.

2.20.20.13 Transmit hold count

Determines the number of BPDUs (Bridge Protocol Data Units) that may be sent when using rapid spanning tree, before a second break is inserted. (With classic spanning tree, this value has no effect.)

Telnet path: /Setup/LAN-Bridge/Spanning-Tree

Possible values:

- Maximum 999

Default: 6

2.20.20.11 Port

This table can be used to set further spanning-tree parameters for each port.

Telnet path: /Setup/LAN- Bridge/Spanning-Tree

2.20.20.11.2 Port

The name of the LAN interface.

Telnet path: /Setup/LAN- Bridge/Spanning-Tree/Port- Data

2.20.20.11.4 Priority

The priority of the port set as an 8-bit value. If more than one port is available as a path to a LAN and the distance to both ports is the same, then this value decides which port is to be selected. If two ports have the same priority, then the port with the smaller number is selected.

Telnet path: /Setup/LAN- Bridge/Spanning-Tree/Port- Data

Possible values:

- Maximum 255

Default: 128



Rapid spanning tree uses only the upper 4 bits of this value, for example, if a value is increased and decreased in 16 steps. Lower values take a higher priority.

2.20.20.11.6 Edge port

A port can be labeled as an edge port

Telnet path: /Setup/LAN- Bridge/Spanning-Tree/Port- Data

Possible values:

- On
- No

Default: No label

2.20.20.11.7 Path cost override

Specifies the influence of path cost.

Telnet path: /Setup/LAN- Bridge/Spanning-Tree/Port- Data

Possible values:

- Maximum 4,294,967,295

Default: 0

2.20.30 IGMP snooping

Telnet path: /Setup/LAN- Bridge/IGMP- Snooping

WEBconfig English: LCOS Menu Tree/Setup/LAN bridge/IGMP snooping

2.20.30.6 Query response interval

Interval in seconds influencing the timing between IGMP queries and router-port aging and/or memberships.

Interval in seconds in which a multicast-capable router (or a simulated querier) expects to receive responses to its IGMP queries. These regular queries influence the time in which memberships age, expire, and are then deleted.

Telnet path: /Setup/LAN-Bridge/IGMP-Snooping

WEBconfig English: LCOS Menu Tree/Setup/LAN bridge/IGMP snooping

Possible values:

- 10-figure number greater than 0

Default: 10



The query response interval must be less than the query interval.

2.20.30.5 Query interval

Interval in seconds in which a multicast-capable router (or a simulated querier) sends IGMP queries to the multicast address 224.0.0.1, so prompting the stations to transmit return messages about multicast group memberships. These regular queries influence the time in which memberships age, expire, and are then deleted.

After the startup phase, the querier sends IGMP queries in this interval.

A querier returns to the querier status after a time equal to " $\text{Robustness} \times \text{Query-Interval} + (\text{Query-Response-Interval} / 2)$ ".

A port loses its router-port status after a time equal to " $\text{Robustness} \times \text{Query-Interval} + (\text{Query-Response-Interval} / 2)$ ".

Telnet path: /Setup/LAN-Bridge/IGMP-Snooping

WEBconfig English: LCOS Menu Tree/Setup/LAN bridge/IGMP snooping

Possible values:

- 10-figure number greater than 0

Default: 125



The query interval must be greater than the query response interval.

2.20.30.1 Operating

Activates or deactivates IGMP snooping in the device and all of the defined querier instances. Without IGMP snooping the bridge functions like a simple switch and forwards all multicasts to all ports.

Telnet path: /Setup/LAN-Bridge/IGMP-Snooping

WEBconfig English: LCOS Menu Tree/Setup/LAN bridge/IGMP snooping

Possible values:

- Yes
- No

Default: No



If this function is deactivated, all IP multicast packets are sent on all ports. If the device operating state changes, the IGMP snooping function is completely reset, i.e. all dynamically learned values are lost (membership, router-port states).

2.20.30.7 Robustness

This value defined the robustness of the IGMP protocol. This option tolerates packet losses of IGMP queries with respect to Join messages.

Telnet path: /Setup/LAN-Bridge/IGMP-Snooping

WEBconfig English: LCOS Menu Tree/Setup/LAN bridge/IGMP snooping

Possible values:

- 10-figure number greater than 0

Default: 2

2.20.30.3 Unregistered data packet handling

This setting defines the handling of multicast data packets with a destination address outside the 224.0.0.x range and for which neither static memberships were defined nor were dynamic memberships learned.

Telnet path: /Setup/LAN-Bridge/IGMP-Snooping

WEBconfig English: LCOS Menu Tree/Setup/LAN bridge/IGMP snooping

Possible values:

- Router ports only: Sends these packets to all router ports.
- Flood: Sends these packets to all ports.
- Discard: Drops these packets.

Default: Router ports only

2.20.30.9 Advertise interval

The interval in seconds in which devices send packets advertising themselves as multicast routers. This information makes it quicker for other IGMP-snooping devices to find which of their ports are to operate as router ports. When activating its ports, a switch (for example) can query for multicast routers, and the router can respond to this query with an advertisement of this type. Under some circumstances this method can be much quicker than the alternative IGMP queries.

Telnet path: /Setup/LAN-Bridge/IGMP-Snooping

WEBconfig English: LCOS Menu Tree/Setup/LAN bridge/IGMP snooping

Possible values:

- 4 to 180 seconds

Default: 20

2.20.30.2 Port settings

This table defines the port-related settings for IGMP snooping.

Telnet path: /Setup/LAN-Bridge/IGMP-Snooping

2.20.30.2.1 Port

The port for which the settings apply.

Telnet path: /Setup/LAN-Bridge/IGMP-Snooping/Port-Settings/Port

Possible values:

- Selects a port from the list of those available in the device.

2.20.30.2.2 Router port

This option defines the port's behavior.

Telnet path: /Setup/LAN-Bridge/IGMP-Snooping/Port-Settings/Router-Port

Possible values:

- Yes: This port will always work as a router port, irrespective of IGMP queries or router messages received at this port.
- No: This port will never work as a router port, irrespective of IGMP queries or router messages received at this port.
- Auto: This port will work as a router port if IGMP queries or router messages are received. The port loses this status if no packets are received for the duration of "Robustness*Query-Interval+(Query-Response-Interval/2)".

Default: Auto

2.20.30.4 Simulated queriers

This table contains all of the simulated queriers defined in the device. These units are employed if IGMP functions are required but there is no multicast router in the network. The querier can be limited to certain bridge groups or VLANs by defining multiple independent queriers to support the corresponding VLAN IDs.

Telnet path: /Setup/LAN- Bridge/IGMP-Snooping

WEBconfig English: LCOS Menu Tree/Setup/LAN bridge/IGMP snooping

Name

Name of the querier instance

Possible values:

- 8 alphanumerical characters.

Default: Blank

Operating

Activates or deactivates the querier instance

Possible values:

- Yes
- No

Default: No

Bridge group

Limits the querier instance to a certain bridge group.

Possible values:

- Select from the list of available bridge groups.

Default: None

Special values: If bridge group is set to "none", the IGMP queries will be sent via all bridge groups.

VLAN ID

Limits the querier instance to a certain VLAN.

Possible values:

- 0 to 4096.

Default: 0

Special values: If "0" is selected as VLAN, the IGMP queries are sent without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

2.20.30.4.1 Name

Name of the querier instance

Telnet path: /Setup/LAN- Bridge/IGMP-Snooping/Simulated-Queriers/Name

Possible values:

- 8 alphanumerical characters.

Default: Blank

2.20.30.4.2 Operating

Activates or deactivates the querier instance

Telnet path: /Setup/LAN- Bridge/IGMP-Snooping/Simulated-Queriers/Operating

Possible values:

- Yes
- No

Default: No

2.20.30.4.3 Bridge group

Limits the querier instance to a certain bridge group.

Telnet path: /Setup/LAN- Bridge/IGMP-Snooping/Simulated-Queriers/Bridge-Group

Possible values:

- Select from the list of available bridge groups.
- None

Special values: If bridge group is set to "none", the IGMP queries will be sent via all bridge groups.

Default: None

2.20.30.4.4 VLAN-ID

Limits the querier instance to a certain VLAN.

Telnet path: /Setup/LAN-Bridge/IGMP-Snooping/Simulated-Queriers/VLAN-ID

Possible values:

- 0 to 4096

Special values: If "0" is selected as VLAN, the IGMP queries are sent without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

Default: 0

2.20.30.8 Static members

This table enables members to be defined manually, for example if they cannot or should not be learned automatically.

Telnet path: /Setup/LAN-Bridge/IGMP-Snooping

Address

The IP address of the manually defined multicast group.

Possible values:

- Valid IP multicast address

Default: Blank

VLAN ID

The VLAN ID which is to support this static member. Each IP multicast address can have multiple entries with different VLAN IDs.

Possible values:

- 0 to 4096

Default: 0

Special values: If "0" is selected as VLAN, the IGMP queries are sent without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

Allow learning

This option activates the automatic learning of memberships in this multicast group. If automatic learning is deactivated, packets can only be sent via the ports which have been manually defined for the multicast group.

Possible values:

- Yes
- No

Default: Yes

Static members

These ports will always be the destination for packets with the corresponding IP multicast address, irrespective of any Join messages received.

Possible values:

- Comma-separated list of the desired ports, max. 215 alphanumeric characters

Default: Blank

2.20.30.8.1 Address

The IP address of the manually defined multicast group.

Telnet path: /Setup/LAN-Bridge/IGMP-Snooping/Static-Members/Address

Possible values:

- Valid IP multicast address

Default: Blank

2.20.30.8.2 Static members

These ports will always be the destination for packets with the corresponding IP multicast address, irrespective of any Join messages received.

Telnet path: /Setup/LAN-Bridge/IGMP-Snooping/Static-Members/Static-Members

Possible values:

- Comma-separated list of the desired ports, max. 215 alphanumerical characters

Default: Blank

2.20.30.8.3 VLAN-ID

The VLAN ID which is to support this static member. Each IP multicast address can have multiple entries with different VLAN IDs.

Telnet path: /Setup/LAN-Bridge/IGMP-Snooping/Static-Members/VLAN-Id

Possible values:

- 0 to 4096

Special values: If "0" is selected as VLAN, the IGMP queries are sent without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

Default: 0

2.20.30.8.4 Allow learning

This option activates the automatic learning of memberships in this multicast group. If automatic learning is deactivated, packets can only be sent via the ports which have been manually defined for the multicast group.

Telnet path: /Setup/LAN-Bridge/IGMP-Snooping/Static-Members/Allow-Learning

Possible values:

- Yes
- No

Default: Yes

2.21 HTTP

This menu contains the HTTP settings.

Telnet path: /Setup

2.21.2 Page headers

Use this setting to choose whether the page headers of the HTTP pages for the Public Spot should be displayed as text or as images.

Telnet path: /Setup/HTTP

Possible values:

- Images
- Texts

Default: Images



The settings for the page headers are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.21.1 Document root

This parameter defines the path to a directory where the help for WEBconfig is stored locally.

Telnet path: /Setup/HTTP/Document-Root

Possible values:

- Maximum 99 alphanumerical characters

Default: Blank



This parameter is for the future, local storage of WEBconfig help. This parameter has no function in current firmware versions.

2.21.6 Error-page style

Normal error display or bluescreen

Telnet path: /Setup/HTTP

Possible values:

- Standard
- Nifty

2.21.15 HTTP compression

The contents of WEBconfig are compressed in order to speed up the display. The compression can be deactivated for browsers that do not support it.

Telnet path: /Setup/HTTP

Possible values:

- Activated
- Deactivated
- Only_for_WAN

Default: Activated

2.21.9 Maximum tunnel connections

The maximum number of simultaneously active HTTP tunnels

Telnet path: /Setup/HTTP

Possible values:

- Max. 255 tunnels

Default: 3

2.21.7 Port

Port for the HTTP server connection

Telnet path: /Setup/HTTP

Possible values:

- Max. 5 characters

Default: 80

2.21.3 Font family

Font family for Web interface display.

Telnet path: /Setup/HTTP

Possible values:

- Max. 39 characters

Default:

- Helvetica
- Sans-serif

2.21.5 Page headers

Select here whether the Public Spot displays the page headers of the standard pages as text or graphics.

Telnet path: /Setup/HTTP/Page-Headers

Possible values:

- Images
- Texts

Default: Images

2.21.11 Session timeout

Period of validity (lease) for the WEBconfig session without user activity, in seconds. When this period expires the password must be reentered.

Telnet path: /Setup/HTTP

Possible values:

- Max. 10 characters

Default: 600

2.21.8 SSL port

Port for the HTTPS server connection

Telnet path: /Setup/HTTP

Possible values:

- Max. 5 characters

Default: 443

2.21.13 Standard design

Selects the design that will be used by default to display WEBconfig.

Telnet path: /Setup/HTTP

Possible values:

- Normal_design
- Design_for_small_resolutions
- Design_for_high_contrast

Default: Normal_design

2.21.10 Tunnel idle timeout

Life-expectancy of an inactive tunnel. After expiry of this time period the tunnel closes automatically unless data transfer is actively taking place.

Telnet path: /Setup/HTTP

Possible values:

- Max. 4294967295 seconds

Default: 300

2.21.14 Show device information

This table defines the system information that is displayed on the System data/ Device status page in WEBconfig.

Telnet path: /Setup/HTTP

2.21.14.1 Device information

Selection of device information to be displayed in WEBconfig.

Telnet path:/Setup/HTTP/Show-device-information

Possible values:

- CPU
- Memory
- Ethernet ports
- Throughput(Ethernet)
- UMTS/modem interface
- Router
- Firewall
- DHCP
- DNS
- VPN
- ADSL
- ISDN
- DSLoL
- Time
- IP addresses

Default: CPU

2.21.14.2 Position

Index for the sequence for the display of device information.

Telnet path:/Setup/HTTP/Show-device-information

Possible values:

- Max. 10 characters

Default: 0

2.21.16 Keep server ports open

This menu contains the parameters for restricting access to the web server services.

Telnet path:/Setup/HTTP/Keep-Server-Ports-Open

2.21.16.1 Interface

Here you select the access path to be set for accessing the web-server services.

Telnet path:/Setup/HTTP/Keep-Server-Ports-Open/Ifc.

Possible values:

- All access methods provided by the device (e.g. LAN, WAN, WLAN, depending on the model).

Default: Blank

2.21.16.2 Keep server ports open

You can decide whether access to the device configuration via HTTP is to be enabled, disabled or limited to read-only. Irrespective of this, access to the web server services can be regulated separately, e.g. to enable communication via CAPWAP, SSL-VPN or SCEP-CA via HTTP(S), even if HTTP(S) has been disabled.

For each access method (LAN, WAN, WLAN, depending on the device), you set the access rights for the device's web server services at the HTTP server port.

Telnet path:/Setup/HTTP/Keep-Server-Ports-Open/Keep-Server-Ports-Open

Possible values:

- Automatic: The HTTP server port is open, as long as a service is registered (e.g. CAPWAP). If no service is registered, the server port will be closed.

- Enabled: The HTTP server port is always open, even if access to the configuration with HTTP is disabled. This can be used to restrict direct access to the configuration. However, the automatic configuration of APs by a WLAN controller is still possible.
- Disabled: The HTTP server port is closed and no service can use the web server. If access to the configuration via HTTP is enabled, then a message is displayed expressing that the web server is not available.

Default: Automatic

2.21.20 Rollout Wizard

This menu contains the settings for the Rollout Wizard.

Telnet path: /Setup/HTTP

2.21.20.6 Renumber actions

As explained above, variables and actions are displayed or processed in the order of their index. Occasionally, variables/actions with neighboring index numbers require a new entry to be entered between them. With this action, the indices can automatically be renumbered with a certain interval between them.

When being executed, the arguments can be defined with the start value and increment. This action renumbers the entries starting with the start value and continuing with the increment as chosen. If the start value and increment are not defined, both are set automatically to 10. If no arguments are entered, the action renumbers the indices with 10, 20, 30, etc.

Telnet path: /Setup/HTTP/Rollout-Wizard

2.21.20.1 Operating

Switches the Rollout Wizard on or off. After being switched on the Wizard appears as an option on the WEB-config start page.

Telnet path: /Setup/HTTP/Rollout-Wizard

Possible values:

- On
- Off

Default: Off

2.21.20.2 Title

The name for the Rollout Wizard as displayed on the start page of WEBconfig.

Telnet path: /Setup/HTTP/Rollout-Wizard

Possible values:

- Max. 50 characters

Default: Rollout

2.21.20.5 Renumber variables

As explained above, variables and actions are displayed or processed in the order of their index. Occasionally, variables/actions with neighboring index numbers require a new entry to be entered between them. With this action, the indices can automatically be renumbered with a certain interval between them.

When being executed, the arguments can be defined with the start value and increment. This action renumbers the entries starting with the start value and continuing with the increment as chosen. If the start value and increment are not defined, both are set automatically to 10. If no arguments are entered, the action renumbers the indices with 10, 20, 30, etc.

Telnet path: /Setup/HTTP/Rollout-Wizard

2.21.20.7 Display connection status

The first screen shows the status of the connection.

Telnet path: /Setup/HTTP/Rollout-Wizard

2.21.20.8 Use extra checks

This option enables consistency tests that check some internal aspects of the wizard.



Executing these additional tests is very time consuming. Activate this option only during development of the wizard and deactivate this option for normal operation.

Telnet path: /Setup/HTTP/Rollout-Wizard

Possible values:

- On
- Off

Default: Off

2.21.20.3 Variables

This table defines the variables for the Rollout Wizard.

Telnet path: /Setup/HTTP/Rollout-Wizard

2.21.20.3.1 Index

Index for the variable. The Rollout Wizard displays the variables in ascending order.

Telnet path: /Setup/HTTP/Rollout-Wizard/Variables

Possible values:

- 1 to 232 - 1

Default: 0

2.21.20.3.2 Identity

Unique identifier of variables that are referenced during the execution of actions. Identifiers are not required for fields that are not used by users to enter their data (e.g. label).

Telnet path: /Setup/HTTP/Rollout-Wizard/Variables

Possible values:

- Max. 64 characters

Default: Blank

2.21.20.3.3 Title

Name of the variable as displayed by the WEBconfig Rollout Wizard in .

Telnet path: /Setup/HTTP/Rollout-Wizard/Variables

Possible values:

- Max. 64 characters

Default: Blank

2.21.20.3.4 Type

Type of variable.

Telnet path: /Setup/HTTP/Rollout-Wizard/Variables

Possible values:

- Label: Text that is displayed to provide explanations of the other variables. Min.-Value and Max.-Value are of no further significance for these entries.

- Integer: Allows the entry of a positive integer number between 0 and 232 - 1. By entering the Min.-Value and Max.-Value, the range of entries can be limited. Also, a default value can be defined. This default value must be between the min. and max. values.
- String: Enables text to be entered. By entering the Min.-Value and Max.-Value, the length of the string can be limited. Also, a default value can be defined. This default text must be shorter than the maximum length, otherwise it will be truncated.
- Password: splayed while being entered. Entering a password has to be repeated. The Rollout Wizard will execute no actions if the passwords do not agree.
- Checkmark: Simple option that can be switched on or off. Min.-Value and Max.-Value are of no further significance for these entries. Checkmarks are activated as standard if the default value is not empty.

Default: 0

2.21.20.3.5 Minimum value

Minimum value for the current variable (if type = integer) or minimum number of characters (where type = String or Password).

Telnet path: /Setup/HTTP/Rollout-Wizard/Variables

Possible values:

- 0 to 232 - 1

Default: 0

2.21.20.3.6 Maximum value

Maximum value for the current variable (if type = integer) or maximum number of characters (where type = String or Password).

Telnet path: /Setup/HTTP/Rollout-Wizard/Variables

Possible values:

- 0 to 232 - 1

Default: 0

2.21.20.3.7 Default value

Default value of the current variable.

Telnet path: /Setup/HTTP/Rollout-Wizard/Variables

Possible values:

- Max. 64 characters

Default: Blank

2.21.20.4 Actions

This table defines the actions for the Rollout Wizard.

Telnet path: /Setup/HTTP/Rollout-Wizard

2.21.20.4.1 Index

Index for the action. The Rollout Wizard executes the actions in ascending order.

Telnet path: /Setup/HTTP/Rollout-Wizard/Actions

Possible values:

- 1 to 232 - 1

Default: 0

2.21.20.4.2 Action

Action to be executed by the Rollout Wizard after the user data have been entered.

Telnet path: /Setup/HTTP/Rollout-Wizard/Actions

Possible values:

- Similar to Cron commands, actions are entered in the syntax [Protocol:] Argument. If no protocol is entered, 'exec.' is applied.

Default: Blank

Special values: exec: Executes any command just as it is used in Telnet to configure a LANCOM. The following example sets the name of the device to 'MyLANCOM':

exec: set /setup/name MyLANCOM

mailto: Enables an e-mail to be sent upon entry of the address, subject and body text, for example:

mailto:admin@mylancom.de?subject=Rollout?body=LANCOM setup completed

http and https: Enables a web site to be accessed, for example to carry out an action there.

<http|https:>//[user[:pass]@]hostname[:port]/...

Variables in the actions: When actions are executed, the values as defined with the Rollout Wizard can be referenced. To this end, the variable's identifier is used for the action with a leading percent character. The identifier must be enclosed by curly brackets if other characters are included in the action. The following example sets the name of the device to the format 'Site (branch)', if the location of the device is being queried as a variable with the identifier 'Location':

exec: set /setup/name %{Location}(Filiale)

For variables of the type Integer or String, the value as entered by the user is used. In the case of variables of the type Checkmark, '1' (switched on) or '0' (switched off) is used.



If the expression for the action contains spaces then the expression must be enclosed by quotation marks.



To make use of the mail function, an SMTP account must be set up in the device.

2.21.20.4.3 Description

Comment on the action.

Telnet path: /Setup/HTTP/Rollout-Wizard/Actions

Possible values:

■ Max. 251 characters

Default: Blank

2.21.30 File server

This menu contains the file-server settings for external USB data media.

Telnet path: /Setup/HTTP/File-Server

2.21.30.2 Operating

This parameter activates or deactivates the file server for USB media.

Telnet path: /Setup/HTTP/File-Server/Operating

Possible values:

■ Yes

■ No

Default: Yes

2.21.30.1 Public subdirectory

This directory is the root directory on a USB medium. The device ignores all other files on the USB medium.

Telnet path: /Setup/HTTP/File-Server/Public-Subdir

Possible values:

■ Maximum 64 alphanumerical characters

Default: public_html

2.22 SYSLOG

This menu contains the SYSLOG settings.

Telnet path: /Setup

2.22.1 Operating

Activates the dispatch of information about system events to the configured SYSLOG client.

Telnet path: /Setup/SYSLOG

Possible values:

- Yes
- No

Default: Yes

2.22.5 Messages table order

This item determines the order in which the messages table is displayed.

Telnet path: /Setup/SYSLOG

Possible values:

- Oldest on top
- Newest on top

Default: Oldest-on-top

2.22.4 Port

Port used for sending SYSLOG messages.

Telnet path: /Setup/SYSLOG

Possible values:

- Max. 10 characters

Default: 514

2.22.2 SYSLOG table

This table defines the SYSLOG clients.

Telnet path: /Setup/SYSLOG

2.22.2.1 Index

Position of the entry in the table.

Telnet path: /Setup/SYSLOG/Server

Possible values:

- Max. 4 characters

Default: Blank

2.22.2.2 IP address

IP address of the SYSLOG client.

Telnet path: /Setup/SYSLOG/Server

Possible values:

- Valid IP address.

Default: 00.0.0

2.22.2.3 Source

Source that caused the message to be sent. Each source is represented by a certain code.

Telnet path: /Setup/SYSLOG/Server

Possible values:

- System time: 01
- Console logins: 02
- System time: 04
- Logins: 08
- Connections: 10
- Accounting: 20
- Administration: 40
- Router: 80

Default: 00

Special values: 00: No source is defined.

2.22.2.4 Level

SYSLOG level with which the message is sent. Each level is represented by a certain code.

Telnet path: /Setup/SYSLOG/Server

Possible values:

- Alert: 01
- Failure: 02
- Warning: 04
- Information: 08
- Debug: 10

Default: 00

Special values: 00: No level is defined.

2.22.2.6 Loopback address

Sender address entered into the SYSLOG message. No answer is expected to a SYSLOG message.

Telnet path: /Setup/SYSLOG/Server

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LB0 to LBF for the 16 loopback addresses
- Any valid IP address

Default: Blank

2.22.3 Facility mapper

This table defines the allocation of SYSLOG sources to facilities.

Telnet path: /Setup/SYSLOG

2.22.3.1 Source

Mapping sources to specific facilities.

Telnet path: Setup/SYSLOG/Facility-Mapper

Possible values:

- System
- Logins
- System time
- Console logins
- connections
- Accounting
- Administration
- Router

2.22.3.2 Facility

Mapping sources to specific facilities.

Telnet path: Setup/SYSLOG/Facility-Mapper

Possible values:

- KERNEL
- AUTH
- CRON
- AUTHPRIV
- LOCAL0
- LOCAL1
- LOCAL2
- LOCAL3

2.23 Interfaces

This menu contains the settings for the interfaces.

Telnet path: /Setup

2.23.19 PCM-SYNC-SOURCE

This ISDN S0 bus is used to synchronize the other buses. If 'Auto' is selected, the first S0 bus running in TE mode is used for synchronization. If you select the wrong S0 bus, you may experience transmission problems (clicking noises).

Telnet path: /Setup/Interfaces/PCM-SYNC-SOURCE

Possible values:

- Auto
- S0-1
- S0-2

Default: Auto



The parameters available to you depend on the equipment of your device.

2.23.18 Permanent L1 activation

Use this option to permanently activate the ISDN bus.

If this option is disabled, the device switches off the ISDN bus if remains unused for 30 seconds. This process helps to save electricity at the switchboard (e.g. an upstream PBX).

Activate this option if the upstream PBX does not respond correctly to the automatic deactivation/activation of the connected device.

Telnet path: /Setup/Interfaces/Permanent-L1-Activation

Possible values:

- Deactivated

- Sync-source-only
- All-TE-interfaces

Default: Deactivated

2.23.1 S0

This item allows you to make further settings for the device interface.

Telnet path: /Setup/Interfaces

2.23.1.1 Interface

Specifies the ISDN interface that the settings refer to.

Telnet path: /Setup/Interfaces/S0/lfc

Possible values:

- Choose from the ISDN interfaces available in the device, e.g. S0-1 or S0-2.

2.23.1.13 Max in calls

This setting allows you to place a limit on the number of concurrent calls that can be made over this interface. One advantage of this is that you can always leave a line free for other devices.

Telnet path: /Setup/Interfaces/S0/Max-in-calls

Possible values:

- None
- One
- Two

Default: Two

2.23.1.13 Max out calls

This setting allows you to place a limit on the number of concurrent calls that can be made over this interface. One advantage of this is that you can always leave a line free for other devices.

Telnet path: /Setup/Interfaces/S0/Max-out-calls

Possible values:

- None
- One
- Two

Default: Two

2.23.1.2 Protocol

This item allows you to select the D-channel protocol for this interface.

Telnet path: /Setup/Interfaces/S0/Protocol

Possible values:

- No
- DSS1
- 1TR6
- P2P-DSS1
- GRPO
- Auto

Default: Auto

2.23.1.7 LL-B channel

This item allows you to set the leased-line channel if the device is operated with a **Group 0**-type leased-line connection.

Telnet path: /Setup/Interfaces/S0/LL-B-chan.

Possible values:

- None
- B1
- B2

Default: None

2.23.1.9 Dial prefix

The number entered here will be placed in front of all telephone numbers making outgoing calls.

This is useful, for example, if your device is operated in a PBX that requires an outside-line access code. This number should be entered here.

Telnet path: /Setup/Interfaces/S0/Dial-prefix

Possible values:

- Max. 8 characters

Default: Blank

2.23.4 DSL

The settings for the DSL interface are located here.

Telnet path: /Setup/Interfaces

2.23.4.1 Interface

Specifies the interface that the settings refer to.

Telnet path: /Setup/Interfaces/S0/Ifc

Possible values:

- Choose from the ISDN interfaces available in the device, e.g. S0-1 or S0-2.
- ADSL
- VDSL
- Choose from the DSL interfaces available in the device, e.g. DSL-1 or DSL-2.
- UMTS



The selection options depend on the equipment of the device.

2.23.4.16 Upstream rate

This item allows you to set the gross upstream rate for this port. The data rate entered here (kbps) limits the outgoing data streams from the device.

Telnet path: /Setup/Interfaces/DSL/Upstream-Rate

Possible values:

- Max. 6 numerical characters

Default: Blank

Special values: 0: No limitation on the amount of data transferred

2.23.4.17 External overhead

The external overhead results from the data that the modem attaches to each packet. For PPPoE connections, this is 4 bytes for the LLC header and 8 bytes for the AAL 5 trailer. The modem is unable to send "broken" ATM cells, so on average half an ATM cell (= 24 bytes) must also be allowed for. The resulting total overhead is thus 36 bytes per transmitted packet.

Telnet path: /Setup/Interfaces/DSL/Ext.-Overhead

Possible values:

- Max. 3 numerical characters

Default: Blank

2.23.4.18 Downstream rate

The downstream rate is measured in kilobits and includes everything arriving at the router over the WAN Ethernet. For example, on a T-DSL connection with guaranteed 768 kbit downstream, the upstream rate negotiated by the modem is 864 kbit. This still includes an overhead typical for this type of connection, which results from the modem using ATM as the transport protocol. If we adjust the 864 kbit to allow for the overhead that results from the structure of an ATM cell (48 bytes of payload for a cell length of 53 bytes), we arrive at $864 * 48/53 = 792$ kbit gross downstream rate, which is transferred from the modem to the router over Ethernet. If data rates negotiated by the modem are unknown, it is possible to multiply the guaranteed data rates by 56/55 to approach the gross data rates.

Telnet path: /Setup/Interfaces/DSL/Downstream-Rate

Possible values:

- Max. 6 numerical characters

Default: Blank

Special values: 0: No restriction on the received data traffic

2.23.4.2 Operating

Here you can specify whether the interface is active or not.

Telnet path: /Setup/Interfaces/DSL/Operating

Possible values:

- No
- Yes

Default: No

2.23.4.23 LAN-Ifc

Select the LAN interface that the DSLoL interface is linked with.

Telnet path: /Setup/Interfaces/DSL-Interfaces/LAN-Ifc

Possible values:

- 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
- Any

Default: LAN-1

2.23.4.6 Mode

This item selects the mode in which the WAN interface is operated. In automatic mode, all PPPoE frames and all data packets belonging to a connection established over the DSLoL interface (as configured in the IP parameter list) are routed via the DSLoL interface (WAN). All other data packets are treated as normal LAN packets. In exclusive mode, the LAN interface operates as a WAN interface only.

Telnet path:/Setup/Interfaces/DSLoL-Interfaces/Mode

Possible values:

- Auto
- Exclusive

Default: Auto

2.23.6 ADSL interface

The settings for the ADSL interface are located here.

Telnet path:/Setup/Interfaces/ADSL-Interface

2.23.6.1 Interface

Select the relevant interface here.

Telnet path:/Setup/Interfaces/ADSL-Interface/Ifc

Possible values:

- ADSL
- S0-1
- DSL-1
- DSL-2
- DSL-3
- UMTS



The selection options depend on the equipment of the device.

2.23.6.2 Protocol

Select the protocol that you want to use for this interface.

With ADSL multimode, the protocols G.DMT, T1.413 and G. Lite are all tried in sequence. Auto mode first attempts to connect using the ADSL2+ protocol. If no connection can be made, the system falls back successively to ADSL2 or G.DMT.

Telnet path:/Setup/Interfaces/ADSL-Interface/Protocol

Possible values:

- No
- Auto
- ADSL2+
- ADSL2
- ADSL Multimode
- Annex-M-Auto
- G.Dmt
- T1.413

Default: No

2.23.6.25 Power management

Activating the power management reduces the power consumption of the integrated ADSL modem.

The L2 mode acts only at the exchange.

The L3-mode enables a reduction of power consumption in the exchange and the ADSL device. To do this, the device enters a sleep mode when the connection is inactive for a defined period of time. Once the connection is activated again, the ADSL device needs a few seconds to initialize and return to operating mode.

Telnet path:/Setup/Interfaces/ADSL-Interface/Power-Management

Possible values:

- Disabled
- L2-allowed
- L3-and-L2-allowed

Default: L2-allowed

2.23.6.26 Linecode

This item sets the mode of operation of the line code. If you select 'Auto', then the system automatically switches to the next entry in the ADSL protocol list within a linecode or, if the end of this list is reached, it switches to the next line code:

- If no signal is detected on the line
- After 3 minutes without sync on ADSL2+
- After 1.5 minutes without sync on ADSL
- Upon the first sync loss after switching to a new line code

The system only switches to line codes that are supported by the currently selected protocol. If a protocol is selected that the current line code does not support, then the system switches to the next appropriate line code.

Line quality is not assessed continuously. The only check in auto mode (protocol and/or line code) is on the number of line faults in the monitoring period. By default, one line fault is allowed per 24 hours. If the maximum number is exceeded, the system switches to the next protocol or line code.

If the number of permissible line faults is not reached during the monitoring time, then the line code currently being used is "fixed" and entered here accordingly. At the same time, the automatic mode for the line code is deactivated. The monitoring period begins one minute after booting or following a change of line code or protocol.

Telnet path:/Setup/Interfaces/ADSL-Interface/Linecode

Possible values:

- Auto
- Annex-A
- Annex-B
- ADSL-A
- ADSL2+A

- ADSL-B
 - ADSL2+B
- Default:** Auto

2.23.7 Modem mobile

The settings for the mobile-telephony modem are located here.

Telnet path: /Setup/Interfaces

2.23.7.1 Interface

Here you select the interface which you want to configure.

Telnet path: /Setup/Interfaces/Mobile/Ifc

Possible values:

- DSL-1
- EXT
- ADSL
- S0-1
- DSL-1
- DSL-2
- DSL-3
- UMTS



The selection options depend on the equipment of the device.

2.23.7.2 Operating

Select the operating mode for the interface.

Telnet path: LCOS Menu Tree/Setup/Interfaces/Mobile/Operating

Possible values:

- No
- Modem
- UMTS-GPRS

Default: No

2.23.7.21 Data rate

Select the data rate in kilobytes per second used to transfer the data streams.

Telnet path: /Setup/Interfaces/Mobile/Datarate

Possible Telnet values:

- 19200
- 38400
- 57600
- 115200

Default: 115200

2.23.7.22 Profile

Here you select the profile to be used for the UMTS interface.

Telnet path: /Setup/Interfaces/Mobile/Profile

Possible values:

- Maximum 16 alphanumeric characters

Default: Blank

2.23.8 VDSL

This table contains an entry for each VDSL interface available in the device with the choice of protocol.

Telnet path: Setup/Interfaces/

2.23.8.1 Interface

Select a VDSL interface for configuration.

Telnet path: /Setup/Interfaces/VDSL

Possible values:

- Select from the VDSL interfaces available in the device.

2.23.8.2 Protocol

This item allows you to select the protocol for the VDSL interface.

Telnet path: /Setup/Interfaces/VDSL

Possible values:

- Auto: VDSL and all ADSL modes
- VDSL: VDSL only
- ADSL: All ADSL modes
- ADSL2+: ADSL2+ (G.992.5) only
- ADSL2: ADSL2 (G.992.3) only
- ADSL1: G.DMT (G.992.1) and also T1.413 with Annex-A

Default: Auto

2.23.20 WLAN

This menu contains the settings for wireless LAN networks

Telnet path: /Setup/Interfaces

2.23.20.1 Network

Here you can adjust further network settings for each logical wireless LAN network (MultiSSID) supported by your device.

Telnet path: /Setup/Interfaces/WLAN

2.23.20.1.1 Interface

Select from the logical WLAN interfaces.

Telnet path: /Setup/Interfaces/WLAN/Network

Possible values:

- Select from the available logical WLAN interfaces.

2.23.20.1.10 Maximum stations

Here you set the maximum number of clients that may associate with this access point in this network. Additional clients wanting to associate will be rejected.

Telnet path: /Setup/Interfaces/WLAN/Network

Possible values:

- 0 to 65535

Default: 0**Special values:** 0 = Limitation switched off**2.23.20.1.11 Client-bridge support**

Whereas address adjustment allows only the MAC address of a directly connected device to be visible to the access point, client-bridge support provides transparency; all MAC addresses of the LAN stations behind the client stations are transferred.

Furthermore, the three MAC addresses usual in client mode are not used for this operating mode (in this example for server, access point and client station), but rather four addresses as with point-to-point connections (the fourth is the MAC address of the station in the LAN of the client station). The fully transparent connection of a LAN to the client station allows targeted transmission of data packets in the WLAN and hence functions such as TFTP downloads, initiated by a broadcast.

Telnet path:/Setup/Interfaces/WLAN/Network**Possible values:**

- Yes: Activates client-bridge support for this logical WLAN.
- No: Deactivates client-bridge support for this logical WLAN.
- Exclusive: Only accepts clients that also support the client-bridge mode.

Default: No

Client-bridge mode can only be used between two LANCOM devices.

2.23.20.1.12 RADIUS accounting

Deactivates accounting via a RADIUS server for this network

Telnet path:/Setup/Interfaces/WLAN/Network**Possible values:**

- On
- Off

Default: Off**2.23.20.1.13 Inter-station traffic**

Depending on the application, it may be required that the WLAN clients connected to an access point can—or expressly cannot—communicate with other clients. Individual settings can be made for every logical WLAN as to whether clients in this SSID can exchange data with one another.

Telnet path:/Setup/Interfaces/WLAN/Network**Possible values:**

- Yes
- No

Default: Yes**2.23.20.1.14 APSD**

Activates APSD power saving for this logical WLAN network.

Telnet path:/Setup/Interfaces/WLAN/Network**Possible values:**

- On
- Off

Default: Off

Please note that in order for the APSD function to work in a logical WLAN, QoS must be activated on the device. APSD uses mechanisms in QoS to optimize power consumption for the application.

2.23.20.1.15 Aironet extensions

Activates Aironet extensions for this logical wireless LAN.

Telnet path:/Setup/Interfaces/WLAN/Network/Aironet-Extensions

Possible values:

- Yes
- No

Default: Yes**2.23.20.1.2 Network name**

Define a unique SSID (the network name) for each of the logical wireless LANs required. Only WLAN clients that have the same SSID can register with this wireless network.

Telnet path: /Setup/Interfaces/WLAN/Network**Possible values:**

- Max. 64 characters

Default: BLANK**2.23.20.1.4 Closed network**

You can operate your wireless LAN either in public or private mode. A wireless LAN in public mode can be contacted by any mobile station in the area. Your wireless LAN is put into private mode by activating the closed network function. In this operation mode, mobile stations that do not know the network name (SSID) are excluded from taking part in the wireless LAN.

Activate the closed network mode if you wish to prevent WLAN clients using the SSID 'ANY' from registering with your network.

Telnet path: /Setup/Interfaces/WLAN/Network**Possible values:**

- On
- Off

Default: Off**2.23.20.1.8 Operating**

Switches the logical WLAN on or off separately.

Telnet path: /Setup/Interfaces/WLAN/Network**Possible values:**

- On
- Off

Default: On**2.23.20.1.9 MAC filter**

The MAC addresses of the clients allowed to associate with an access point are stored in the MAC filter list. The 'MAC filter' switch allows the use of the MAC filter list to be switched off for individual logical networks.

Telnet path: /Setup/Interfaces/WLAN/Network**Possible values:**

- On
- Off

Default: On

Use of the MAC filter list is required for logical networks in which the clients register via LEPS with an individual passphrase. The passphrase used by LEPS is also entered into the MAC filter list. The MAC filter list is always consulted for registrations with an individual passphrase, even if this option is deactivated.

2.23.20.2 Transmission

Here you can adjust further transmission settings for each logical wireless LAN network (MultiSSID) supported by your device.

Telnet path: /Setup/Interfaces/WLAN

2.23.20.2.1 Interface

Opens the settings for the logical WLAN networks.

Telnet path:/Setup/Interfaces/WLAN/Transmission

Possible values:

- Select from the available logical WLAN interfaces.

2.23.20.2.10 Min. fragment length

Packet fragment length below which fragments are rejected

Telnet path:/Setup/Interfaces/WLAN/Transmission

Possible values:

- 0 to 2347

Default: 16

2.23.20.2.11 Soft retries

If the hardware was unable to send a packet, the number of soft retries defines how often the system should attempt retransmission.

The total number of attempts is thus (soft retries + 1) * hard retries.

The advantage of using soft retries at the expense of hard retries is that the rate-adaption algorithm immediately begins the next series of hard retries with a lower data rate.

Telnet path:/Setup/Interfaces/WLAN/Transmission

Possible values:

- 0 to 999

Default: 0

2.23.20.2.12 Hard retries

This value defines the number of times that the hardware should attempt to send packets before a Tx error message is issued. Smaller values mean that a packet which cannot be sent blocks the sender for a shorter time.

Telnet path:/Setup/Interfaces/WLAN/Transmission

Possible values:

- 0 to 15

Default: 10

2.23.20.2.13 Short guard interval

The default setting automatically optimizes the value for guard interval. If the momentary operating conditions allow, the interval will be set to the shortest possible value.

You also have the option of deactivating this mechanism to prevent the short-guard interval from being used.

Put simply, the guard interval reduces the signal distortion caused by intersymbol interference (ISI) when using signal multiplexing (OFDM).

Telnet path:/Setup/Interfaces/WLAN/Transmission/Short-Guard-Interval

Possible values:

- Activated
- Deactivated

Default: Activated

2.23.20.2.14 Max. spatial streams

Spatial streams add a third dimension to the frequency-time matrix available to radio communications: Space. An array of multiple antennas provides the receiver with spatial information that enables the use of spatial multiplexing, a technique that increases transmission rates. This involves the parallel transmission of multiple data streams over a single radio channel. Multiple transmitter and receiver antennas can be operated at the same time. This leads to a significant increase in the performance of the radio system.

The default setting allows settings for the spatial streams to be made automatically to make optimal use of the radio system.

You also have the option of limiting the spatial streams to one or two to reduce the load on the radio system.

Telnet path:/Setup/Interfaces/WLAN/Transmission/Max.-Spatial-Streams

Possible values:

- Automatic
- One
- Two

Default: Automatic

2.23.20.2.15 Send aggregates

The settings for frame aggregation are located here. Frame aggregation is an official standard and, according to the 802.11n standard, it is to be vendor-independent. It is comparable to the long-existing burst mode.

With frame aggregation for WLAN, the frame is enlarged so that multiple Ethernet packets fit into it. This method shortens the waiting time between data packets and increases throughput. The overhead is reduced to release capacity for transmitting data.

However, the increasing length of the frames increases the likelihood that radio interference will make it necessary to retransmit packets. Furthermore, other stations must wait longer for a channel to become available, and they have to collect several data packets for transmission all at once. By default, frame aggregation is activated. This makes sense if you want to increase the throughput for this station and others on this medium are not important. .

Telnet path:/Setup/Interfaces/WLAN/Transmission/Send-Aggregates

Possible values:

- Yes
- No

Default: Yes

2.23.20.2.16 Min. HT MCS

MCS (Modulation Coding Scheme) automatically adapts transmission speeds. In the 802.11n standard it defines a number of variables that specify the number of spatial streams, the modulation and the data rate of each data stream, among others.

In the default setting the station automatically selects the best possible MCS for each stream, based on the conditions of each channel. If interference arises during operation and the channel conditions change, for example due to movement of the transmitter or signal deterioration, the MCS is dynamically adjusted to suit the new conditions.

You also have the option of setting the MCS to a constant value. This may facilitate testing, or it may be useful in particularly dynamic environments to avoid unnecessary parameterizing where an optimal value simply cannot be expected.

Telnet path:/Setup/Interfaces/WLAN/Transmission/Min.-HT-MCS

Possible values:

- Automatic
- 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: Automatic

2.23.20.2.17 Max. HT MCS

MCS (Modulation Coding Scheme) automatically adapts transmission speeds. In the 802.11n standard it defines a number of variables that specify the number of spatial streams, the modulation and the data rate of each data stream, among others.

In the default setting the station automatically selects the best possible MCS for each stream, based on the conditions of each channel. If interference arises during operation and the channel conditions change, for example due to movement of the transmitter or signal deterioration, the MCS is dynamically adjusted to suit the new conditions.

You also have the option of setting the MCS to a constant value. This may facilitate testing, or it may be useful in particularly dynamic environments to avoid unnecessary parameterizing where an optimal value simply cannot be expected.

Telnet path:/Setup/Interfaces/WLAN/Transmission/Max.-HT-MCS

Possible values:

- Automatic
- 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: Automatic

2.23.20.2.18 Min. spatial streams

Spatial streams add a third dimension to the frequency-time matrix available to radio communications: Space. An array of multiple antennas provides the receiver with spatial information that enables the use of spatial multiplexing, a technique that increases transmission rates. This involves the parallel transmission of multiple data streams over a single radio channel. Multiple transmitter and receiver antennas can be operated at the same time. This leads to a significant increase in the performance of the radio system.

The default setting allows settings for the spatial streams to be made automatically to make optimal use of the radio system.

You also have the option of limiting the spatial streams to one or two to reduce the load on the radio system.

Telnet path:/Setup/Interfaces/WLAN/Transmission/Min.-Spatial-Streams

Possible values:

- Automatic
- One
- Two

Default: Automatic

2.23.20.2.19 EAPOL rate

Set the data rate for EAPOL transmission here.

Telnet path:/Setup/Interfaces/WLAN/Transmission

Possible values:

- Like-Data

Select from the available speeds:

- 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: Like-Data

Special values: Like-Data transmits the EAPOL data at the same rate as payload data.

2.23.20.2.2 Packet size

Smaller data packets cause fewer transmission errors than larger packets, although the proportion of header information in the traffic increases, leading to a drop in the effective network load. Increase the factory value only if your wireless network is largely free from interference and very few transmission errors occur. Reduce the value to reduce the occurrence of transmission errors.

Telnet path: /Setup/Interfaces/WLAN/Transmission

Possible values:

- 500 to 1600 (even values only)

Default: 1600

2.23.20.2.20 Max. aggregated packets

This parameter defines the maximum number of packets that may be packed into an aggregate. Aggregation in IEEE 802.11n WLAN transmissions combines multiple data packets to a large package, so reducing the overhead and speeding up the transmission.

Telnet path: /Setup/Interfaces/WLAN/Transmission/Max.-Aggr.-Packet-Number

Possible values:

- Max. 2 numerical characters

Default: 16

2.23.20.2.21 ProbeRsp retries

This is the number of hard retries for probe responses, i.e. messages sent from an access point in answer to a probe request from a client.

Telnet path: /Setup/Interfaces/WLAN/Transmission

Possible values:

- 0 to 15

Default: 3



Values larger than 15 are taken as 15.

2.23.20.2.3 Min-Tx-Rate

Normally the access point negotiates the data transmission speeds continuously and dynamically with the connected WLAN clients. The access point adjusts the transmission speeds to the reception conditions. As an alternative, you can set fixed values for the minimum transmission speed if you wish to prevent the dynamic speed adjustment.

Telnet path: /Setup/Interfaces/WLAN/Transmission

Possible values:

- Automatic
- Select from the available speeds

Default: Automatic

2.23.20.2.4 Basic rate

The defined broadcast rate should allow the slowest clients to connect to the WLAN even under poor reception conditions. A higher value should only be set here if all clients in this logical WLAN can be reached "faster".

Telnet path: /Setup/Interfaces/WLAN/Transmission

Possible values:

- Select from the available speeds

Default: 2 Mbps

2.23.20.2.6 RTS threshold

The RTS threshold uses the RTS/CTS protocol to prevent the occurrence of the "hidden station" phenomenon. A collision between the very short RTS packets is improbable, although the use of RTS/CTS leads to an increase in overhead. The use of this procedure is only worthwhile where long data packets are being used and the risk of collision is higher. The RTS threshold is used to define the minimum packet length for the use of RTS/CTS. The best value can be found using trial and error tests on location.

Telnet path: /Setup/Interfaces/WLAN/Transmission

Possible values:

- 512 to 2347

Default: 2347

2.23.20.2.7 11b preamble

Normally, the clients in 802.11b mode negotiate the length of the preamble with the access point. "Long preamble" should only be set when the clients require this setting to be fixed.

Telnet path: /Setup/Interfaces/WLAN/Transmission

Possible values:

- On
- Off

Default: Off

2.23.20.2.9 Max-Tx-Rate

Normally the access point negotiates the data transmission speeds continuously and dynamically with the connected WLAN clients. The access point adjusts the transmission speeds to the reception conditions. As an alternative, you can set fixed value for the maximum transmission speed if you wish to prevent the dynamic speed adjustment.

Telnet path: /Setup/Interfaces/WLAN/Transmission

Possible values:

- Automatic
- Select from the available speeds

Default: Automatic

2.23.20.3 Encryption

This is where you can make encryption settings for each logical wireless LAN network (MultiSSID).

Telnet path: /Setup/Interfaces/WLAN

2.23.20.3.1 Interface

Opens the WPA/WEK settings for the logical WLAN networks.

Telnet path: /Setup/Interfaces/WLAN/Encryption

Possible values:

- Select from the available logical WLAN interfaces.

2.23.20.3.10 Client EAP method

LANCOM wireless routers and access points in WLAN client operating mode can authenticate themselves to another access point using EAP/802.1X. To activate the EAP/802.1X authentication in client mode, the client EAP method is selected as the encryption method for the first logical WLAN network.

Please note that the selected client EAP method must match the settings of the access point that this LANCOM access point is attempting to register with.

Telnet path:/Setup/Interfaces/WLAN/Encryption

Possible values:

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

Default: TLS



In addition to setting the client EAP method, also be sure to observe the corresponding setting for the WLAN client operation mode.

2.23.20.3.11 WPA rekeying cycle

Defines how often a WPA key handshake will be retried during an existing connection (rekeying)

Telnet path:/Setup/Interfaces/WLAN/Encryption

Possible values:

- 0 to 4294967295 s

Default: 0

Special values: 0 = Rekeying deactivated

2.23.1.1.27 WPA1 session key types

Here you select the methods which are to be made available for generating WPA session keys and group key. There is a choice of the Temporal Key Integrity Protocol (TKIP), the Advanced Encryption Standard (AES), or both.

Telnet path:/Setup/Interfaces/WLAN/Encryption

Possible values:

- TKIP
- AES
- TKIP/AES

Default: TKIP

2.23.20.3.13 WPA2 session key types

Here you select the methods which are to be made available for generating WPA session keys and group key. There is a choice of the Temporal Key Integrity Protocol (TKIP), the Advanced Encryption Standard (AES), or both.

Telnet path:/Setup/Interfaces/WLAN/Encryption

Possible values:

- TKIP
- AES
- TKIP/AES

Default: AES

2.23.20.3.2 Encryption

Activates the encryption for this logical WLAN.

Telnet path:/Setup/Interfaces/WLAN/Encryption

Possible values:

- On
- Off

Default: On**2.23.20.3.3 Default key**

Selects the WEP key to be used for encrypting packets sent by this logical WLAN.

Telnet path:/Setup/Interfaces/WLAN/Encryption**Possible values:**

- Key 1
- Key 2
- Key 3
- Key 4

Default: Key 1

Key 1 only applies for the current logical WLAN, keys 2 to 4 are valid as group keys for all logical WLANs with the same physical interface.

2.23.20.3.4 Method

Selects the encryption method and, for WEP, the key length that is to be used to encrypt data packets on the WLAN.

Telnet path:/Setup/Interfaces/WLAN/Encryption**Possible values:**

- 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)

Please consider that not all wireless cards support all encryption methods.

2.23.20.3.5 Authentication

The encryption method can be selected when using WEP.

Telnet path:/Setup/Interfaces/WLAN/Encryption**Possible values:**

- Open system: For the Open System authentication procedure, all clients are accepted. There is no authentication. The WLAN clients must always transmit correctly encrypted data for this to be forwarded by the base station.
- Shared key: With the shared key authentication procedure, authentication requires that the WLAN client initially responds by returning a correctly encrypted data packet. Only if this succeeds will the encrypted data from the client be accepted and forwarded. However, this method presents an attacker with a data packet in its encrypted and unencrypted form, so providing the basis for an attack on the key itself.

Default: Open system

For reasons of security we recommend that you use the open system authentication procedure.

2.23.20.3.6 Key

You can enter the key or passphrase as an ASCII character string. An option for WEP is to enter a hexadecimal number by adding a leading '0x'.

The following lengths result for the formats used:

Method, Length

WPA-PSK, 8 to 63 ASCII characters

WEP152 (128 bit), 16 ASCII or 32 HEX characters

WEP128 (104 bit), 13 ASCII or 26 HEX characters

WEP64 (40 bit), 5 ASCII or 10 HEX characters

Telnet path:/Setup/Interfaces/WLAN/Encryption

Possible values:

- ASCII character string or hexadecimal number

Default: Blank



0



When using 802.1x in AP mode, the name entered here refers to the RADIUS server.



When using 802.1x in client mode and PEAP or TTLS as the client EAP method, the credentials (user:password) are saved here.

2.23.20.3.9 WPA version

Data in this logical WLAN will be encrypted with this WPA version.

Telnet path:/Setup/Interfaces/WLAN/Encryption

Possible values:

- WPA1
- WPA2
- WPA1/2

Default: WPA1/2

2.23.20.4 Group encryption keys

This is where you can specify for each physical wireless LAN interface those WEP group keys 2 to 4, that are used there by the logical wireless LAN networks in common.

Telnet path: /Setup/Interfaces/WLAN



If 802.1x/EAP is activated, the group encryption keys are used by 802.1x/EAP and are thus no longer available for WEP encryption.

2.23.20.4.1 Interface

Opens the WEP group keys for the physical WLAN interface.

Telnet path:/Setup/Interfaces/WLAN/Group-Encryption-Keys

Possible values:

- Select from the available physical WLAN interfaces.

2.23.20.4.3 Key-2

WEP group encryption key 2

Telnet path:/Setup/Interfaces/WLAN/Group-Encryption-Keys

Possible values:

- You can enter the key as an ASCII character string or as a hexadecimal number (with a leading '0x')
- The following lengths result for the formats used:
- Method, Length
- WEP152 (128 bit), 16 ASCII or 32 HEX characters
- WEP128 (104 bit), 13 ASCII or 26 HEX characters

- WEP64 (40 bit), 5 ASCII or 10 HEX characters

Default: Blank

2.23.20.4.4 Key-3

WEP group encryption key 3

Telnet path:/Setup/Interfaces/WLAN/Group-Encryption-Keys

Possible values:

- You can enter the key as an ASCII character string or as a hexadecimal number (with a leading '0x')
- The following lengths result for the formats used:
- Method, Length
- WEP152 (128 bit), 16 ASCII or 32 HEX characters
- WEP128 (104 bit), 13 ASCII or 26 HEX characters
- WEP64 (40 bit), 5 ASCII or 10 HEX characters

Default: Blank

2.23.20.4.5 Key-4

WEP group encryption key 4

Telnet path:/Setup/Interfaces/WLAN/Group-Encryption-Keys

Possible values:

- You can enter the key as an ASCII character string or as a hexadecimal number (with a leading '0x')
- The following lengths result for the formats used:
- Method, Length
- WEP152 (128 bit), 16 ASCII or 32 HEX characters
- WEP128 (104 bit), 13 ASCII or 26 HEX characters
- WEP64 (40 bit), 5 ASCII or 10 HEX characters

Default: Blank

2.23.20.4.7 Key type 2

Select the key length to be used for the WEP group encryption key 2.

Telnet path:/Setup/Interfaces/WLAN/Group-Encryption-Keys

Possible values:

- WEP-156 (128 bit)
- WEP-128 (104 bit)
- WEP-64 (40 bit)

Default: WEP-64 (40 bit)

2.23.20.4.8 Key type 3

Select the key length to be used for the WEP group encryption key 3.

Telnet path:/Setup/Interfaces/WLAN/Group-Encryption-Keys

Possible values:

- WEP-156 (128 bit)
- WEP-128 (104 bit)
- WEP-64 (40 bit)

Default: WEP-64 (40 bit)

2.23.20.4.9 Key type 4

Select the key length to be used for the WEP group encryption key 4.

Telnet path:/Setup/Interfaces/WLAN/Group-Encryption-Keys

Possible values:

- WEP-156 (128 bit)
- WEP-128 (104 bit)
- WEP-64 (40 bit)

Default: WEP-64 (40 bit)

2.23.20.5 Interpoint settings

Here you can specify important parameters for the communication between and the behavior of base stations.

Telnet path: /Setup/Interfaces/WLAN

2.23.20.5.1 Interface

Opens the settings for the physical WLAN interface.

Telnet path: /Setup/Interfaces/WLAN/Interpoint- Peers

Possible values:

- Select from the available physical WLAN interfaces.

2.23.20.5.10 Channel selection scheme

In the 5-GHz band, the automatic search for vacant WLAN channels can lead to several simultaneous test transmissions from multiple access points, with the result that they do not find each other. This stalemate situation can be avoided with the appropriate "Channel selection scheme".

Thus it is recommended for the 5GHz band that one central access point should be configured as 'Master' and all other point-to-point partners should be configured as 'Slave'. In the 2.4GHz band, too, this setting simplifies the establishment of point-to-point connections if the automatic channel search is activated.

Telnet path: /Setup/Interfaces/WLAN/Interpoint- Peers

Possible values:

- Master: This access point makes the decisions when selecting a free WLAN channel.
- Slave: All other access points will keep searching until they find a transmitting Master.

Default: Master



It is imperative that the channel selection scheme is configured correctly if the point-to-point connections are to be encrypted with 802.11i/WPA.

2.23.20.5.11 Link-loss timeout

Time in seconds after which a (DFS) slave considers the link to the master to be lost if no beacons have been received.

Telnet path: /Setup/Interfaces/WLAN/Interpoint- Peers

Possible values:

- 0 to 4294967295 seconds

Default: 4

2.23.20.5.12 Key handshake role

Specifies whether this party should act as authenticator or supplicant when WPA is being used. In default mode, the authenticator is the master of a link, in auto mode the authenticator is the device with the lower MAC address

Telnet path: /Setup/Interfaces/WLAN/Interpoint- Peers

Possible values:

- Default
- Auto

Default: Default

2.23.20.5.13 Local Name

For this physical WLAN interface, enter a name which is unique in the WLAN: This name can be used by other WLAN devices to connect this base station over point-to-point.

You can leave this field empty if the device has only one WLAN interface and already has a device name which is unique in the WLAN, or if the other base stations identify this interface by means of the WLAN adapter's MAC address.

Telnet path:/Setup/Interfaces/WLAN/Interpoint- Peers

Possible values:

- Max. 64 characters

Default: Blank

2.23.20.5.2 Enable

The behavior of an access point when exchanging data with other access points is defined in the "Point-to-point operation mode".

Telnet path:/Setup/Interfaces/WLAN/Interpoint- Peers

Possible values:

- Off: The access point only communicates with mobile clients
- On: The access point can communicate with other access points and with mobile clients
- Exclusive: The access point only communicates with other base stations

Default: Off

2.23.20.5.9 Isolated mode

Allows or prohibits the transmission of packets between P2P links on the same WLAN interface (compatibility setting for LCOS versions prior to version 2.70)

Telnet path:/Setup/Interfaces/WLAN/Interpoint- Peers

Possible values:

- On
- Off

Default: Off

2.23.20.6 Client modes

If you operate your LANCOM wireless device in client mode, you can make detailed settings on its behavior here.

Telnet path: /Setup/Interfaces/WLAN

2.23.20.6.1 Interface

Opens the settings for the physical WLAN interface.

Telnet path:/Setup/Interfaces/WLAN/Client- Modes

Possible values:

- Select from the available physical WLAN interfaces.

2.23.20.6.10 Rx limit

Bandwidth restriction for registering WLAN clients.

A client communicates its own settings to the base station when logging in. The base station uses these values to set the minimum bandwidth.

Telnet path:/Setup/Interfaces/WLAN/Client- Modes

Possible values:

- 0 to 4294967296 (2^{32})

Default: 0

Special values: 0: No limit



The significance of the Rx and Tx values depends on the device's operating mode. In this case, as an access point, Rx stands for "Send data" and Tx stands for "Receive data".

2.23.20.6.12 Selection preference

Here you select how this interface is to be used.

Telnet path:/Setup/Interfaces/WLAN/Client- Modes/WLAN-1

Possible values:

- Signal strength: Selects the profile for the WLAN offering the strongest signal. This setting causes the WLAN module in client mode to automatically switch to a different WLAN as soon as it offers a stronger signal.
- Profile: Selects the profile for available WLANs in the order that they have been defined (WLAN index, e.g. WLAN-1, WLAN-2, etc.), even if another WLAN offers a stronger signal. In this setting, the WLAN module in client mode automatically switches to a different WLAN as soon as a WLAN with a lower WLAN index is detected (irrespective of signal strengths).

Default: Signal strength

2.23.20.6.3 Connection keepalive

This option ensures that the client station keeps the connection to the access point alive even if the connected devices are not exchanging any data packets. If this option is disabled, the client station is automatically logged off the wireless network if no packets are transferred over the WLAN connection within a specified time.

Telnet path:/Setup/Interfaces/WLAN/Client- Modes

Possible values:

- On
- Off

Default: On

2.23.20.6.4 Network types

'Network types' specifies whether the station can only register with infrastructure networks or with adhoc networks as well.

Telnet path:/Setup/Interfaces/WLAN/Client- Modes

Possible values:

- Infrastructure
- Adhoc

Default: Infrastructure

2.23.20.6.5 Scan bands

This defines whether the client station scans just the 2.4 GHz, just the 5 GHz, or all of the available bands for access points.

Telnet path:/Setup/Interfaces/WLAN/Client- Modes

Possible values:

- 2.4/5 GHz
- 2.4 GHz
- 5 GHz

Default: 2.4/5 GHz

2.23.20.6.6 Preferred BSS

If the client station is to log onto one particular access point only, the MAC address of the WLAN card in this access point can be entered here.

Telnet path:/Setup/Interfaces/WLAN/Client- Modes

Possible values:

- Valid MAC address

Default: Blank

2.23.20.6.7 Address adaptation

In client mode, the client station normally replaces the MAC addresses in data packets from the devices connected to it with its own MAC address. The access point at the other end of the connection only ever “sees” the MAC address of the client station, not the MAC address of the computer(s) connected to it.

In some installations it may be desirable for the MAC address of a computer to be transmitted to the access point and not the MAC address of the client station. The option ‘Address adaptation’ prevents the MAC address from being replaced by the client station. Data packets are transferred with their original MAC addresses.

Telnet path: /Setup/Interfaces/WLAN/Client- Modes

Possible values:

- On
- Off

Default: Off



Address adaptation only works when just one computer is connected to the client station.

2.23.20.6.8 Client-bridge support

Whereas address adaptation allows only the MAC address of a single attached device to be visible to the access point, client-bridge support provides transparency in that all MAC addresses of the LAN stations behind the client stations are transferred to the access point.

Telnet path: /Setup/Interfaces/WLAN/Client- Modes

Possible values:

- On
- Off

Default: Off



0

2.23.20.6.9 Tx limit

Bandwidth restriction for registering WLAN clients.

A client communicates its own settings to the base station when logging in. The base station uses these values to set the minimum bandwidth.

Telnet path: /Setup/Interfaces/WLAN/Client- Modes

Possible values:

- 0 to 4294967296 (2^{32})

Default: 0

Special values: 0: No limit



The significance of the Rx and Tx values depends on the device's operating mode. In this case, as an access point, Rx stands for “Send data” and Tx stands for “Receive data”.

2.23.20.7 Operational settings

In the operational settings you can set basic parameters for operating your WLAN interface.

Telnet path: /Setup/Interfaces/WLAN

2.23.20.7.1 Interface

Opens the settings for the physical WLAN interface.

Telnet path: /Setup/Interfaces/WLAN/Operational

Possible values:

- WLAN-1
- WLAN-2

2.23.20.7.2 Operating

Switches the physical WLAN interface on or off separately.

Telnet path:/Setup/Interfaces/WLAN/Operational

Possible values:

- On
- Off

Default: On

2.23.20.7.3 Operation mode

LANCOM wireless devices can always operate in various modes.

Telnet path:/Setup/Interfaces/WLAN/Operational

Possible values:

- Base station: As a base station (access point), it forms the link between WLAN clients and the cabled LAN.
- Client: In client mode, the device itself locates the connection to another access point and attempts to register with a wireless network. In this case the device serves to link a cabled network device to an access point over a wireless connection.
- Managed: As a managed access point, the device searches for a central WLAN Controller from which it can obtain a configuration.

Default: LANCOM wireless router: Base station; LANCOM access points: Managed

2.23.20.7.4 Link LED function

When setting up point-to-point connections or operating the device as a WLAN client, the best possible positioning of the antennas is facilitated if the signal strength can be recognized at different positions. The WLAN link LED can be used for displaying the signal quality during the set-up phase. In the corresponding operating mode, the WLAN link LED blinks faster with better reception quality according to the antenna position.

Telnet path:/Setup/Interfaces/WLAN/Operational

Possible values:

- Number of connections: In this operation mode, the LED uses "inverse flashing" in order to display the number of WLAN clients that are logged on to this access point as clients. There is a short pause after the number of flashes for each client. Select this operation mode when you are operating the LANCOM wireless router in access point mode.
- Client signal strength: In this operation mode, this LED displays the signal strength of the access point with which the LANCOM wireless router has registered itself as a client. The faster the LED blinks, the better the signal. Select this operation mode only when you are operating the LANCOM wireless router in client mode.
- P2P1 to P2P6 signal strength: In this operation mode, the LED displays the signal strength of respective P2P partner with which the LANCOM wireless router forms a P2P path. The faster the LED blinks, the better the signal.

Default: Number of connections

2.23.20.7.5 Broken link detection

When an access point is not connected to the cabled LAN, it is normally unable to fulfill its primary task, namely the authorization of WLAN clients for access to the LAN. The broken-link detection function allows a device's WLAN to be disabled if the connection to the LAN should fail. Clients associated with that access point are then able to login to a different one (even if it has a weaker signal).

Until LCOS version 7.80, broken-link detection always applied to LAN-1, even if the device was equipped with multiple LAN interfaces. Furthermore, deactivation affected all of the WLAN modules in the device. With LCOS version 8.00, broken-link detection could be bound to a specific LAN interface.

This function allows the WLAN modules in a device to be disabled if the allocated LAN interface has no connection to the LAN.

Telnet path:/Setup/Interfaces/WLAN/Operational/Broken-Link-Detection

Possible values:

- No: Broken-link detection is disabled.

- LAN-1 to LAN-n (depending on the LAN interfaces available in the device). All of the WLAN modules in the device will be deactivated if the LAN interface set here should lose its connection to the cabled LAN.

Default:

- No



The interface descriptors LAN-1 to LAN-n stand for the logical LAN interfaces. To make use of this function, the physical Ethernet ports on the device must be set with the corresponding values LAN-1 to LAN-n.



Broken-link detection can also be used for WLAN devices operating in WLAN client mode. With broken-link detection activated, the WLAN modules of a WLAN client are only activated when a connection exists between the relevant LAN interfaces and the cabled LAN.

2.23.20.8 Radio settings

Here you can adjust settings that regulate the physical transmission and reception over your WLAN interface.

Telnet path: /Setup/Interfaces/WLAN

2.23.20.8.1 Interface

Opens the settings for the physical WLAN interface.

Telnet path: /Setup/Interfaces/WLAN/Radio-Settings

Possible values:

- Select from the available physical WLAN interfaces.

2.23.20.8.10 AP density

The more access points there are in a given area, the more the reception areas of the antennae intersect. The setting 'Access point density' can be used to reduce the reception sensitivity of the antenna.

Telnet path: /Setup/Interfaces/WLAN/Radio-Settings

Possible values:

- Low
- Medium
- High
- Minicell
- Microcell

Default: Low

2.23.20.8.12 Antenna gain

This item allows you to specify the antenna gain factor (in dBi) minus attenuation of the cable and (if applicable) lightning protection. Based on this, and depending on the country where the system is operated and the frequency band, the base station calculates the maximum permitted transmission power.

Transmission power can be reduced to a minimum of 0.5 dBm in the 2.4-GHz band and 6.5 dBm in the 5-GHz band. This limits the maximum value that can be added to 17.5 dBi in the 2.4-GHz band and 11.5 dBi in the 5-GHz band. Please ensure that your combination of antenna, cable and lightning-protection complies with the legal requirements of the country where the system is operated.

The receiver's sensitivity is unaffected by this.

Example: AirLancer O-18a: Antenna gain: 18dBi, cable attenuation: 4dB --> Value to be entered = 18dBi - 4dB = 14dBi.

Telnet path: /Setup/Interfaces/WLAN/Radio-Settings

Possible values: Max. 4 characters

Default: 3



The minimum of 6.5 dBm only applies to legacy abg radio modules with G-mode wireless LAN.



The current transmission power is displayed by the device's web interface or by telnet under 'Status->WLAN statistics->WLAN parameters->Transmission power' or with LANconfig under 'System information->WLAN card->Transmission power'.

2.23.20.8.13 Channel list

This field specifies the subset of channels to be used for automatic channel selection or in client mode.

Telnet path: /Setup/Interfaces/WLAN/Radio-Settings

Possible values:

■ Comma-separated list of individual numbers or ranges.

Default: Blank

2.23.20.8.14 Background scan

In order to identify other access points within the device's local radio range, the LANCOM Wireless router can record the beacons received (management frames) and store them in the scan table. Since this recording occurs in the background in addition to the access points' "normal" radio activity, it is called a "background scan".

If a value is entered here, the LANCOM wireless router searches the active band for currently unused frequencies to find available access points. This value is the time interval between search cycles.

LANCOM wireless routers in access point mode normally use the background scan function for rogue AP detection. This scan interval should correspond to the time span within which rogue access points should be recognized, e.g. 1 hour.

Conversely, LANCOM wireless routers in client mode generally use the background scan function to improve mobile WLAN client roaming. In order to achieve fast roaming, the scan time is limited here, for example, to 260 seconds.

Telnet path: /Setup/Interfaces/WLAN/Radio-Settings

Possible values:

■ 0 to 4294967295

Default: 0

Special values: 0: When the background scan time is '0' the background scanning function is deactivated.

2.23.20.8.15 DFS rescan hours

In some countries, the use of the DFS method for automatic channel selection is a legal requirement.

With the DFS method (Dynamic Frequency Selection) an unused frequency is automatically selected, for example, to avoid interference from radar systems or to distribute WLAN devices as evenly as possible over the entire frequency band. After switching on or booting, the device randomly selects one of the available channels (e.g. based on the country settings). It checks whether radar signals exist on this channel, and whether it is already in use by another WLAN. This scan procedure repeats until a channel is found that is free of radar signals and which has the lowest possible number of other networks. The selected channel is then monitored for radar signals for a further 60 seconds. For this reason, data traffic may be interrupted for a period of 60 seconds while the frequencies are scanned for a free channel.

To avoid having the 60 second pause at an inconvenient time, you can set the time of the scan and thus the database update. To define the time you can use the options provided by cron commands, e.g. '1,6,13' to force a DFS scan at 01:00h, 06:00h or 13:00h, or '0-23/4' for a DFS scan between 0:00h and 23:00h every 4 hours.

Telnet path: /Setup/Interfaces/WLAN/Radio-Settings

Possible values:

■ Comma-separated list of hours

Default: Blank



Forced DFS scans require that the device is set with the correct system time.

2.23.20.8.16 Allow 40MHz

The default setting automatically optimizes the value for bandwidth. If the momentary operating conditions allow, a bandwidth of 40MHz will be enabled, which is otherwise limited to 20MHz.

You also have the option of switching this mechanism off, so limiting the bandwidth to the narrower 20MHz. The 802.11n standard specifies a channel bonding from 20MHz to 40MHz.

Telnet path:/Setup/Interfaces/WLAN/Radio-Settings/Allow-40MHz

2.23.20.8.17 Antenna mask

Antenna grouping can be configured in order to optimize the gain from spacial multiplexing. By default the system automatically selects the optimum grouping setting to match current conditions. You also have the possibility to set an antenna group with a user-defined combination of antennas. The setting has an affect on radiation and reception behavior of the radio system.

Telnet path: /Setup/Interfaces/WLAN/Radio-Settings/Antenna-Mask

Possible values:

- Auto
- Antenna-1
- Antenna-1+2
- Antenna-1+3
- Antenna-1+2+3

Default: Auto

2.23.20.8.18 Background scan unit

Unit for the definition of the background scan interval

Telnet path:/Setup/Interfaces/WLAN/Radio-Settings

Possible values:

- Milliseconds
- Seconds
- Minutes
- Hours
- Days

Default: Seconds

2.23.20.8.19 Channel pairing

This value sets the channel pairs used by 11n devices in 40-MHz mode.

Telnet path:/Setup/Interfaces/WLAN/Radio-Settings/Channel-Pairing

Possible values:

- 11n-compliant: The device uses the channels as specified by 802.11n. Compared to the former proprietary channels used in Turbo Mode, the 40-MHz channels have shifted by 20 MHz.
- Legacy-turbo-friendly: Only useful in outdoor environments to avoid overlapping with other 11a paths in turbo mode.

Default: 11n-compliant

2.23.20.8.2 Tx power reduction

In contrast to antenna gain, the entry in the field 'Tx power reduction' causes a static reduction in the power by the value entered, and ignores the other parameters.

Telnet path:/Setup/Interfaces/WLAN/Radio-Settings

Possible values:

- 0 to 999 dB

Default: 0



The transmission power reduction simply reduces the emitted power. The reception sensitivity (reception antenna gain) remains unaffected. This option is useful, for example, where large distances have to be bridged by radio when using shorter cables. The reception antenna gain can be increased without exceeding the legal limits on transmission power. This leads to an improvement in the maximum possible range and, in particular, the highest possible data transfer rates.

2.23.20.8.20 Preferred DFS scheme

All WLAN systems put into operation after EN 301 893-V1.5 came into effect are required to use DFS3 in the 5-GHz band.

Here you can select between DFS2 (EN 301 893-V1.3) and DFS3 (EN 301 893-V1.5).

Telnet path:/Setup/Interfaces/WLAN/Radio-Settings/Preferred-DFS-scheme

Possible values:

- EN 301 893-V1.5
- EN 301 893-V1.3

Default: EN 301 893-V1.5



When upgrading from a firmware version older than LCOS version 8.00 to an LCOS version 8.00 or higher, the existing setting of DFS2 (EN 301 893-V1.3) remains in effect.



No selection can be made for devices permanently set to DFS3, for those with processors that do not support DFS3 or for those which transmit on the 2.4-GHz frequency only.

2.23.20.8.3 5GHz mode

Using two neighboring, vacant channels for wireless transmissions can increase the transfer speeds in Turbo Mode up to 108 Mbps.

Telnet path:/Setup/Interfaces/WLAN/Radio-Settings

Possible values:

- Normal (54 Mbps mode)
- 108 Mbps (Turbo mode)

Default: Normal (802.11a) or 802.11a/n mixed (with 11n devices)



This setting is only available for devices that support DFS2 or DFS3.

2.23.20.8.4 Maximum distance

Large distances between transmitter and receiver give rise to increasing delays in the runtime for the data packets. If a certain limit is exceeded, the responses to transmitted packets no longer arrive within a given time limit. The entry for maximum distance increases the wait time for the responses. This distance is converted into a delay as required by the data packets for wireless communications.

Telnet path:/Setup/Interfaces/WLAN/Radio-Settings

Possible values:

- 0 to 65535 km

Default: 0

2.23.20.8.5 Diversity

The diversity settings specify which antennas should be used for transmission and for reception:

Telnet path:/Setup/Interfaces/WLAN/Radio-Settings

Possible values:

- RX only: In this default setting, the antenna connected to the access point's main connector is used for data transmission. For reception (RX), the antenna with the best signal is selected (at Main or AUX).
- TX/RX: If the diversity function is used for transmission (TX) as well, the antenna with the strongest signal is taken.
- None: The main antenna only is used for transmission, and for reception the antenna at the AUX connector is preferred. Using this alternative, high-performance antennas that are legally prohibited from transmitting can be used for reception.

Default: RX only

2.23.20.8.6 Radio band

Selecting the frequency band determines whether the wireless LAN adapter operates in the 2.4 GHz or 5 GHz band, which in turn determines the available radio channels.

Telnet path: /Setup/Interfaces/WLAN/Radio-Settings

Possible values:

- 2.4 GHz
- 5 GHz

Default: 2.4 GHz



0

2.23.20.8.7 Subbands

In the 5-GHz band, it is also possible to select a subband, which is linked to certain radio channels and maximum transmission powers.

Telnet path: /Setup/Interfaces/WLAN/Radio-Settings

Possible values:

- Depends on the frequency band selected

Default: Band-1

2.23.20.8.8 Radio channel

The radio channel selects a portion of the conceivable frequency band for data transfer.

Telnet path: /Setup/Interfaces/WLAN/Radio-Settings

Possible values:

- Depend on the selected frequency band and the selected country.

Default: 11



In the 2.4-GHz band, two separate wireless networks must be at least three channels apart to avoid interference.

2.23.20.8.9 2.4-GHz mode

In the 2.4 GHz band, there are two different wireless standards: The IEEE 802.11b standard with a transmission speed of up to 11 Mbps and the IEEE 802.11g standard offering up to 54 Mbps. If 2.4 GHz is selected as the operating frequency, the transmission speed can be selected in addition.

The 802.11g/b compatibility mode offers the highest possible speeds and yet also offers the 802.11b standard so that slower clients are not excluded. In this mode, the WLAN card in the access point principally works with the faster standard and falls back on the slower mode should a client of this type log into the WLAN. In the '2Mbit compatible' mode, the access point supports older 802.11b cards with a maximum transmission speed of 2 Mbps.

Telnet path: /Setup/Interfaces/WLAN/Radio-Settings

Possible values:

- 802.11g/b mixed
- 802.11g/b 2-Mbit compatible
- 802.11b (11 Mbit)
- 802.11g (54 Mbit)
- 802.11g (108 Mbit)

Default: 802.11b/g mixed or 802.11b/g/n mixed (with 11n devices)



Please observe that clients supporting only the slower standards may not be able to register with the WLAN if the speeds set here are higher.

2.23.20.9 Performance

Here you can set the parameters that influence the performance of your WLAN interface.

Telnet path: /Setup/Interfaces/WLAN

2.23.20.9.1 Interface

Opens the settings for the physical WLAN interface.

Telnet path: /Setup/Interfaces/WLAN/Performance

Possible values:

- Select from the available physical WLAN interfaces.

2.23.20.9.2 Tx bursting

Enables/prevents packet bursting for increasing throughput. Bursting leads to less fairness on the medium.

Telnet path: /Setup/Interfaces/WLAN/Performance

Possible values:

- On
- Off

Default: Off

2.23.20.9.3 Compression

Allows or prohibits the hardware packet compression.

Telnet path: /Setup/Interfaces/WLAN/Performance

Possible values:

- On
- Off

Default: Off

2.23.20.9.5 QoS

With the extension to the 802.11 standard, 802.11e, Quality of Service can be provided for transfers via WLAN. Among others, 802.11e supports the prioritization of certain data-packet types. This extension is an important basis for the use of voice applications in WLANs (Voice over WLAN, VoWLAN). The WiFi alliance certifies products that support Quality of Service according to 802.11e, and refer to WMM (WiFi Multimedia, formerly known as WME or Wireless Multimedia Extension). WMM defines four categories (voice, video, best effort and background) which make up separate queues to be used for prioritization. The 802.11e standard sets priorities by referring to the VLAN tags or, in the absence of these, by the DiffServ fields of IP packets. Delay times (jitter) are kept below 2 milliseconds, a magnitude which is inaudible to the human ear. 802.11e controls access to the transfer medium with EDCF, the Enhanced Distributed Coordination Function.

Telnet path: /Setup/Interfaces/WLAN/Performance

Possible values:

- On
- Off

Default: Off



Priorities can only be set if the WLAN client and the access point both support 802.11e or WMM, and also if the applications are able to mark the data packets with the corresponding priorities.

2.23.20.10 Beaconing

Roaming settings are only relevant in the base-station operating mode. The wireless LAN access point (WLAN AP) periodically transmits a radio signal (beacon) so that the clients can detect it or the logical wireless networks (SSIDs) that it provides.

Telnet path: /Setup/Interfaces/WLAN

2.23.20.10.1 Interface

Opens the Expert settings for the physical WLAN interface.

Telnet path: /Setup/Interfaces/WLAN/Beaconing

Possible values:

- Select from the available physical WLAN interfaces.

2.23.20.10.2 Beacon period

This value defines the time interval in K μ s between beacon transmission (1 K μ s corresponds to 1024 micro-seconds and is a measurement unit of the 802.11 standard. 1 K μ s is also known as a Timer Unit (TU)). Smaller values result in a shorter beacon timeout period for the client and enable quicker roaming in case of failure of an access point, but they also increase the WLAN overhead.

Telnet path: /Setup/Interfaces/WLAN/Beaconing

Possible values:

- 20 to 65535 TU

Default: 100

2.23.20.10.3 DTIM period

This value defines the number of beacons which are collected before multicasts are broadcast. Higher values enable longer client sleep intervals, but worsen the latency times.

Telnet path: /Setup/Interfaces/WLAN/Beaconing

Possible values:

- 1 to 255

Default: 1

2.23.20.10.4 Beacon order

Beacon order refers to the order in which beacons are sent to the various WLAN networks. For example, if three logical WLAN networks are active and the beacon period is 100 K μ s, then the beacons will be sent to the three WLANs every 100 K μ s. Depending on the beacon order, the beacons are transmitted at times as follows

Telnet path: /Setup/Interfaces/WLAN/Beaconing

Possible values:

- **Cyclic:** In this mode the access point transmits the first beacon transmission at 0 K μ s to WLAN-1, followed by WLAN-2 and WLAN-3. For the second beacon transmission (100 K μ s) WLAN-2 is the first recipient, followed by WLAN-3 and then WLAN-1. For the third beacon transmission (200 K μ s) the order is WLAN-3, WLAN-1, WLAN-2. After this the sequence starts again.
- **Staggered:** In this mode, the beacons are not sent together at a particular time, rather they are divided across the available beacon periods. Beginning at 0 K μ s, WLAN-1 only is sent; after 33.3 K μ s WLAN-2, after 66.6 K μ s WLAN-3. At the start of a new beacon period, transmission starts again with WLAN-1.
- **Simple burst:** In this mode the access point always transmits the beacons for the WLAN networks in the same order. The first beacon transmission (0 K μ s) is WLAN-1, WLAN-2 and WLAN-3; the second transmission is in the same order, and so on.

Default: Cyclic



Some older WLANs are unable to process the quick succession of beacons which occur with simple burst. Consequently these clients often recognize the first beacons only and can only associate with this network. Staggered transmission of beacons produces better results but increases load on the access point's processor. Cyclic transmission proves to be a good compromise as all networks are transmitted first in turn.

2.23.20.11 Roaming

Roaming settings are only relevant in the client operating mode. They regulate the way that the client switches between multiple base stations, where available.

Telnet path: /Setup/Interfaces/WLAN

2.23.20.11.1 Interface

Opens the Expert settings for the physical WLAN interface.

Telnet path: /Setup/Interfaces/WLAN/Roaming

Possible values:

- Select from the available physical WLAN interfaces.

2.23.20.11.10 Min. connect hold signal level

Similar to the connection hold threshold, but specified as absolute signal strength

Telnet path:/Setup/Interfaces/WLAN/Roaming

Possible values:

■ 0 to -128 dBm

Default: 0

2.23.20.11.11 Block time

If your device is operating as a WLAN client in an environment with multiple WLAN access points all with the same SSID, you can define a time period during which the WLAN client will avoid associating with a particular access point after receiving an "association-reject" from it.

Telnet path:/Setup/Interfaces/WLAN/Roaming

Possible values:

■ 0 to 4294967295 seconds

■ Maximum 10 characters

Default:

■ 0

2.23.20.11.2 Beacon miss threshold

The beacon loss threshold defines how many access-point beacons can be missed before a registered client starts searching again.

Higher values will delay the recognition of an interrupted connection, so a longer time period will pass before the connection is re-established.

The lower the value set here, the sooner a potential interruption to the connection will be recognized; the client can start searching for an alternative access point sooner.

Telnet path:/Setup/Interfaces/WLAN/Roaming

Possible values:

■ 0 to 99%

Default: 4



Values which are too small may cause the client to detect lost connections more often than necessary.

2.23.20.11.3 Roaming threshold

This value is the percentage difference in signal strength between access points above which the client will switch to the stronger access point.

Telnet path:/Setup/Interfaces/WLAN/Roaming

Possible values:

■ 0 to 99%

Default: 15



Other contexts require the value of signal strengths in dB. The following conversion applies:



64dB - 100%



32dB - 50%



0dB - 0%

2.23.20.11.4 No roaming threshold

This threshold refers to the field strength in percent. Field strengths exceeding the value set here are considered to be so good that no switching to another access point will take place.

Telnet path:/Setup/Interfaces/WLAN/Roaming

Possible values:

■ 0 to 99%

Default: 45

2.23.20.11.5 Force roaming threshold

This threshold refers to the field strength in percent. Field strengths below the value set here are considered to be so poor that a switch to another access point is required.

Telnet path:/Setup/Interfaces/WLAN/Roaming

Possible values:

■ 0 to 99%

Default: 12

2.23.20.11.6 Soft roaming

This option enables a client to use scan information to roam to a stronger access point (soft roaming). Roaming due to connection loss (hard roaming) is unaffected by this. The roaming threshold values only take effect when soft roaming is activated.

Telnet path:/Setup/Interfaces/WLAN/Roaming

Possible values:

■ On

■ Off

Default: On

2.23.20.11.7 Connect threshold

This value defines field strength in percent defining the minimum that an access point has to show for a client to attempt to associate with it.

Telnet path:/Setup/Interfaces/WLAN/Roaming

Possible values:

■ 0 to 99%

Default: 0

2.23.20.11.8 Connect hold threshold

This threshold defines field strength in percent. A connection to an access point with field strength below this value is considered as lost.

Telnet path:/Setup/Interfaces/WLAN/Roaming

Possible values:

■ 0 to 99%

Default: 0

2.23.20.11.9 Min. connect signal level

Similar to the connection threshold, but specified as absolute signal strength

Telnet path:/Setup/Interfaces/WLAN/Roaming

Possible values:

■ 0 to -128 dBm

Default: 0

2.23.20.12 Interpoint peers

Here you enter the wireless bases stations that are to be networked via the point-to-point connection.

Telnet path: /Setup/Interfaces/WLAN

2.23.20.12.1 Interface

Opens settings for the point-to-point peers.

Telnet path: /Setup/Interfaces/WLAN/Interpoint-Settings

Possible values:

- Select from the available point-to-point connections.

2.23.20.12.2 Recognize by

Here you select the characteristics to be used to identify the P2P peer.

Telnet path: /Setup/Interfaces/WLAN/Interpoint-Settings

Possible values:

- MAC address: Select this option if the devices are to recognize P2P partners by their MAC address. In this case, fill-out the 'MAC address' with the WLAN MAC address of the physical WLAN interface of the P2P partner.
- Name: Select this option if the devices are to recognize P2P partners by their peer name. In this case, fill-out the 'Peer name' with the device name of the P2P peer or, alternatively, the 'Peer name' defined in the physical settings.
- Serial autoconfig: Use this setting if the P2P peers are to exchange their MAC addresses via a serial connection.

Default: MAC address

2.23.20.12.3 MAC address

MAC address of the P2P remote station

Telnet path: /Setup/Interfaces/WLAN/Interpoint-Settings

Possible values:

- Valid MAC address

Default: Blank



If you work with detection by MAC address, enter the MAC address of the WLAN adapter here and not that of the device itself.

2.23.20.12.4 Peer name

Station name of the P2P remote station

Telnet path: /Setup/Interfaces/WLAN/Interpoint-Settings

Possible values:

- Select from the list of defined peers.

Default: Blank

2.23.20.12.5 Operating

Activates or deactivates this point-to-point channel.

Telnet path: /Setup/Interfaces/WLAN/Interpoint-Settings

Possible values:

- On
- Off

Default: Off

2.23.20.13 Network alarm limits

This table contains the settings for the network alarm limits for the device's logical WLAN networks (SSIDs).

Telnet path: /Setup/Interfaces/WLAN

2.23.20.13.1 Interface

Select the logical WLAN network (SSID) for which you want to edit the network alarm limits.

Telnet path: /Setup/Interfaces/WLAN/Network-Alarm-Limits

Possible values:

- Choose from the SSIDs available in the device, e.g. WLAN-1, WLAN-2, etc.

2.23.20.13.2 Phy signal

The negative threshold value for the signal level of the corresponding SSID. If the value falls below this threshold, an alarm is issued. Setting this value to 0 deactivates the check.

Telnet path: /Setup/Interfaces/WLAN/Network-Alarm-Limits

Possible values:

- 3 numerical characters

Default: 0

2.23.20.13.3 Total retries

The threshold value for the total number of transmission retries for the corresponding SSID. Once the value is reached, an alarm is issued. Setting this value to 0 deactivates the check.

Telnet path: /Setup/Interfaces/WLAN/Network-Alarm-Limits

Possible values:

- 4 numeric characters to specify the repetitions in per mille

Default: 0 per mille

2.23.20.13.4 TX errors

The total number of lost packets for the corresponding SSID. Once the value is reached, an alarm is issued. Setting this value to 0 deactivates the check.

Telnet path: /Setup/Interfaces/WLAN/Network-Alarm-Limits

Possible values:

- 4 numeric characters to specify the repetitions in per mille

Default: 0 per mille

2.23.20.14 Interpoint alarm limits

This table contains the settings for the interpoint alarm limits for the device's P2P connections (SSIDs).

Telnet path: /Setup/Interfaces/WLAN

2.23.20.14.1 Interface

Select the P2P connection here for which you wish to set the interpoint alarm limits.

Telnet path: /Setup/Interfaces/WLAN/Interpoint-Alarm-Limits

Possible values:

- Choose from the P2P connections available in the device, e.g. P2P-1, P2P-2, etc.

2.23.20.14.2 Phy signal

The negative threshold value for the signal level of the corresponding P2P connection. If the value falls below this threshold, an alarm is issued. Setting this value to 0 deactivates the check.

Telnet path: /Setup/Interfaces/WLAN/Interpoint-Alarm-Limits

Possible values:

- 3 numerical characters

Default: 0

2.23.20.14.3 Total retries

The threshold value for the total number of transmission retries for the corresponding P2P connection. Once the value is reached, an alarm is issued. Setting this value to 0 deactivates the check.

Telnet path: /Setup/Interfaces/WLAN/Interpoint-Alarm-Limits

Possible values:

- 4 numeric characters to specify the repetitions in per mille

Default: 0 per mille

2.23.20.14.4 TX errors

The total number of lost packets for the corresponding P2P connection. Once the value is reached, an alarm is issued. Setting this value to 0 deactivates the check.

Telnet path: /Setup/Interfaces/WLAN/Interpoint-Alarm-Limits

Possible values:

- 4 numeric characters to specify the repetitions in per mille

Default: 0 per mille

2.23.21 LAN interfaces

This menu contains the settings for the LAN interfaces.

Telnet path: Setup/Interfaces/LAN-Interfaces

2.23.21.1 Interface

This is where you select the LAN interface to which the subsequent settings are to apply.

Telnet path: /Setup/Interfaces/LAN-Interfaces/lfc

Possible values:

- Select from the available LAN interfaces.

2.23.21.2 Connector

Select the network connection you will use to connect to your local network. If you select **Auto**, the device will automatically detect the connection used.

Telnet path: /Setup/Interfaces/LAN-Interfaces/Connector

Possible values:

- Auto
- Auto-10
- Auto-100
- 10B-T
- FD10B-TX
- 100B-TX
- FD100B-TX
- FD1000B-TX
- Power-Down

Default: Auto



The LAN interfaces of the device are equipped with different types of hardware depending on the model. The first LAN interface supports up to 1000 Mbps in full-duplex mode. The second LAN interface supports a maximum of 100 Mbps in full-duplex mode.

2.23.21.3 MDI mode

This switch activates/deactivates the automatic crossover of send and receive wire pairs (Auto-MDIX) making it unnecessary use node/hub switches or crossover cables. In individual cases (e.g. with certain fiber-optic media converters) it may be necessary to deactivate this automatic function and fix the setting to crossed (MDIX) or non-crossed (MDI).

Telnet path: /Setup/Interfaces/LAN-Interfaces/MDI-Mode

Possible values:

- Auto
- MDI
- MDIX

Default: Auto

2.23.21.5 Clock role

An Ethernet port working in 1000BASE-Tx mode requires a continuous stream of data between both connected partners in order to stay synchronized. The nature of this requires the two ends to have a synchronized clock to transmit data. IEEE 802.3 introduced the concept of a master and a slave for this type of connection. The master provides the clocking for data transmission in both directions while the slave synchronizes to this clock. The roles of clocking master and slave are shared out in the automatic negotiation phase. This aspect can normally be ignored since automatic negotiation works very well in most cases. In some cases it may be necessary to influence master-slave negotiation. For this purpose the following values can be set for clocking:

Telnet path: /Setup/Interfaces/LAN-Interfaces/Clock-Role

Possible values:

- Slave-Preferred: This is the recommended default setting for devices that are not used as a switch. During the negotiation phase, the port will attempt to negotiate the slave role. It will accept the role of master if necessary.
- Master-Preferred: During the negotiation phase, the port will attempt to negotiate the master role. It will accept the role of slave if necessary.
- Slave: The port is set to the role slave only. A connection will be refused if both connection partners use the role of slave.
- Master: The port is set to the role master only. A connection will be refused if both connection partners use the role of master.

Default: Slave-Preferred



The LAN interfaces of the device are equipped with different types of hardware depending on the model. Setting the clocking role has no effect on the second LAN interface.

2.23.21.7 Active

Aktiviere oder deaktiviere die ausgewählte LAN-Schnittstelle.

Telnet path: /Setup/Interfaces/LAN-Interfaces/

Possible values:

- Yes
- No

Default: Yes

2.23.21.8 Tx limit

Enter the bandwidth limit (kbps) in the transmission direction. The value 0 means there is no limit.

Telnet path: Setup/Interfaces/LAN-Interfaces

Possible values:

- Maximum 10 numerical characters

Default: 0



This setting is only available for devices with a WLAN module.

2.23.21.9 Rx limit

Enter the bandwidth limit (kbps) in the receive direction. The value 0 means there is no limit.

Telnet path: Setup/Interfaces/LAN-Interfaces

Possible values:

- Maximum 10 numerical characters

Default: 0

This setting is only available for devices with a WLAN module.

2.23.30 Ethernet ports

The Ethernet interfaces on any publicly accessible LANCOM device can potentially be used by unauthorized persons to gain physical access to a network. The Ethernet interfaces on the device can be disabled to prevent this.

Telnet path: /Setup/Interfaces

2.23.30.1 Port

The name of the selected port.

Telnet path: /Setup/Interfaces/Ethernet-Ports

2.23.30.2 Connector

Select the network connection you will use to connect to your local network. If you select Auto, the device will automatically detect the connection used.

Telnet path: /Setup/Interfaces/Ethernet-Ports

Possible values:

- Auto
- 10B-T
- FD10B-TX
- 100B-TX
- FD100B-TX

Default: Auto

2.23.30.3 Private mode

Once private mode is activated, this switch port is unable to exchange data directly with the other switch ports.

Telnet path: /Setup/Interfaces/Ethernet-Ports

Possible values:

- Yes
- No

Default: No

2.23.30.4 Assignment

Here you select how this interface is to be used.

Telnet path: /Setup/Interfaces/Ethernet-Ports

Possible values:

- LAN-1 to LAN-n: The interface is allocated to a logical LAN.
- DSL-1 to DSL-n: The interface is allocated to a DSL interface.

- Idle: The interface is not allocated to any particular task, but it remains physically active.
- Monitor: The port is a monitor port, i.e. everything received at the other ports is output via this port. A packet sniffer such as Ethereal can be connected to this port, for example.
- Power down: The interface is deactivated.

Default: Depends on the particular interface or the hardware model.

2.23.30.5 MDI mode

This item is used to set the connection type of the switch port. The connection type is either selected automatically or it can be fixed as a crossed (MDIX) or not crossed (MDI) connection.

Telnet path: /Setup/Interfaces/Ethernet-Ports

Possible values: Auto, MDI, MDIX

Default: Auto

2.23.30.6 Clock role

An Ethernet port working in 1000BASE-Tx mode requires a continuous stream of data between both connected partners in order to stay synchronized. The nature of this requires the two ends to have a synchronized clock to transmit data. IEEE 802.3 introduced the concept of a master and a slave for this type of connection. The master provides the clocking for data transmission in both directions while the slave synchronizes to this clock. The roles of clocking master and slave are shared out in the automatic negotiation phase. This aspect can normally be ignored since automatic negotiation works very well in most cases. In some cases it may be necessary to influence master-slave negotiation.

Telnet path: /Setup/Interfaces/Ethernet-Ports/Clock-Role

Possible values:

- Slave-Preferred: This is the recommended default setting for non-switch devices. During the negotiation phase, the port will attempt to negotiate the slave role. It will accept the role of master if necessary.
- Master-Preferred: During the negotiation phase, the port will attempt to negotiate the master role. It will accept the role of slave if necessary.
- Slave: The port is forced to negotiate the slave role. A connection will **not** be established if both connection partners are forced to negotiate the slave role.
- Master: The port is forced to negotiate the master role. A connection will **not** be established if both connection partners are forced to negotiate the master role.

Default: Slave-Preferred

2.23.40 Modem

More commands and options used for an optional external modem connected to the serial interface.

Telnet path: /Setup/Interfaces

2.23.40.5 Dial command

The device issues this command when the external modem is to dial a number. The device takes the telephone number from the list of remote stations and appends it to the string specified here.

Telnet path: /Setup/Interfaces/Modem/Dial-Command

Possible values:

- Maximum 31 alphanumerical characters

Default: DT

2.23.40.14 AT poll count

If the external modem does not respond to the number of AT polls from the device set here, then the device performs a hardware reset for the external modem.

Telnet path:/Setup/Interfaces/Modem/AT-Poll-Count

Possible values

- Numerical characters from 0 to 9

Default: 5

2.23.40.2 Echo-off command

When the modem echo is enabled, the external modem sends back every character it receives. The modem echo must be disabled in order for the external modem to function properly with the device described here. The device uses this command to disable the modem echo.

Telnet path:/Setup/Interfaces/Modem/Echo-Off-Command

Possible values:

- Maximum 9 alphanumerical characters

Default: E0

2.23.40.9 Escape sequence

The device uses this command sequence to transmit individual commands to the modem in the data phase.

Telnet path:/Setup/Interfaces/Modem/Escape-Sequence

Possible values:

- Max. 9 alphanumerical characters

Default: + + +

2.23.40.11 Init. dial

The device sends the initialization sequence for dialing to the external modem before outputting the dial command.

Telnet path:/Setup/Interfaces/Modem/Init.-Dial

Possible values:

- Maximum 63 alphanumerical characters

Default: Blank

2.23.40.11 Init. answer

The device sends the initialization sequence for answering to the external modem before outputting the accept-call command.

Telnet path:/Setup/Interfaces/Modem/Init.-Answer

Possible values:

- Maximum 63 alphanumerical characters

Default: Blank

2.23.40.4 Initialization command

The device uses this command to initialize the external modem.

The device sends this sequence to the external modem after this has had a hardware reset.

Telnet path:/Setup/Interfaces/Modem/Init-Command

Possible values:

- Maximum 63 alphanumerical characters

Default: L0X1M1S0=0

2.23.40.6 Request ID

The device uses this command to query the modem ID. The result is output in the modem status.

Telnet path: /Setup/Interfaces/Modem/Request-ID**Possible values:**

- Maximum 9 alphanumerical characters

Default: I6

2.23.40.3 Reset

The device uses this command to perform a hardware reset on the externally connected modem.

Telnet path: /Setup/Interfaces/Modem/Reset**Possible values:**

- Maximum 9 alphanumerical characters

Default: 8F

2.23.40.1 Ring count

Number of rings before answering.

Telnet path: /Setup/Interfaces/Modem/Ring-Count**Possible values:**

- Numerical characters from 0 to 99

Default: 1

2.23.40.7 Answer command

The device uses this command to accept a call arriving at the external modem.

Telnet path: /Setup/Interfaces/Modem/Answer-Command**Possible values:**

- Max. 9 alphanumerical characters

Default: A

2.23.40.8 Disconnect command

The device uses this command to terminate calls made by the external modem (hang up).

Telnet path: /Setup/Interfaces/Modem/Disconnect-Command**Possible values:**

- Max. 9 alphanumerical characters

Default: H

2.23.40.10 Escape prompt delay (ms)

After the escape sequence, the device waits for the time set here before issuing the command to hang up.

Telnet path: /Setup/Interfaces/Modem/Escape-Prompt-Delay-(ms)

Possible values:

- Numerical values from 0 to 9999 milliseconds

Default: 1000

2.23.40.13 Cycletime AT poll (s)

When disconnected, the device checks the presence and correct functioning of the external modem by sending the string "AT" to the modem. If the modem is connected properly and working, it responds with "OK". The cycle time for the "AT-Poll" defines the time interval between checks.

Telnet path:/Setup/Interfaces/Modem/Cycletime-AT-Poll-(s)

Possible values:

- Numerical characters from 0 to 9 seconds

Default: 1 second

2.23.41 Mobile telephony

The settings for mobile telephony are located here.

Telnet path: /Setup/Interfaces/Mobile

2.23.41.4 Connect monitoring

Monitors WAN-connection establishment. If this fails for the number of connection attempts set under "2.23.41.5. Attempts", the device performs a hard reset of the mobile module.

Telnet path:/Setup/Interfaces/Mobile/Connect-Monitoring

Possible values:

- None: The device does not monitor connection establishment.
- PPP: The device monitors connection establishment for PPP connections.
- PPP+IP: The device monitors connection establishment for PPP and IP connections.

Default: None



Devices with firmware version 8.00 or later ignore the value set under "2.23.41.5 Attempts" and work with the fixed value of "10" connection attempts. This parameter is not available in firmware versions of 8:20 or higher as the device always monitors connection establishment.

2.23.41.8 Enable HSUPA

HSUPA can be activated or deactivated here.

Telnet path:/Setup/Interfaces/Mobile/Enable- HSUPA

Possible values:

- Yes
- No

Default: Yes

2.23.41.2 Scan networks

This command starts a scan for available networks. The networks discovered are listed as a network list under the modem status.

Telnet path:/Setup/Interfaces/Mobile/Scan-Networks

2.23.41.6 History interval (sec)

Logging interval in seconds for the values displayed for the modem status under History.

Telnet path: /Setup/Interfaces/Mobile/History-Interval(sec)

Possible values:

■ 0 to 999999 seconds

Default: 0

Special values: '0' disables the logging of history values.

2.23.41.3 Input PUK

If PIN entry is locked after multiple entries of the wrong number (e.g. because the profile is incorrect), the SIM card must be activated again by entering the PUK. This command starts the the PUK entry procedure.

Telnet path: /Setup/Interfaces/Mobile/Input-PUK

2.23.41.11 Check while connected

Activate this option if the device is also to be allowed to fallback to 2G connections when WAN connections exist.

Telnet path: /Setup/Interfaces/Mobile/Check-while-connected

Possible values:

■ Yes

■ No

Default: Yes



This setting only takes effect if the fallback from 3G to 2G connections has been configured.

2.23.41.10 Threshold 3G-to-2G (dB)

This value specifies the threshold for falling back from 3G to 2G connections. If the signal strength in 3G mode falls below this threshold, then the device switches to a 2G connection (if available). Positive values are automatically converted into negative values.

Telnet path: /Setup/Interfaces/Mobile/Threshold-3G-to-2G[dB]

Possible values:

■ -51 to -111 or 51 to 111 dB

Default: -89 dB

Special values: '0' disables the fallback from 3G to 2G connections.

2.23.41.9 Signal check interval (min)

This value specifies the time in minutes after which the device may switch back a 3G connection (if available).

Telnet path: /Setup/Interfaces/Mobile/Signal-check-interval(min)

Possible values:

■ 0 to 9999 minutes

Default: 0 minutes

Special values: '0' disables the fallback from 3G to 2G connections.

2.23.41.7 Syslog enabled

Activate this option if the history values for modem status (also see '2.23.41.6 History interval (sec)') are additionally to be logged by SYSLOG.

Telnet path:/Setup/Interfaces/Mobile/Syslog-enabled

Possible values:

- Yes
- No

Default: No

2.23.41.5 Tries

Number of connection attempts after which the device performs a hardware reset for the mobile module.

Telnet path:/Setup/Interfaces/Mobile/Attempts

Possible values:

- 3 numerical characters

Default: Blank



The device only uses the number of connection attempts if the option "2.23.41.4 Connect monitoring" is activated. Devices with firmware version 8.00 or later ignore this value and work with the fixed value of "10" connection attempts. This parameter is not available in firmware versions of 8:20 or higher as the device always monitors connection establishment.

2.23.41.1 Profiles

This table contains the settings for the GPRS/UMTS profiles.

Telnet path:/Setup/Interfaces/Mobile/Profiles

2.23.41.1.1 Profile

Specify here a unique name for this UMTS/GPRS profile. This profile can then be selected in the UMTS/GPRS WAN settings.

Telnet path:/Setup/Interfaces/Mobile/Profiles/Profile

Possible values:

- Maximum 16 alphanumerical characters

Default: Blank

2.23.41.1.2 PIN

Enter the 4-digit PIN of the mobile phone SIM card used at the UMTS/GPRS interface. The router needs this information to operate the UMTS/GPRS interface.

Telnet path:/Setup/Interfaces/Mobile/Profiles/PIN

Possible values:

- Max. 6 numerical characters

Default: Blank



The SIM card logs every failed attempt with an incorrect PIN. The number of failed attempts remains stored even when the device is temporarily disconnected from the mains. After 3 failed attempts, the SIM card is locked from further access attempts. If this occurs, you usually need the 8-digit PUK or SuperPIN to unlock it.

2.23.41.1.3 APN

Here you enter the name of the access server for mobile data services known as the APN (Access Point Name). This information is specific to your mobile telephony service provider, and you will find this information in the documentation for your mobile telephony contract.

Telnet path:/Setup/Interfaces/Mobile/Profiles/APN

Possible values:

- Maximum 48 alphanumerical characters

Default: Blank

2.23.41.1.4 Network

If you have opted for manual mobile network selection, then the UMTS/GPRS interface will login only to the mobile network specified here with its full name.

Telnet path:/Setup/Interfaces/Mobile/Profiles/Network

Possible values:

- Maximum 16 alphanumerical characters

Default: Blank

2.23.41.1.5 Select

If you have opted for automatic mobile network selection, then the UMTS/GPRS interface will login to any available and valid mobile network. If you select manual mobile network selection, then the UMTS/GPRS interface will only login to the specified mobile network.

Telnet path:/Setup/Interfaces/Mobile/Profiles/Select

Possible values:

- Auto
- Manual

Default: Auto



Manual selection of the mobile network is useful if the router is operated in a fixed location and the UMTS/GPRS interface should be prevented from logging into other networks, which may offer strong signals, but which may be undesirable or more expensive.

2.23.41.1.6 Mode

This item selects the cellular data transmission standard that is preferred to be used by the UMTS/GPRS interface.

Telnet path:/Setup/Interfaces/Mobile/Profiles/Mode

Possible values:

- Auto
- GPRS
- UMTS

Default: Auto

2.23.41.1.7 QoS downstream data rate

The transfer rates used by the UMTS connection should be entered here to ensure that the Quality of Service (QoS) functions in the firewall work properly.

Telnet path:/Setup/Interfaces/Mobile/Profiles/QoS-Downstream-Datarate

Possible values:

- Max. 5 numerical characters

Default: 0

Special values: 0: The interface is unrestricted and QoS mechanisms do not take effect.

2.23.41.1.8 QoS upstream data rate

The transfer rates used by the UMTS connection should be entered here to ensure that the Quality of Service (QoS) functions in the firewall work properly.

Telnet path:/Setup/Interfaces/Mobile/Profiles/QoS-Upstream-Datarate

Possible values:

- Max. 5 numerical characters

Default: 0

Special values: 0: The interface is unrestricted and QoS mechanisms do not take effect.

2.23.50 Analog

The settings for the analog interface are located here.

Telnet path: /Setup/Interfaces/Analog

2.23.50.8 Lifeline

This item allows you to permanently connect the inactive interface Analog-1 to the line interface.

Telnet path: /Setup/Interfaces/Analog/Lifeline

Possible values:

- ☐ No
- ☐ Yes

Default: No

2.23.50.1 Operating

The analog interfaces on your device can be activated or deactivated here.

Telnet path: /Setup/Interfaces/Analog/Operating

2.23.50.1.1 Interface

Here you select the analog interface that is to be enabled or disabled.

Telnet path: /Setup/Interfaces/Analog/Operating/Ifc

Possible values:

- ☐ Line-1
- ☐ Analog-1
- ☐ Analog-2

Default: Line-1

2.23.50.1.2 Active

Activate or deactivate the corresponding interface here.

Telnet path: /Setup/Interfaces/Analog/Operating/Active

Possible values:

- ☐ Yes
- ☐ No

Default: Yes

2.24 Public Spot module

This menu contains the settings for the Public Spot.

Telnet path: /Setup

2.24.19 Add user wizard

This wizard in WEBconfig provides you with an easy way to create Public Spot user accounts. The wizard automatically generates a username and password and then presents a page for printing out with all the necessary credentials. This menu contains the settings for this wizard.

Telnet path: Setup/Public-Spot-Module

2.24.19.5 Default runtime

In this table, you define the optional default runtimes as presented by the Public Spot Add-User wizard. The wizard offers these options when you create a user account.

Telnet path: Setup/Public-Spot-Module/Add-User-Wizard

2.24.19.5.1 Runtime

Select the runtime of a user account on the Public Spot.

Telnet path: /Setup/Public-Spot-Module/Default-Runtime

Possible values: Max. 5 characters

Default: Blank

2.24.19.5.2 Unit

Select the unit to be used for the runtime of a user account on the Public Spot.

Telnet path: /Setup/Public-Spot-Module/Default-Runtime

Possible values:

■ Minute(s)



■ Hour(s)



■ Day(s)



Default: Hour(s)

2.24.19.6 Comment fields

In this table, you define the comment fields for the Public Spot Add-User wizard.

Telnet path: /Setup/Public-Spot-Module/Add-User-Wizard/Comment-Fields

2.24.19.6.1 Field name

The Public Spot Add-User wizard can print out up to 5 comments on the form. This item is used to set the names of the comment fields that are displayed by the wizard when creating the user accounts.

Telnet path: /Setup/Public-Spot-Module/Add-User-Wizard/Comment-Fields/Field-Name

Possible values:

■ Max. 31 characters



Default: Blank



Activate the printout of the comments with the option 2.24.19.8 Print-Comments-On-Voucher.

2.24.19.2 Username pattern

This item defines the format of the name of new user accounts.

Telnet path: Setup/Public-Spot-Module/Add-User-Wizard

Possible values:

■ Max. 19 characters The string '%n' is a placeholder for a unique account number that is automatically generated by the Public Spot.



Default: user%n

2.24.19.8 Print comments on voucher

This item activates or deactivates the printout of the comment fields on the voucher for a Public Spot user.

Telnet path: /Setup/Public-Spot-Module/Add-User-Wizard/Print-Comments-On-Voucher

Possible values:

- Yes
- No

Default: No

2.24.19.9 Maximal voucher validity period

This value defines the maximum validity period of the voucher in days.

Telnet path: /Setup/Public-Spot-Module/Add-User-Wizard/Maximal-Voucher-Validity-Period

Possible values:

- Max. 10 characters
-

Default: 365 days

If you starting time for the voucher's runtime to 'first login' (2.24.19.7 Default starting time), the runtime for the vouchers will begin at some time in the future. The maximum validity period takes precedence over the runtime of the individual voucher. If the user activates the voucher, the runtime could potentially have expired already or could expire during the intended runtime.

2.24.19.3 Password length

Define the length of the password generated for a new account by the Public Spot Add-User wizard.

Telnet path: Setup/Public-Spot-Module/Add-User-Wizard

Possible values:

- 0 to 255

Default: 6

2.24.19.4 SSID

Enter the SSID that Public Spot Add-User wizard prints out on the form for the user.

Telnet path: Setup/Public-Spot-Module/Add-User-Wizard

English description: SSID

Possible values:

- Max. 32 alphanumerical characters

Default: Blank

If you leave this field blank, the Public Spot Add-User wizard fills out the form with the SSID of the first logical WLAN with an activated Public Spot.

2.24.19.7 Default starting time

Here you select the starting time at which the voucher's runtime begins. By using the option to commence the runtime at the first login, you can print out a supply of vouchers in advance. The user can still use the full runtime.

Telnet path: /Setup/Public-Spot-Module/Add-User-Wizard/Default-Starting-time

Specify the default starting time here.

Possible values:

- Immediately
- First login

Default: First login

2.24.19.10 Available expiry methods

Use this setting to determine which expiry methods are offered by the Public-Spot add-user wizard when creating new user accounts.

Telnet path: /Setup/Public-Spot-Module/Add-User-Wizard/Available-Expiry-Methods

Possible values:

- All methods: The wizard offers all of the available expiry methods.
- Current time method: The expiry method offered by the wizard is based on the current time. The runtime of a user account created with this method begins immediately when the user account is created.
- Login-time method: The expiry method offered by the wizard is based on the login time. The runtime of a user account created with this method begins when the user logs in to the Public Spot for the first time.

Default: All methods *If you select the login-time method, the user account could feasibly expire before the user has logged in for the first time if this time is longer than the maximum voucher validity period (2.24.19.9 Maximum-Voucher-Validity-Period).*

2.24.3 Provider table

When you configure a public spot, the user credentials for authentication and for accounting can be forwarded to one or more RADIUS servers. These are configured in the provider list.

Telnet path: Setup/Public-Spot-Module



In addition to the dedicated parameters for the RADIUS providers, you must enter the general RADIUS parameters, such as the retry and timeout values, into the appropriate configuration areas.

2.24.3.1 Name

Name of the RADIUS server provider who supplies the authentication and/or accounting.

Telnet path: /Setup/Public-Spot-Module/Provider-Table/Name

Possible values:

- Max. 16 alphanumeric characters



Default: Blank

2.24.3.2 Auth. server address

Enter here the IP address of the server that the Public Spot contacts for authenticating the access sessions with this provider.

Telnet path: /Setup/Public-Spot-Module/Provider-Table/Auth.-Server-Address

Possible values:

- Valid IP address

Default: 0.0.0.0

2.24.3.3 Auth. server port

Enter here the port used by the server that the Public Spot requests for authenticating the access sessions with this provider.

Telnet path: /Setup/Public-Spot-Module/Provider-Table/Auth.-Server-Port

Possible values:

- Valid port descriptor

Default: 10

2.24.3.4 Auth. server secret

Enter here the key (shared secret) for access to the RADIUS server of the provider. Ensure that this key is consistent with that in the RADIUS server.

Telnet path: /Setup/Public-Spot-Module/Provider-Table/Auth.-Server-Secret

Possible values:

- Max. 32 alphanumerical characters

Default: Blank

2.24.3.9 Auth. server loopback addr.

Enter here the loopback address of the server that the Public Spot contacts for authenticating the access sessions with this provider.

Telnet path: /Setup/Public-Spot-Module/Provider-Table/Auth.-Server-Loopback-Addr.

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LBO... LBF for the 16 loopback addresses
- Any valid IP address

Default: Blank

2.24.3.11 Auth. server protocol

This item selects the protocol that the Public Spot is to use for authenticating access sessions with this provider.

Telnet path: /Setup/Public-Spot-Module/Provider-Table/Auth.-Server-Protocol

Possible values:

- RADIUS
- RADSEC

Default: RADIUS

2.24.3.5 Acc. server address

Enter here the IP address of the server that the Public Spot contacts for accounting the access sessions with this provider.

Telnet path: /Setup/Public-Spot-Module/Provider-Table/Auth.-Server-Address

Possible values:

- Valid IP address

Default: 0.0.0.0

2.24.3.6 Acc. server port

Enter here the port used by the server that the Public Spot uses for the accounting of the access sessions with this provider.

Telnet path: /Setup/Public-Spot-Module/Provider-Table/Acc.-Server-Port

Possible values:

- Valid port descriptor

Default: 10

2.24.3.7 Acc. server secret

Enter here the key (shared secret) for access to the accounting server of the provider. Ensure that this key is consistent with that in the accounting server.

Telnet path: /Setup/Public-Spot-Module/Provider-Table/Acc.-Server-Secret

Possible values:

- Max. 32 alphanumerical characters

Default: Blank

2.24.3.10 Acc. server loopback addr.

Enter here the loopback address of the server that the Public Spot contacts for accounting the access sessions with this provider.

Telnet path: /Setup/Public-Spot-Module/Provider-Table/Acc.-Server-Loopback-Addr.

Possible values:

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LBO... LBF for the 16 loopback addresses
- Any valid IP address

Default: Blank

2.24.3.12 Acc. server protocol

This item selects the protocol that the Public Spot is to use for the accounting of the access sessions with this provider.

Telnet path: /Setup/Public-Spot-Module/Provider-Table/Acc.-Server-Protocol

Possible values:

- RADIUS
- RADSEC

Default: RADIUS

2.24.3.8 Backup

From the provider table, select a different entry to be used as backup. If the server at the primary provider is unavailable, the Public Spot contacts the backup provider for authentication and/or accounting of access sessions.

Telnet path: /Setup/Public-Spot-Module/Provider-Table/Backup

Possible values:



- Selection from the list of defined RADIUS providers (max. 16 characters).



Default: Blank

2.24.2 User table

Users who are to be granted access to your network are created as entries in the user table.

Telnet path: Setup/Public-Spot-Module

2.24.2.1 Name

Enter the user's name.

Telnet path:/Setup/Public-Spot-Module/User-Table/Name

Possible values:

- Max. 64 characters

2.24.2.2 Password

Enter a password.

Telnet path:/Setup/Public-Spot-Module/User-Table/Password

Possible values:

- Max. 16 characters

2.24.2.3 MAC address

Enter the MAC address here.

Telnet path:/Setup/Public-Spot-Module/User-Table/MAC-Address

Possible values:

- Max. 12 characters

2.24.2.4 Comment

You can enter a comment here.

Telnet path:/Setup/Public-Spot-Module/User-Table/Comment

Possible values:

- Max. 80 characters

2.24.2.5 Provider

Enter the provider's name.

Telnet path:/Setup/Public-Spot-Module/User-Table/Provider

Possible values:

- Max. 16 characters

2.24.2.6 Expiry

Enter the validity period for this setting (date).

Telnet path:/Setup/Public-Spot-Module/User-Table/Expiry

Possible values:

- Max. 20 characters

2.24.31 Free networks

In addition to freely available web servers, you can define other networks which your customers can access without having to log on.

Telnet path: Setup/Public-Spot-Module

2.24.31.1 Host name

Enter an IP address or host name here for a server or network that your customers are allowed to access.

Telnet path: /Setup/Public-Spot-Module/Add-User-Wizard/Free-Networks/Host-Name

Possible values:

- Max. 64 characters

Default: Blank

2.24.31.2 Mask

Enter the associated netmask here. If you wish to authorize just a single workstation with the previously specified IP address, enter 255.255.255.255 here. If you wish to authorize a whole IP network, enter the corresponding netmask.

Telnet path: /Setup/Public-Spot-Module/Add-User-Wizard/Free-Networks/Mask

Possible values:

- Max. 15 characters

Default: 0.0.0.0

2.24.15 Port table

This table is used to activate or deactivate the authentication by Public Spot for the ports on the device.

Telnet path: /Setup/Public-Spot module/Port-Table

2.24.15.2 Port

Select the port for which you want to activate or deactivate authentication by the Public Spot.

Telnet path: /Setup/Public-Spot-Module/Port-Table/Port

Possible values:

- Choose from the device's ports, e.g. LAN-1

2.24.15.3 Authentication necessary

Activate or deactivate authentication by the Public Spot for the selected port.

Telnet path: /Setup/Public-Spot-Module/Port-Table/Authentication-Necessary

Possible values:

- Yes
- No

Default: No

2.24.8 Page table

In addition to freely available web servers, you can define customized pages which your customers can access without having to log on.

The page table allows you to link certain pre-defined events with certain pages on your servers, so that when these events occur the standard pages are displayed.

Telnet path: Setup/Public-Spot-Module

2.24.8.1 Page

Name of the page that your customers can use without logging in.

Telnet path: /Setup/Public-Spot-Module/Page-Table/Page

2.24.8.2 URL

URL of the page that your customers can use without logging in.

Telnet path: /Setup/Public-Spot-Module/Page-Table/URL

Possible values:

- Max. 100 characters

Default: By default, different HTML pages stored on the device file system can be displayed, depending on the page chosen by the user.

2.24.8.3 Fallback

Enable or disable the fallback to the "on-board" page in case the Public Spot cannot display the user-defined URL.

Telnet path: /Setup/Public-Spot-Module/Page-Table/Fallback

Possible values:

- Yes
- No

Default: No

2.24.8.4 Type

Select the type of the page.

Telnet path: /Setup/Public-Spot-Module/Page-Table/Type

Possible values:

- Template
- Redirect

Default: Template

2.24.8.5 Loopback address

Enter a loopback address.

Telnet path: /Setup/Public-Spot-Module/Page-Table/Loopback-Addr.

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ

- LBO to LBF for the 16 loopback addresses
- Any valid IP address

Default: Blank

2.24.20 VLAN table

By default, all data is routed via the relevant interface. However if VLAN-ID tags are specified, the only data to be routed via the relevant interface is that tagged with the specified VLAN-ID. Only select VLAN-IDs here if you do not want all data packets to be routed via the corresponding interface.

Telnet path: Setup/Public-Spot-Module

2.24.20.1 VLAN-ID

Enter the VLAN ID here.

Telnet path: /Setup/Public-Spot-Module/Add-User-Wizard/VLAN-Table/VLAN-ID

Possible values:

- 0 to 4096

Default: Blank

2.24.7 Accounting cycle

Define the time in seconds for the accounting cycle.

Telnet path: Setup/Public-Spot-Module

2.24.1 Authentication mode

Your device supports user login at a Public Spot. To login, the user has to enter a user name and password. You can also specify an additional check by MAC address.

Users who are to be granted access to your network are created as entries in the user table.

Telnet path: Setup/Public-Spot-Module

Possible values:

- None
- User+password
- MAC+user+password

2.24.16 Auto-cleanup user table

This item determines whether the user list is automatically cleaned up. Since the size of the user table is limited, outdated user accounts should be deleted as soon as possible.

Telnet path: Setup/Public-Spot-Module

Possible values:

- Yes
 - ☐
- No
 - ☐

Default: No

2.24.30 Free server

Enter the IP address of the public page used by your Public Spot service. This page should provide information enabling the new user to contact you and register.

Telnet path: /Setup/Public-Spot-Module/Free-Server

Possible values:

- Max. 64 characters

Default: Blank

2.24.22 Device hostname

Certificates are normally issued for DNS names, so the Public Spot must specify the certificate's DNS name as the destination and not an internal IP address. This name has to be resolved by the DNS server to provide the corresponding IP address of the Public Spot.

Telnet path: Setup/Public-Spot-Module

Possible values:

- Max. 31 characters

Default: Blank

2.24.14 Idle timeout

If an idle timeout has been defined (either here or by RADIUS) the Public Spot terminates the connection if no data was received from the client within the specified interval.

Telnet path: Setup/Public-Spot-Module

Possible values:

- Max. 10 characters

Default: 0

2.24.12 Communication port

Here you set the port that the Public Spot uses to communicate with the clients associated with it.

Telnet path: /Setup/Public-Spot-Module/Communication-Port

Possible values:

- - Any valid port descriptor, max. 5 characters
 -

Default: Blank

2.24.21 Login page type

Here you select the protocol to be used by the Public Spot to display the login pages.

Telnet path: /Setup/Public-Spot-Module/Login-Page-Type

Possible values:

- HTTP
- HTTPS

Default: HTTPS

2.24.9 Roaming secret

When moving into the signal coverage area of another base station (roaming), it is necessary to login again. If you are located in the overlap area between two stations, you may even experience a regular change of connection between the two base stations. The task of the roaming secret is to allow Public Spot sessions to be passed between access points without the user having to login again.

Telnet path: /Setup/Public-Spot-Module/Roaming-Secret

Possible values:

- Max. 32 characters

Default: Blank

2.24.17 Provide server database

Here you can select whether the Public Spot provides the MAC address list via RADIUS.

Telnet path: /Setup/Public-Spot-Module/Provide-Server-Database

Possible values:

- Yes
- No

Default: No

2.24.6 Server subdir

Enter the directory for the public page used by your Public Spot service. This page should provide information enabling the new user to contact you and register.

Telnet path: /Setup/Public-Spot-Module/Server-Subdir

Possible values:

- Max. 127 characters

Default: Blank

2.24.5 Traffic limit bytes

Even before login and quite independent of the servers, networks and pages mentioned earlier, traffic is generated by DHCP, DNS and ARP requests. These requests are allowed. However, they can be misused to tunnel other data.

To counter this, you can define a maximum transfer volume here. This affects only the data exchanged before login and not the data sent to or from the free web servers mentioned above. This remains unlimited at all times.

Telnet path: Setup/Public-Spot-Module

Possible values:

- - Max. 10 characters
 -

Default: 0

2.24.18 Disallow multiple logins

Allows a single user account to login multiple times simultaneously.

Telnet path: Setup/Public-Spot-Module

Possible values:

■ No

□

■ Yes

□

Default: No *The multiple-login option must be deactivated if the RADIUS server is to monitor a time budget. The time budget can only be monitored if the user is running just one session at a time.*

2.25 RADIUS

This menu contains the settings for the RADIUS server.

Telnet path: /Setup

2.25.4 Authentication timeout

This value specifies how many milliseconds should elapse before retrying RADIUS authentication.

Telnet path: /Setup/RADIUS

Possible values:

■ Max. 10 characters

Default: 5000

2.25.5 Authentication retry

This value specifies how many authentication attempts are made in total before a Reject is issued.

Telnet path: /Setup/RADIUS

Possible values:

■ Max. 10 characters

Default: 3

2.25.9 Backup query strategy

This value specifies how the device should handle unanswered queries from multiple RADIUS servers.

Telnet path: /Setup/RADIUS/Backup-Query-Strategy

Possible values:

■ Block: The device first returns the maximum number of repeat queries to the first server before forwarding them to the backup server.

■ Cyclic: The device sends unanswered queries to the configured servers by turns.

Default: Block

2.25.10 Server

This menu contains the settings for the RADIUS server.

Telnet path: /Setup/RADIUS

2.25.10.12 Accounting interim interval

Enter the value that the RADIUS server should output as "Accounting interim interval" after successful authentication. Provided the requesting device supports this attribute, this value determines the intervals (in seconds) at which an update of the accounting data is sent to the RADIUS server.

Telnet path: /Setup/RADIUS/Server

Possible values:

■ Max. 4 numbers

Default: 0

Special values: 0: Switches the use of this function off.

2.25.10.11 Accounting port

Enter the port used by the RADIUS server to receive accounting information. Port '1813' is normally used.

Telnet path: /Setup/RADIUS/Server

Possible values:

■ Max. 4 numbers

Default: 0

Special values: 0: Switches the use of this function off.

2.25.10.1 Authentication port

Specify here the port used by the authenticators to communicate with the RADIUS server in the access point.

Telnet path: /Setup/RADIUS/Server

Possible values:

■ Max. 5 numbers

Default: 0

Special values: 0: Switches the RADIUS server off.

2.25.10.14 Auto-cleanup user table

With this feature enabled, the RADIUS server automatically deletes accounts from the Users table when the expiry date has passed.

Telnet path: /Setup/RADIUS/Server/Auto-Cleanup-User-Table

Possible values:

■ Yes

■ No

Default: No

2.25.10.5 Default realm

This realm is used if the user name is supplied with an unknown realm that is not in the list of forwarding servers.

Telnet path: /Setup/RADIUS/Server

Possible values:

■ Max. 24 characters

Default: Blank

2.25.10.6 Empty realm

This realm is used when the user name supplied does not contain a realm.

Telnet path: /Setup/RADIUS/Server

Possible values:

■ Max. 24 characters

Default: Blank

2.25.10.13 RADSEC port

Enter the (TCP) port used by the server to accept accounting or authentication requests encrypted using RADSEC. Port 2083 is normally used.

Telnet path: /Setup/RADIUS/Server

Possible values:

■ Max. 5 numbers

Default: 0

Special values: 0: Deactivates RADSEC in the RADIUS server.

2.25.10.2 Clients

Clients that can communicate with the RADIUS server are entered in the clients table.

Telnet path: /Setup/RADIUS/Server

2.25.10.2.1 IP network

IP network (IP address range) of RADIUS clients for which the password defined in this entry applies.

Telnet path: /Setup/RADIUS/Server/Clients

Possible values:

■ Valid IP address.

Default: Blank

2.25.10.2.2 Secret

Password required by the client for access to the RADIUS server in the LANCOM access point.

Telnet path: /Setup/RADIUS/Server/Clients

Possible values:

■ Max. 32 characters

Default: Blank

2.25.10.2.3 IP netmask

IP network mask of the RADIUS client.

Telnet path: /Setup/RADIUS/Server/Clients

Possible values:

■ Valid IP address.

Default: Blank

2.25.10.2.4 Protocol

Protocol for communication between the internal RADIUS server and the clients.

Telnet path: /Setup/RADIUS/Server/Clients

Possible values:

■ RADSEC

■ RADIUS

■ all

Default: RADIUS

2.25.10.3 Forward servers

If you wish to use RADIUS forwarding, you have to specify further settings here.

Telnet path: /Setup/RADIUS/Server

2.25.10.3.1 Realm

Character string identifying the forwarding destination.

Telnet path: /Setup/RADIUS/Server/Forward-Servers

Possible values:

- Max. 24 characters

Default: Blank

2.25.10.3.2 IP address

IP address of the RADIUS server to which the request is to be forwarded.

Telnet path: /Setup/RADIUS/Server/Forward-Servers

Possible values:

- Valid IP address.

Default: 00.0.0

2.25.10.3.3 Port

Open port for communications with the forwarding server.

Telnet path: /Setup/RADIUS/Server/Forward-Servers

Possible values:

- Max. 10 characters

Default: 0

2.25.10.3.4 Secret

Password required for accessing the forwarding server.

Telnet path: /Setup/RADIUS/Server/Forward-Servers

Possible values:

- Max. 32 characters

Default: Blank

2.25.10.3.5 Backup

Alternative forwarding server in case the first forwarding server is not available.

Telnet path: /Setup/RADIUS/Server/Forward-Servers

Possible values:

- Max. 24 characters

Default: Blank

2.25.10.3.6 Loopback address

This is where you can configure an optional sender address to be used instead of the one otherwise automatically selected for the destination address.

Telnet path: /Setup/RADIUS/Server/Forward-Servers

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LBO to LBF for the 16 loopback addresses
- Any valid IP address

Default: Blank



If the list of IP networks or loopback addresses contains an entry named 'DMZ' then the associated IP address will be used.

2.25.10.3.7 Protocol

Protocol for communication between the internal RADIUS server and the forwarding server.

Telnet path: /Setup/RADIUS/Server/Forward- Servers

Possible values:

- RADSEC
- RADIUS

Default: RADIUS

2.25.10.7 Users

In the following table, enter the data for the users that are to be authenticated by this server.

Telnet path: /Setup/RADIUS/Server/Users

Multiple logins

Allows a single user account to login multiple times simultaneously.

Possible values: Yes, No

Default: Yes



The multiple-login option must be deactivated if the RADIUS server is to monitor a time budget. The time budget can only be monitored if the user is running just one session at a time.

Expiry type

This option defines how the validity period is limited for a user account.

Possible values:

- Absolute: The validity of the user account terminates at a set time.
- Relative: The validity of the user account terminates a certain period of time after the first user login.

Default: Blank: The user account never expires, unless a predefined time or volume budget expires.



The two options can be combined. In this case the user account expires when one of the two limiting values has been reached.



The device must have a valid time in order for the device to work with user-account time budgets.

Abs. expiry

If "absolute" has been selected as the expiry type, the user account becomes invalid at the time defined by this value.

Possible values: Valid time information (date and time). Max. 20 characters from 0123456789/..Pp

Default: Blank

Special values: 0 switches off the monitoring of the absolute expiry time.

Rel. expiry

If "relative" has been selected as the expiry type, the user account becomes invalid after this time period has expired since the user logged in for the first time.

Possible values: Time span in seconds. Max. 10 characters from 0123456789

Default: 0

Special values: 0 switches off the monitoring of the relative expiry time.

Time budget

The maximum duration of access time for this user account. The user can use this duration of access time until a relative or absolute expiry time (if set) is reached.

Possible values: Time span in seconds. Max. 10 characters from 0123456789

Default: 0

Special values: 0 switches off the monitoring of the time budget.

Volume budget

The maximum data volume for this user account. The user can use this data volume until a relative or absolute expiry time (if set) is reached.

Possible values: Volume budget in Bytes. Max. 10 characters from 0123456789

Default: 0

Special values: 0 switches off the monitoring of data volume.

Comment

Comment on this entry.

Service type

The service type is a special attribute of the RADIUS protocol. The NAS (Network Access Server) sends this with the authentication request. The response to this request is only positive if the requested service type agrees with the user account service type.

Possible values:

- Framed: For checking WLAN MAC addresses via RADIUS or IEEE 802.1x.
- Login: For Public-Spot logins.
- Auth. only: For RADIUS authentication of dialup peers via PPP.
- Any

Default: Any



The number of entries permissible with the service type "any" or "login" is 64 or 256, depending on the model. This means that the table is not completely filled with entries for Public Spot access accounts (using the service type "Any") and it enables the parallel use of logins via 802.1x.

2.25.10.7.1 User name

User name.

Telnet path: /Setup/RADIUS/Server/Users

Possible values:

- Max. 48 characters

Default: Blank

2.25.10.7.10 Absolute expiry

If "absolute" has been selected as the expiry type, the user account becomes invalid at the time defined by this value.

Telnet path: /Setup/RADIUS/Server/Users/Abs.-Expiry

Possible values:

- Valid time information (date and time). Max. 20 characters from 0123456789/.

Default: 0

Special values: 0 switches off the monitoring of the absolute expiry time.

2.25.10.7.11 Time budget

The maximum duration of access time for this user account. The user can use this duration of access time until a relative or absolute expiry time (if set) is reached.

Telnet path: /Setup/RADIUS/Server/Users/Time-Budget

Possible values:

- Time span in seconds. Max. 10 characters from 0123456789

Default: 0

Special values: 0 switches off the monitoring of the time budget.

2.25.10.7.12 Volume budget

The maximum data volume for this user account. The user can use this data volume until a relative or absolute expiry time (if set) is reached.

Telnet path: /Setup/RADIUS/Server/Users/Volume-Budget

Possible values:

- Volume budget in Bytes. Max. 10 characters from 0123456789

Default: 0

Special values: 0 switches off the monitoring of data volume.

2.25.10.7.13 Expiry type

This option defines how the validity period is limited for a user account.

Telnet path: /Setup/RADIUS/Server/Users/Expiry-Type

Possible values:

- Absolute: The validity of the user account terminates at a set time.
- Relative: The validity of the user account terminates a certain period of time after the first user login.
- None: The user account never expires, unless a predefined time or volume budget expires.

Default: Absolute *The two options can be combined. In this case the user account expires when one of the two limiting values has been reached.*



The device must have a valid time in order for the device to work with user-account time budgets.

2.25.10.7.14 Relative expiry

If "relative" has been selected as the expiry type, the user account becomes invalid after this time period has expired since the user logged in for the first time.

Telnet path: /Setup/RADIUS/Server/Users/Rel.-Expiry

Possible values:

- Time span in seconds. Max. 10 characters from 0123456789

Default: 0

Special values: 0 switches off the monitoring of the relative expiry time.

2.25.10.7.15 Comment

Comment on this entry.

Telnet path: LCOS Menu Tree/Setup/RADIUS/Server/Users/Comment

Possible values:

- Max. 64 characters

Default: Blank

2.25.10.7.16 Service type

The service type is a special attribute of the RADIUS protocol. The NAS (Network Access Server) sends this with the authentication request. The response to this request is only positive if the requested service type agrees with the user account service type. For example, the service type for Public Spot is 'Login' and for 802.1x 'Framed'.

Telnet path: /Setup/RADIUS/Server/Users/Service-Type

Possible values:

- Any
- Framed: For checking WLAN MAC addresses via RADIUS or IEEE 802.1x.
- Login: For Public-Spot logins.
- Auth. only: For RADIUS authentication of dialup peers via PPP.

Default: Any



The number of entries permissible with the service type "any" or "login" is 64 or 256, depending on the model. This means that the table is not completely filled with entries for Public Spot access accounts (using the service type "Any") and it enables the parallel use of logins via 802.1x.

2.25.10.7.2 Password

User password.

Telnet path: /Setup/RADIUS/Server/Users

Possible values:

- Max. 32 characters

Default: Blank

2.25.10.7.3 Limit authentication methods

This option allows you to place limitations on the authentication methods permitted for the user.

Telnet path: /Setup/RADIUS/Server/Users

Possible values:

- Any combination of the following values:
- PAP
- CHAP
- MSCHAP
- MSCHAPv2
- EAP
- All

Default: All

2.25.10.7.4 VLAN-ID

This option allows a certain VLAN ID to be assigned to the user on successful authorization.

Telnet path: /Setup/RADIUS/Server/Users

Possible values:

- 0 to 4094

Default: 0

Special values: 0: No VLAN ID will be assigned.

2.25.10.7.5 Calling station ID mask

This mask is used to restrict the validity of the entry to certain IDs that are communicated by the calling station (wireless LAN client). When authenticating via 802.1x the calling station's MAC address is transmitted in ASCII format (capital letters only), with a hyphen separating pairs of characters (for example "00-10-A4-23-19-C0")

Telnet path: /Setup/RADIUS/Server/Users

Possible values:

- Max. 48 characters

Default: Blank

Special values: The wildcard * can be used to include whole groups of IDs and define them as mask.

2.25.10.7.6 Called station ID mask

This mask is used to restrict the validity of the entry to certain IDs that are communicated by the called station (access point's BSSID and SSID). When authenticating via 802.1x the called station's MAC address (BSSID) is transmitted in ASCII format (capital letters only), with a hyphen separating pairs of characters. The SSID is appended using a colon as separator (for example "00-10-A4-23-19-C0:AP1")

Telnet path: /Setup/RADIUS/Server/Users

Possible values:

- Max. 48 characters

Default: Blank

Special values: The wildcard * can be used to include whole groups of IDs and define them as mask. The mask "*:AP1*", for example, defines an entry that applies to a client in a radio cell with the name "AP1" irrespective of the access point that the client uses to log in. This allows the client to switch (roam) from one access point to the next while always using the same authentication data.

2.25.10.7.7 Tx limit

Limitation of bandwidth for RADIUS clients.

Telnet path: /Setup/RADIUS/Server/Users/Tx-Limit

Possible values:

- 0 to 4294967295 ($2^{32}-1$)

Default: 0

2.25.10.7.8 Rx limit

Limitation of bandwidth for RADIUS clients.

Telnet path: /Setup/RADIUS/Server/Users/Rx-Limit

Possible values:

■ 0 to 4294967295 ($2^{32}-1$)

Default: 0

2.25.10.7.9 Multiple login

Allows or prohibits more than one parallel session with the same user ID. If parallel sessions are prohibited, the device rejects authentication requests for a user ID for which a session is already running in the active session accounting table. This is a prerequisite to enforce time and volume budgets.

Telnet path: /Setup/RADIUS/Server/Users/Multiple-Login

Possible values:

■ Yes

■ No

Default: Yes



The multiple-login option must be deactivated if the RADIUS server is to monitor a time budget. The time budget can only be monitored if the user is running just one session at a time.

2.25.10.10 EAP

This menu contains the EAP settings.

Telnet path: /Setup/RADIUS/Server

2.25.10.10.6 PEAP default tunnel method

Two authentication methods are negotiated when PEAP is used. A secure TLS tunnel is first negotiated using EAP. Then a second authentication method is negotiated in this tunnel. In each of these negotiating processes the server offers a method that the client can either accept (ACK) or reject (NAK). The the client rejects it, it sends the server a proposal for a method that it would like to use. If enabled in the server, the method proposed by the client is will be used. Otherwise the server breaks off negotiation.

This parameter is used to determine the method that the server offers to clients for authentication in the TLS tunnel. The value specified here can help to avoid rejected proposals and thus speed up the process of negotiation.

Telnet path: /Setup/RADIUS/Server/EAP

Possible values:

■ None

■ MD5

■ GTC

■ MSCHAPv2

Default: MSCHAPv2

2.25.10.10.3 Reauthentication period

When the internal RADIUS server responds to a client request with a CHALLENGE (negotiation of authentication method not yet completed), the RADIUS server can inform the authenticator how long it should wait (in seconds) for a response from the client before issuing a new CHALLENGE.

Telnet path: /Setup/RADIUS/Server/EAP

Possible values:

■ Max. 10 numbers

Default: 0

Special values: 0: No timeout is sent to the authenticator.



The function is not supported by all authenticators.

2.25.10.10.4 Retransmit timeout

When the internal RADIUS server responds to a client request with an ACCEPT (negotiation of authentication method completed successfully), the RADIUS server can inform the authenticator how long it should wait (in seconds) before triggering repeat authentication of the client.

Telnet path: /Setup/RADIUS/Server/EAP

Possible values:

- Max. 10 numbers

Default: 0

Special values: 0: No timeout is sent to the authenticator.



The function is not supported by all authenticators.

2.25.10.10.2 TLS check username

TLS authenticates the client via certificate only. If this option is activated, the RADIUS server additionally checks if the username in the certificate is contained in the RADIUS user table.

Telnet path: /Setup/RADIUS/Server/EAP

Possible values:

- Yes
- No

Default: No

2.25.10.10.5 TTLS default tunnel method

Two authentication methods are negotiated when TTLS is used. A secure TLS tunnel is first negotiated using EAP. Then a second authentication method is negotiated in this tunnel. In each of these negotiating processes the server offers a method that the client can either accept (ACK) or reject (NAK). The the client rejects it, it sends the server a proposal for a method that it would like to use. If enabled in the server, the method proposed by the client is will be used. Otherwise the server breaks off negotiation.

This parameter is used to determine the method that the server offers to clients for authentication in the TLS tunnel. The value specified here can help to avoid rejected proposals and thus speed up the process of negotiation.

Telnet path: /Setup/RADIUS/Server/EAP

Possible values:

- None
- MD5
- GTC
- MSCHAPv2

Default: MD5

2.25.10.10.1 Tunnel server

This realm refers to the entry in the table of the forwarding server that is to be used for tunneled TTLS or PEAP requests.

Telnet path: /Setup/RADIUS/Server/EAP

Possible values:

- Max. 24 characters

Default: Blank

2.25.10.10.7 Default method

This value specifies which method the RADIUS server should offer to the client outside of a possible TTLS/PEAP tunnel.

Telnet path: /Setup/RADIUS/Server/EAP

Possible values:

- None
- MD5

- GTC
- MSCHAPv2
- TLS
- TTLS
- PEAP

Default: MD5

2.25.10.10.8 Default MTU

Define the Maximum Transmission Unit to be used by the device as the default for EAP connections.

Telnet path: /Setup/RADIUS/Server/EAP/Default-MTU

Possible values:

- 100 to 1496 bytes

Default: 1036 bytes

2.26 NTP

This menu contains the NTP settings.

Telnet path: /Setup

2.26.2 Operating

Here you switch on the time server in your device for the local network. Other devices in the same network can then synchronize with the server via the network time protocol (NTP).

Telnet path: /Setup/NTP

Possible values:

- Yes
- No

Default: No

2.26.4 BC interval

Here you set the time interval after which your device's time server sends the current time to all devices or stations accessible via the local network.

Telnet path: /Setup/NTP

Possible values:

- Max. 10 characters

Default: 64

2.26.3 BC mode

Here you switch the time server in your device into the send mode. This mode regularly sends the current time to all devices or stations accessible via the local network.

Telnet path: /Setup/NTP

Possible values:

- Yes
- No

Default: No

2.26.7 RQ interval

Specify the time interval in seconds after which the internal clock of the device is re-synchronized with the specified time server (NTP).

Telnet path: /Setup/NTP

Possible values:

■ Max. 10 characters

Default: 86400



A connection may be established in order to access the time server. Please be aware that this may give rise to additional costs.

2.26.12 RQ tries

Enter the number of times that synchronization with the time server should be attempted. Specifying a value of zero means that attempts will continue until a valid synchronization has been achieved.

Telnet path: /Setup/NTP

Possible values:

■ Max. 10 characters

Default: 4

2.26.11 RQ address

Here you enter the time server that supplies the correct current time.

Telnet path: /Setup/NTP

2.26.11.1 RQ address

Enter the time servers (NTP) in the order in which you want to query them. The servers should be accessible via one of the existing interfaces. Caution: A connection may be established in order to access the time server. Please be aware that this may give rise to additional costs.

Telnet path: /Setup/NTP/RQ-Address

Possible values:

■ Max. 31 characters

Default: Blank

2.26.11.2 Loopback address

Here you can optionally configure a sender address to be used instead of the one used automatically for this destination address.

If you have configured loopback addresses, you can specify them here as sender address.

Various forms of entry are accepted:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet.
- "DMZ" for the address of the first DMZ (Note: If there is an interface named "DMZ", its address will be taken).
- LBO... LBF for the 16 loopback addresses.
- Furthermore, any IP address can be entered in the form x.x.x.x.

Telnet path: /Setup/NTP/RQ-Address

Possible values:

■ Name of the IP networks whose address should be used

■ "INT" for the address of the first intranet

- "DMZ" for the address of the first DMZ
- LBO to LBF for the 16 loopback addresses
- Any valid IP address

Default: Blank



If there is an interface called "DMZ", its address will be taken in this case).

2.27 Mail

This menu contains the e-mail settings.

Telnet path: /Setup

2.27.5 User name

Enter the name of the user who is to receive e-mail notifications at the aforementioned SMTP server.

Telnet path: /Setup/Mail

Possible values:

- Max. 63 characters

Default: Blank

2.27.7 E-mail sender

Enter here a valid e-mail address that your device is to use as a sender address for e-mailing notifications. This address is used by the SMTP servers to provide information in case of delivery problems. In addition, some servers check the validity of the sender e-mail address and deny delivery service if the address is missing, if the domain is unknown, or if the e-mail address is invalid.

Telnet path: /Setup/Mail

Possible values:

- Max. 63 characters

Default: Blank

2.27.11 Loopback address

Here you can optionally configure a sender address to be used instead of the one used automatically for this destination address. If you have configured loopback addresses, you can specify them here as sender address.

Telnet path: /Setup/Mail

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LBO to LBF for the 16 loopback addresses
- Any valid IP address

Default: Blank



If there is an interface called "DMZ", its name will be taken in this case.

2.27.6 Password

Enter the password to be used to send e-mail notifications to the aforementioned SMTP server.

Telnet path: /Setup/Mail

Possible values:

- Max. 31 characters

Default: Blank

2.27.4 POP3 port

Enter the number of the POP3 port of the aforementioned server for unencrypted mail. The default value is 110.

Telnet path: /Setup/Mail

Possible values:

■ Max. 10 characters

Default: 110

2.27.3 POP3 server

The only difference between names of many POP3 servers and SMTP servers is the prefix. All you have to do is enter the same of your SMTP server and replace 'SMTP' with 'POP' or "POP3".

Telnet path: /Setup/Mail

Possible values:

■ Max. 31 characters

Default: Blank

2.27.10 Buffers

In case of connection problems with the SMTP server, mails will be buffered here and repeated tries will be made to send them. This also applies for mails which cannot be delivered due to incorrect settings such as incorrect SMTP parameters or unknown recipients. Set the maximum number of buffered messages. When this limit is exceeded, the oldest messages will be discarded to make room for incoming messages.

Telnet path: /Setup/Mail

Possible values:

■ Max. 10 characters

Default: 100

2.27.8 Send again (min)

In case of connection problems with the SMTP server, mails will be buffered here and repeated tries will be made to send them. This also applies for mails which cannot be delivered due to incorrect settings such as incorrect SMTP parameters or unknown recipients. Set the time after which an attempt will be made to re-submit buffered messages. Attempts are also made to re-submit each time a new e-mail is received.

Telnet path: /Setup/Mail

Possible values:

■ Max. 10 characters

Default: 30

2.27.2 SMTP port

Enter the number of the SMTP port of the aforementioned server for unencrypted mail. The default value is 25.

Telnet path: /Setup/Mail

Possible values:

■ Max. 10 characters

Default: 25

2.27.1 SMTP server

Enter the name or the IP address for an SMTP server that you have access to. This information is required if your device is to inform you about certain events by e-mail.

Telnet path: /Setup/Mail

Possible values:

■ Max. 31 characters

Default: Blank



A connection may be established in order to send e-mail messages. Please be aware that this may give rise to additional costs.

2.27.9 Hold time (hrs)

In case of connection problems with the SMTP server, mails will be buffered here and attempts to send them will be repeated. This also applies for mails which cannot be delivered due to incorrect settings such as incorrect SMTP parameters or unknown recipients. Set the maximum hold time for a message. Once this time has elapsed, all attempts to submit a certain message will be discontinued.

Telnet path: /Setup/Mail

Possible values:

■ Max. 10 characters

Default: 72

2.30 IEEE802.1x

This menu contains the settings for the IEEE802.1x protocol.

Telnet path: /Setup

2.30.3 Radius server

Authentication in all wireless LAN networks by a central RADIUS server (named DEFAULT) can be managed here. You can also define RADIUS servers that are dedicated to certain wireless LAN networks (instead of defining the passphrase for the logical wireless LAN network). Furthermore, a backup server can be specified for every RADIUS server.

Telnet path: /Setup/IEEE802.1x

2.30.3.1 Name

The name of the server.

Telnet path: /Setup/IEEE802.1x /RADIUS-Server

Possible values:

■ Max. 16 characters

Default: Blank

2.30.3.2 IP address

IP address of the RADIUS server. The name 'DEFAULT' is reserved for all WLAN networks that use IEEE 802.1x for authentication and that do not have their own RADIUS server. Every WLAN that uses authentication by IEEE 802.1x can use its own RADIUS server after specifying appropriate values for 'Key1/Passphrase'.

Telnet path: /Setup/IEEE802.1x /RADIUS-Server

Possible values:

■ Valid IP address.

Default: 00.0.0

2.30.3.3 Port

The port the RADIUS server.

Telnet path: /Setup/IEEE802.1x /RADIUS-Server

Possible values:

- Max. 10 characters

Default: 0

2.30.3.4 Secret

The secret used by the RADIUS server.

Telnet path: /Setup/IEEE802.1x /RADIUS-Server

Possible values:

- Max. 32 characters

Default: Blank

2.30.3.5 Backup

You can enter the name of a backup server for the specified RADIUS server. The backup server will be connected only if the specified RADIUS server is unavailable. The name of the backup server can be selected from the same table.

Telnet path: /Setup/IEEE802.1x /RADIUS-Server

Possible values:

- Max. 24 characters

Default: Blank

2.30.3.6 Loopback address

Here you can optionally configure a sender address to be used instead of the one used automatically for this destination address. If you have configured loopback addresses, you can specify them here as sender address.

Telnet path: /Setup/IEEE802.1x /RADIUS-Server

Possible values:

- Various forms of entry are accepted:
- Name of the IP networks whose addresses are to be used.
- "INT" for the address of the first intranet.
- "DMZ" for the address of the first DMZ



If there is an interface called "DMZ", its address will be taken in this case.

- LBO – LBF for the 16 loopback addresses.
- Furthermore, any IP address can be entered in the form x.x.x.x.

Default: Blank

2.30.3.7 Protocol

Protocol for communication between the internal RADIUS server and the forwarding server.

Telnet path: /Setup/IEEE802.1x/RADIUS-Server/Protocol

Possible values:

- RADSEC

■ RADIUS

Default: RADIUS

2.30.4 Ports

You should specify the login settings separately for each local network.

Telnet path: /Setup/IEEE802.1x

2.30.4.10 Re-authentication

Here you activate regular re-authentication. If a new authentication starts, the user remains registered during the negotiation. A typical value as a re-authentication interval is 3,600 seconds.

Telnet path: /Setup/IEEE802.1x /Ports

Possible values:

■ Yes

■ No

Default: No

2.30.4.11 Re-authorization interval

A typical value as a re-authentication interval is 3,600 seconds.

Telnet path: /Setup/IEEE802.1x /Ports

Possible values:

■ Max. 10 characters

Default: 3600

2.30.4.12 Key transmission

Here you activate the regular generation and transmission of a dynamic WEP key.

Telnet path: /Setup/IEEE802.1x /Ports

Possible values:

■ Yes

■ No

Default: No

2.30.4.13 Key transmission interval

A typical value as a key-transmission interval is 900 seconds.

Telnet path: /Setup/IEEE802.1x /Ports

Possible values:

■ Max. 10 characters

Default: 900

2.30.4.2 Port

The interface that this entry refers to.

Telnet path: /Setup/IEEE802.1x /Ports

Possible values:

■ All of the interfaces available in the device.

Default: Blank

2.30.4.4 Re-authentication, max.

This parameter is a timer in the authentication state machine for IEEE 802.1x.

Telnet path: /Setup/IEEE802.1x /Ports

Possible values:

■ Max. 10 characters

Default: 3



Changes to these parameters require expert knowledge of the IEEE 802.1x standard. Only make changes here if your system configuration absolutely requires them.

2.30.4.5 Max-Req

This parameter is a timer in the authentication state machine for IEEE 802.1x.

Telnet path: /Setup/IEEE802.1x /Ports

Possible values:

■ Max. 10 characters

Default: 3



Changes to these parameters require expert knowledge of the IEEE 802.1x standard. Only make changes here if your system configuration absolutely requires them.

2.30.4.6 Tx period

This parameter is a timer in the authentication state machine for IEEE 802.1x.

Telnet path: /Setup/IEEE802.1x /Ports

Possible values:

■ Max. 10 characters

Default: 30



Changes to these parameters require expert knowledge of the IEEE 802.1x standard. Only make changes here if your system configuration absolutely requires them.

2.30.4.7 Supp-Timeout

This parameter is a timer in the authentication state machine for IEEE 802.1x.

Telnet path: /Setup/IEEE802.1x /Ports

Possible values:

■ Max. 10 characters

Default: 30



Changes to these parameters require expert knowledge of the IEEE 802.1x standard. Only make changes here if your system configuration absolutely requires them.

2.30.4.8 Server-Timeout

This parameter is a timer in the authentication state machine for IEEE 802.1x.

Telnet path: /Setup/IEEE802.1x /Ports

Possible values:

■ Max. 10 characters

Default: 30



Changes to these parameters require expert knowledge of the IEEE 802.1x standard. Only make changes here if your system configuration absolutely requires them.

2.30.4.9 Quiet period

This parameter is a timer in the authentication state machine for IEEE 802.1x.

Telnet path: /Setup/IEEE802.1x /Ports

Possible values:

■ Max. 10 characters

Default: 60



Changes to these parameters require expert knowledge of the IEEE 802.1x standard. Only make changes here if your system configuration absolutely requires them.

2.31 PPPoE

This menu contains the PPPoE settings.

Telnet path: /Setup

2.31.1 Operating

This switch enables and disables the PPPoE server.

Telnet path: /Setup/PPPoE-Server

Possible values:

■ Yes

■ No

2.31.3 Service

The name of the service offered is entered under 'Service'. This enables a PPPoE client to select a certain PPPoE server that is entered for the client.

Telnet path: /Setup/PPPoE-Server

Possible values:

■ Max. 32 characters

Default: Blank

2.31.4 Session-Limit

The 'Session limit' specifies how often a client can be logged on simultaneously with the same MAC address. Once the limit has been reached, the server no longer responds to the client queries that are received. Default value is '1', maximum value '99'. A Session limit of '0' stands for an unlimited number of sessions.

Telnet path: /Setup/PPPoE-Server

Possible values:

■ 0 to 99

Default: 1

Special values: 0 switches the session limit off.

2.31.2 Name list

In the list of peers/ remote sites, define those clients that are permitted access by the PPPoE server and define further properties and rights in the PPP list or the firewall.

Telnet path: /Setup/PPPoE-Server

2.31.2.1 Peer

Here you can define a remote-station name for each client. The remote-site name must be used by the client as the PPP user name.

Telnet path: /Setup/PPPoE-Server/Name-List

Possible values:

- Select from the list of defined peers.

Default: Blank

2.31.2.2 Short-hold time

Define the short-hold time for the PPPoE connection here.

Telnet path: /Setup/PPPoE-Server/Name-List

Possible values:

- Max. 10 characters

Default: 0

2.31.2.3 MAC address

If a MAC address is entered, then the PPP negotiation is terminated if the client logs on from a different MAC address.

Telnet path: /Setup/PPPoE-Server/Name-List

Possible values:

- Max. 12 characters

Default: 000000000000

2.31.5 Ports

Here you can specify for individual ports whether the PPPoE server is active.

Telnet path: /Setup/PPPoE-Server

2.31.5.2 Port

Port for which the PPPoE server is to be activated/deactivated.

Telnet path: /Setup/PPPoE-Server/Ports

Possible values:

- Selects a port from the list of those available in the device.

2.31.5.3 Enable PPPoE

Activates or deactivates the PPPoE server for the selected port.

Telnet path: /Setup/PPPoE-Server/Ports

Possible values:

- Yes

■ No

Default: Yes

2.32 VLAN

There are two important tasks when configuring the VLAN capabilities of the devices:

- Defining virtual LANs and giving each one a name, a VLAN ID, and allocating the interfaces
- For each interface, define how data packets with or without VLAN tags are to be handled

Telnet path: /Setup

2.32.4 Operating

You should only activate the VLAN module if you are familiar with the effects this can have.

Telnet path: /Setup/VLAN**Possible values:**

■ Yes

□

■ No

□

Default: No

Faulty VLAN settings may cause access to the device's configuration to be blocked.

2.32.5 Tag value

When transmitting VLAN tagged networks via provider networks that use VLAN themselves, providers sometimes use special VLAN tagging IDs. In order for VLAN transmission to allow for this, the Ethernet2 type of the VLAN tag can be set as a 16-bit hexadecimal value as 'tag value'. The default is '8100' (802.1p/q VLAN tagging) other typical values for VLAN tagging could be '9100' or '9901'.

Telnet path: /Setup/VLAN**Possible values:**

■ Max. 4 characters

Default: 8100

2.32.1 Networks

The network list contains the name of each VLAN, the VLAN ID and the ports. Simply click on an entry to edit it.

Telnet path: /Setup/VLAN

2.32.1.1 Name

The name of the VLAN only serves as a description for the configuration. This name is not used anywhere else.

Telnet path: /Setup/VLAN/Networks

2.32.1.2 VLAN-ID

This number uniquely identifies the VLAN.

Telnet path: /Setup/VLAN/Networks

Possible values:

- 0 to 4096

Default: 0

2.32.1.4 Ports

Enter here the device interfaces that belong to the VLAN. For a device with a LAN interface and a WLAN port, ports that to be entered could include "LAN-1" and "WLAN-1". Port ranges are defined by entering tilde between the individual ports: "P2P-1~P2P-4".

Telnet path: /Setup/VLAN/Networks**Possible values:**

- Max. 251 characters

Default: Blank

The first SSID of the first wireless LAN module is WLAN-1, and further SSIDs are WLAN-1-2 to WLAN-1-8. If the device has two WLAN modules, the SSIDs are called WLAN-2 and WLAN-2-2 to WLAN-2-8.

2.32.2 Port table

The port table is used to configure each of the device's ports that are used in the VLAN. The table has an entry for each of the device's ports.

Telnet path: /Setup/VLAN

2.32.2.1 Port

The name of the port; this cannot be edited.

Telnet path: /Setup/VLAN/Port-Table

2.32.2.4 Allow all VLANs

This option defines whether tagged data packets with any VLAN ID should be accepted, even if the port is not a "member" of this VLAN.

Telnet path: /Setup/VLAN/Port-Table**Possible values:**

- Yes
- No

Default: Yes

2.32.2.5 Port VLAN ID

This port ID has two functions:

- Untagged packets received at this port in 'Mixed' or 'Ingress-mixed' mode are assigned to this VLAN, as are all ingress packets received in 'Never' mode.
- In the 'Mixed' mode, this value determines whether outgoing packets receive a VLAN tag or not: Packets assigned to the VLAN defined for this port receive no VLAN tag; all others are given a VLAN tag.

Telnet path: /Setup/VLAN/Port-Table**Possible values:**

- Max. 4 characters

Default: 1

2.32.2.6 Tagging mode

Controls the processing and assignment of VLAN tags at this port.

Telnet path: /Setup/VLAN/Port-Table

Possible values:

- **Never:** Outbound packets are not given a VLAN tag at this port. Incoming packets are treated as though they have no VLAN tag. If incoming packets have a VLAN tag, it is ignored and treated as though it were part of the packet's payload. Incoming packets are always assigned to the VLAN defined for this port.
- **Always:** Outgoing packets at this port are always assigned with a VLAN tag, irrespective of whether they belong to the VLAN defined for this port or not. Incoming packets must have a VLAN tag, otherwise they will be dropped.
- **Mixed:** Allows mixed operation of packets with and without VLAN tags at the port. Packets without a VLAN tag are assigned to the VLAN defined for this port. Outgoing packets are given a VLAN tag unless they belong to the VLAN defined for this port.
- **Ingress mixed:** Arriving (ingress) packets may or may not have a VLAN tag; outbound (egress) packets are never given a VLAN tag.

Default: Ingress mixed

2.33 Voice Call Manager

This menu contains general settings for the Voice Call Manager.

Telnet path: /Setup

2.33.1 Operating

Switches the Voice Call Manager on / off

Telnet path: /Setup/Voice-Call-Manager

Possible values:

- Yes
- No

Default: No

2.33.2 General

This menu contains general settings for the Voice Call Manager.

Telnet path: /Setup/Voice-Call-Manager

2.33.2.10 Analog gateway codecs

Use the codec filter to restrict the codecs that are permitted for analog terminal equipment and to permit only certain codecs.

Telnet path: /Setup/Voice-Call-Manager/General

Possible values:

- Hexadecimal value to display the permitted codecs.

Default: All available codecs

2.33.2.11 ClnPartyNumType

This sets the type of the calling number (CallingPartyNumber) for outgoing numbers on an ISDN interface. This is necessary for PBXs and exchanges in some countries as these require a specific type.

Telnet path: /Setup/Voice-Call-Manager/General

Possible values:

- Subscriber
- Unknown
- National

Default: Subscriber(0)

2.33.2.13 Convert canonicals

This item activates the conversion of canonical VoIP names.

Telnet path: /Setup/Voice Call Manager/General/Convert-Canonicals

Possible values:

- Yes
- No

Default: Yes

2.33.2.9 Country

The country setting determines the inband tones generated in the LANCOM device

Telnet path: /Setup/Voice-Call-Manager/General

Possible values:

- Unknown
- Austria
- Belgium
- Switzerland
- Germany
- France
- Italy
- The Netherlands
- Spain
- Great Britain

Default: Unknown

2.33.2.1 Domain

Name of the domain in which the connected telephones and the LANCOM VoIP router are operated.

Terminal devices working in the same domain register as local subscribers at the LANCOM VoIP router and make use of the SIP proxy.

Terminal devices working with the other domain of an active SIP PBX line register themselves as subscribers at an upstream PBX.

Telnet path: /Setup/Voice-Call-Manager/General

Possible values:

- Max. 63 characters

Default: Internal

2.33.2.4 Echo_Canceler

Activates the echo canceling of remote echoes. With an echo that is too strong, subscribers can hear their own voices after a short delay. Activating this option reduces the echo at the SIP gateway.

Telnet path: /Setup/Voice-Call-Manager/General

Possible values:

- On
- Off

Default: On

2.33.2.6 Incoming packet reduction

Similar to the outgoing data packets, you configure how non-VoIP data packets are handled when bandwidth is reserved for SIP data.

Telnet path: /Setup/Voice-Call-Manager/General

Possible values:

- PMTU reduction: The subscribers of the data connection are informed that they should only send data packets up to a certain length (Path Maximum Transmission Unit, PMTU).
- No change: The length of the data packets is not changed by the VoIP operation.

Default: No change

2.33.2.8 ISDN gateway codecs

During connection establishment, the ISDN terminal devices negotiate which codecs are to be used to compress the voice data. Use the codec filter to restrict the codecs that are permitted and to permit only certain codecs.

Telnet path: /Setup/Voice-Call-Manager/General

Possible values:

- Hexadecimal value to display the permitted codecs.

Default: All available codecs

2.33.2.3 Local authentication

The SIP proxy usually accepts a registration from all SIP users who register themselves with a valid domain. If local authentication is forced, only those subscribers who are saved in one of the user tables with relevant access information can register with the SIP proxy.

Telnet path: /Setup/Voice-Call-Manager/General

Possible values:

- No
- Yes

Default: No/Off



Automatic registration without entering a password is restricted to the SIP users in the LAN. SIP users from the WAN and ISDN users must always be authenticated by a user entry with password.

2.33.2.5 Outgoing packet reduction

For all SIP calls, sufficient bandwidth through the firewall is reserved as required by the audio codec being used (provided sufficient bandwidth is available). Here you can set how remaining data packets should be handled that are not part of SIP data streams in order to manage the firewall.

Telnet path: /Setup/Voice-Call-Manager/General

Possible values:

- PMTU: The subscribers of the data connection are informed that they should only send data packets up to a certain length (Path Maximum Transmission Unit, PMTU).
- Fragmentation: The LANCOM VoIP router reduces the data packets by fragmenting them to the required length.
- NONE: The length of the data packets is not changed by the VoIP operation.
- PMTU + Fragmentation

Default: NONE/PMTU reduction**2.33.2.2 Overlap timeout**

When dialing from an ISDN telephone, this time period is waited until the called number is considered to be complete and then sent to the call router.

Telnet path: /Setup/Voice-Call-Manager/General**Possible values:**

- 0 to 99

Default: 6

Special values: 0: With a dial delay of '0', a '#' has to be entered at the end of the called number. Entering the '#' character after the called number manually reduces the dial delay.

2.33.2.7 Reduced packet size

This parameter specifies the packet size that should be used for PMTU adjustment or fragmentation while the SIP data have priority.

Telnet path: /Setup/Voice-Call-Manager/General**Possible values:**

- 0 to 9999

Default: 576**2.33.2.12 Register time**

This value specifies the re-registration time that is signaled to a SIP user locally

This function allows the VoIP client to be registered at shorter intervals, so as to detect more quickly when a VoIP client has been switched off, for example.

Telnet path: /Setup/Voice-Call-Manager/General**Possible values:**

- 60 to 3600

Default: 120**2.33.2.16 RTP-DSCP**

This defines which DiffServ CodePoints (DSCP) the RTP packets (voice data stream) are to be marked with.

Telnet path: /Setup/Voice-Call-Manager/General**Possible values:**

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



With DSCP set to BE or CS-0 the packets are sent unmarked. Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

2.33.2.15 SIP-DSCP

This defines which DiffServ CodePoints (DSCP) the SIP packets (for call signaling) are to be marked with.

Telnet path: /Setup/Voice-Call-Manager/General

Possible values:

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



The option CS-1 is actually outdated now, but it is set as the default value to ensure backwards compatibility. Common values for modern VoIP installations are CS-3, AF-31 or AF-41. We recommend using CS-3, one of the most widespread settings on the market.

2.33.2.14 Symmetric RTP

This parameter switches off the strict checking of the RTP sender. In general, two-way communications take place between the two RTP socket addresses (IP: port), i.e. the media data sources (outgoing) are at the same time also media data sinks (incoming). The data flow is symmetric.

However, there are media servers which are implemented differently in that the RTP source and the RTP target do not have the same socket address. In these cases deactivate the "Symmetrical RTP" option.

Telnet path: /Setup/Voice-Call-Manager/General/Symmetric-RTP

Possible values:

■ Yes

■ No

Default: Yes

2.33.3 Users

This menu contains user settings for the Voice Call Manager.

Telnet path: /Setup/Voice-Call-Manager

2.33.3.1 SIP-User

This menu contains SIP user settings for the Voice Call Manager.

Telnet path: /Setup/Voice-Call-Manager/Users

2.33.3.1.3 Extern Cln Prefix

If an incoming external call is directed to a SIP user, this prefix is added to the calling party ID, if available.

Telnet path: /Setup/Voice-Call-Manager/User/SIP-User

Possible values:

■ Max. 15 numbers or *

Default: Blank

2.33.3.1.2 Intern Cln Prefix

If an incoming internal call is directed to a SIP user, this prefix is added to the calling party ID, if available.

Telnet path: /Setup/Voice-Call-Manager/User/SIP-User

Possible values:

- Max. 15 numbers or *

Default: *

A call is regarded as external if it comes from a "line". If this line is a SIP PBX line, then the call is only external if the incoming calling party ID is preceded by a "0". All other calls are regarded as internal.

2.33.3.1 Users

Depending on the model, different numbers of SIP users can be created. You cannot create more than the maximum number of users permitted; similarly, duplicate names or called numbers are not permitted.

Telnet path: /Setup/Voice- Call- Manager/User/SIP- User

The domain that is used by the SIP subscriber is usually configured in the terminal equipment itself.

2.33.3.1.1 Number/Name

Telephone number of the SIP telephone or name of the user (SIP URI).

Telnet path: /Setup/Voice- Call- Manager/User/SIP- User/Users**Possible values:**

- Max. 20 characters

Default: Blank**2.33.3.1.1.2 Authentication name**

Name for authentication at the SIP proxy, and also to any upstream SIP PBX when the user's domain is the same as the domain of a SIP PBX line. This name is required if registration is mandatory (e.g. when logging in to an upstream SIP PBX or when "Force local authentication" is set for local users).

Telnet path: /Setup/Voice- Call- Manager/User/SIP- User/Users**Possible values:**

- Max. 63 characters

Default: Blank

Special values: Blank: If nothing is entered here, the authentication is attempted using the SIP name (internal call number).

2.33.3.1.1.3 Secret

Password for authentication to the SIP proxy, and also to any upstream SIP PBX, when the user's domain is the same as the domain of a SIP PBX line. It is possible for users to log in to the local SIP proxy without authentication ("Force local authentication" is deactivated for SIP users) and where applicable to an upstream SIP PBX using a shared password ("Standard password" on the SIP PBX line).

Telnet path: /Setup/Voice- Call- Manager/User/SIP- User/Users**Possible values:**

- Max. 32 characters

Default: Blank**2.33.3.1.1.4 Active**

Activates or deactivates the entry.

Telnet path: /Setup/Voice- Call- Manager/User/SIP- User/Users**Possible values:**

- Yes
- No

Default: On**2.33.3.1.1.5 Comment**

Comment on this entry.

Telnet path: /Setup/Voice- Call- Manager/User/SIP- User/Users

Possible values:

- Max. 63 characters

Default: Blank

2.33.3.1.1.6 Device type

Type of device connected.

The type determines whether an analog connection should be converted into SIP T.38, where applicable. Selecting "Fax" or "Telephone/Fax" activates fax signal recognition that could result in an impairment of the connection quality for telephones. Therefore please select the corresponding type of device connected in order to ensure optimum quality.

Telnet path: /Setup/Voice- Call- Manager/User/SIP- User/Users

Possible values:

- Phone
- Fax
- Auto

Default: Phone

2.33.3.1.1.7 CLIR

Switches the transmission of the calling-line identifier on/off.

Telnet path: /Setup/Voice- Call- Manager/User/SIP- User/Users

Possible values:

- Yes: Transmission of the calling-line identifier is suppressed whatever the setting in the user's device.
- No: Transmission of the calling-line identifier is not suppressed in the device; the settings in the user's terminal device control the transmission of the calling-line identifier.

Default: No/Off

2.33.3.2 ISDN user

This menu contains ISDN user settings for the Voice Call Manager.

Telnet path: /Setup/Voice- Call- Manager/Users

2.33.3.2.4 Extern Cln Prefix

If an incoming external call is directed to an ISDN user, this prefix is added to the calling party ID, if available. If a line prefix is defined, this is placed in front of the whole of the called number.

Telnet path: /Setup/Voice- Call- Manager/Users/ISDN- User

Possible values:

- Max. 15 numbers or *

Default: Blank

2.33.3.2.1 Interfaces

Here you select the interface that the ISDN user is connected to.

Telnet path: /Setup/Voice- Call- Manager/Users/ISDN- User

2.33.3.2.1.3 Active

Activates or deactivates the entry.

Telnet path: /Setup/Voice- Call- Manager/User/ISDN- User/Interfaces

Possible values:

- Yes
- No

Default: Yes/On

2.33.3.2.1.2 Interface

Interface to which the ISDN subscribers are connected.

Telnet path: /Setup/Voice- Call- Manager/User/ISDN- User/Interfaces

Possible values:

- Selection from ISDN interfaces available e.g. S0-1 and S0-2

Default: Varies between models.

2.33.3.2.1.1 Name

Name of interface

Telnet path: /Setup/Voice- Call- Manager/User/ISDN- User/Interfaces

Possible values:

- ISDN

Default: ISDN

2.33.3.2.1.4 Comment

Comment on this entry.

Telnet path: /Setup/Voice- Call- Manager/User/ISDN- User/Interfaces

Possible values:

- Max. 63 characters

Default: Blank

2.33.3.2.3 Intern Cln Prefix

If an incoming internal call is directed to an ISDN user, this prefix is added to the calling party ID, if available. If a line prefix is defined, this is placed in front of the whole of the called number.

Telnet path: /Setup/Voice- Call- Manager/Users/ISDN- User

Possible values:

- Max. 15 numbers or *

Default: *

2.33.3.2.5 Internal dial tone

The dial tone determines the sound a user hears after lifting the receiver. The "internal dial tone" is the same as the tone that a user hears at a PBX without spontaneous outside-line access (three short tones followed by a pause). The "external dial tone" is thus the same as the tone that indicates an external line when the receiver is lifted (constant tone without any interruptions). If necessary, adapt the dial tone to the use for spontaneous outside-line access to simulate the behavior of an external connection.

Telnet path: /Setup/Voice- Call- Manager/Users/ISDN- User

Possible values:

- Yes
- No

Default: No, the external dial tone will be used.

2.33.3.2 Users

Here you can define all local ISDN users (terminal devices). You can also specify the authentication data for SIP registration.

Telnet path: /Setup/Voice- Call- Manager/Users/ISDN- User

2.33.3.2.2.1 Number/Name

Internal number of the ISDN telephone or name of the user (SIP URI).

Telnet path: /Setup/Voice- Call- Manager/User/ISDN- User/Users

Possible values:

- Max. 20 characters

Default: Blank



By using the # character as a placeholder, entire groups of numbers (e.g. when using extension numbers at a point-to-point connection) can be addressed via a single entry. With the number '#' and the DDI '#', for example, extension numbers can be converted into internal telephone numbers wit-

hout making any changes. With the call number '3#' and the DDI '#', for example, an incoming call for extension '55' is forwarded to the internal number '355', and for outgoing calls from the internal number '377', the extension number '77' will be used.



User entries that use # characters to map user groups cannot be used for registration at an upstream PBX. This registration always demands a specific entry for the individual ISDN user.

2.33.3.2.2.10 Comment

Comment on this entry.

Telnet path: /Setup/Voice- Call- Manager/User/ISDN- User/Users

Possible values:

- Max. 63 characters

Default: Blank

2.33.3.2.2.11 Device type

Type of device connected.

The type determines whether an analog connection should be converted into SIP T.38, where applicable. Selecting "Fax" or "Telephone/Fax" activates fax signal recognition that could result in an impairment of the connection quality for telephones. Therefore please select the corresponding type of device connected in order to ensure optimum quality.

Telnet path: /Setup/Voice- Call- Manager/User/ISDN- User/Users

Possible values:

- Phone
- Fax
- Auto

Default: Phone

2.33.3.2.2.12 CLIR

Switches the transmission of the calling-line identifier on/off.

Telnet path: /Setup/Voice- Call- Manager/User/ISDN- User/Users

Possible values:

- Yes: Transmission of the calling-line identifier is suppressed whatever the setting in the user's device.
- No: Transmission of the calling-line identifier is not suppressed in the device; the settings in the user's terminal device control the transmission of the calling-line identifier.

Default: No/Off

2.33.3.2.2.2 Interface

ISDN interface that should be used to establish the connection.

Telnet path: /Setup/Voice- Call- Manager/User/ISDN- User/Users

Possible values:

- None, one or several available S0 buses.

Default: Depends on type of device.

2.33.3.2.2.3 MSN/DDI

Internal MSN that is used for this user on the internal ISDN bus.

MSN: Number of the telephone connection if it is a point-to-multipoint connection.

DDI (Direct Dialing in): Telephone extension number if the connection is configured as a point-to-point line.

Telnet path: /Setup/Voice- Call- Manager/User/ISDN- User/Users

Possible values:

- Max. 19 numbers and # characters

Default: Blank



By using the # character as a placeholder, entire groups of call numbers, e.g. when using extension numbers, can be addressed via a single entry.



User entries that use # characters to map user groups cannot be used for registration at an upstream PBX. This registration always demands a specific entry for the individual ISDN user.

2.33.3.2.2.4 Display name

Name for display on the telephone being called.

Telnet path: /Setup/Voice- Call- Manager/User/ISDN- User/Users

Possible values:

- Max. 32 alphanumerical characters

Default: Blank

2.33.3.2.2.5 Authentication name

Name for authentication at any upstream SIP PBX when the user's domain is the same as the domain of a SIP PBX line.

Telnet path: /Setup/Voice- Call- Manager/User/ISDN- User/Users

Possible values:

- Max. 63 characters

Default: Blank



Only required when the user registers at an upstream SIP PBX.

2.33.3.2.2.6 Secret

Password for authentication as a SIP user at any upstream SIP PBX when the user's domain is the same as the domain of a SIP PBX line. It is possible for ISDN users to log in to an upstream SIP PBX using a shared password ("Standard password" on the SIP PBX line).

Telnet path: /Setup/Voice- Call- Manager/User/ISDN- User/Users

Possible values:

- Max. 32 characters

Default: Blank

2.33.3.2.2.7 Domain

Domain of an upstream SIP PBX when the ISDN user is to be logged in as a SIP user. The domain must be configured for a SIP PBX line in order for upstream login to be performed.

Telnet path: /Setup/Voice- Call- Manager/User/ISDN- User/Users

Possible values:

- Max. 63 characters

Default: Blank



Only required when the user registers at an upstream SIP PBX.

2.33.3.2.2.8 DialComplete

En-block dial detection allows the dialed number to be marked as complete (e.g. for speed dialing or repeat dialing) so that the call is established more quickly. Suffix dialing is not possible.

Telnet path: /Setup/Voice- Call- Manager/User/ISDN- User/Users

Possible values:

- Auto: Block dialing is detected automatically (for example, with speed dial or repeat dialing), so that the call is established more quickly. Suffix dialing is not possible.
- Manual: No block dialing; the number can be marked as complete with '#' and the call can be initiated.

Default: Auto



The number can be manually marked as complete with '#' and the call can be initiated.

2.33.3.2.9 Active

Activates or deactivates the entry.

Telnet path: /Setup/Voice-Call-Manager/User/ISDN-User/Users

Possible values:

- No
- Yes

Default: Yes/On

2.33.3.3 Analog user

This menu contains analog user settings for the Voice Call Manager.

Telnet path: /Setup/Voice-Call-Manager/Users

2.33.3.3.4 Extern Cln Prefix

If an incoming external call is directed to an analog user, this prefix is added to the calling party ID, if available. If a line prefix is defined, this is placed in front of the whole of the called number.

Telnet path: /Setup/Voice-Call-Manager/Users/Analog-User

Possible values:

- Max. 15 numbers or *

Default: Blank

2.33.3.3.1 Interfaces

Here you select the interface that the analog user is connected to.

Telnet path: /Setup/Voice-Call-Manager/Users/Analog-User

2.33.3.3.1.1 Name

Name for the interface

Telnet path: /Setup/Voice-Call-Manager/Users/Analog-User/Interfaces

Possible values:

- ANALOG

Default: ANALOG

2.33.3.3.1.2 Interface

An internal interface to which the analog subscribers are connected.

Telnet path: /Setup/Voice-Call-Manager/Users/Analog-User/Interfaces

Possible values:

- None
- Analog-1
- Analog-2

Default: Analog-1

2.33.3.3.1.3 Active

Activates or deactivates the entry.

Telnet path: /Setup/Voice-Call-Manager/Users/Analog-User/Interfaces

Possible values:

- Yes
- No

Default: Yes

2.33.3.3.1.4 Comment

Comment on this entry

Telnet path: /Setup/Voice- Call- Manager/Users/Analog- User/Interfaces

Possible values:

■ Max. 63 characters

Default: Blank

2.33.3.3.3 Intern Cln Prefix

This prefix is added to the calling party ID, if available, for an incoming, internal call if the call is directed to an analog user. If a line prefix is defined, this is placed in front of the whole of the called number.

Telnet path: /Setup/Voice- Call- Manager/Users/Analog- User

Possible values:

■ Max. 15 numbers or *

Default: *

2.33.3.3.5 Internal dial tone

The dial tone determines the sound a user hears after lifting the receiver. The "internal dial tone" is the same as the tone that a user hears at a PBX without spontaneous outside-line access (three short tones followed by a pause). The "external dial tone" is thus the same as the tone that indicates an external line when the receiver is lifted (constant tone without any interruptions). If necessary, adapt the dial tone to the use for spontaneous outside-line access to simulate the behavior of an external connection.

Telnet path: /Setup/Voice- Call- Manager/Users/Analog- User

Possible values:

■ Yes

■ No

Default: No, the external dial tone will be used.

2.33.3.3 Users

Here you can define all local analog users (terminal devices). You can also specify the authentication data for SIP registration.

Telnet path: /Setup/Voice- Call- Manager/Users/Analog- User

2.33.3.3.2.1 Number/Name

Internal number of the analog telephone or name of the user (SIP URI).

Telnet path: /Setup/Voice- Call- Manager/Users/Analog- User/Users

Possible values:

■ Max. 20 characters

Default: Blank

2.33.3.3.2.10 Active

Activates or deactivates the entry.

Telnet path: /Setup/Voice- Call- Manager/Users/Analog- User/Users

Possible values:

■ On

■ Off

Default: On

2.33.3.3.2.11 Comment

Comment on this entry.

Telnet path: /Setup/Voice- Call- Manager/Users/Analog- User/Users

Possible values:

■ Max. 63 characters

Default: Blank

2.33.3.3.2.12 Device type

Type of device connected.

The type determines whether an analog connection should be converted into SIP T.38, where applicable. Selecting "Fax" or "Telephone/Fax" activates fax signal recognition that could result in an impairment of the connection quality for telephones. Therefore please select the corresponding type of device connected in order to ensure optimum quality.

Telnet path: /Setup/Voice- Call- Manager/Users/Analog- User/Users

Possible values:

- Phone
- Fax
- Auto

Default: Phone

2.33.3.3.2.2 Interface

Analog interface that should be used to establish the connection.

Telnet path: /Setup/Voice- Call- Manager/Users/Analog- User/Users

Possible values:

- Analog-1
- Analog-2
- None

Default: Analog-1

2.33.3.3.2.3 Display name

Name for display on the telephone being called.

Telnet path: /Setup/Voice- Call- Manager/Users/Analog- User/Users

Possible values:

- Max. 63 characters

Default: Blank

2.33.3.3.2.4 Authentication name

Name for authentication at any upstream SIP PBX when the user's domain is the same as the domain of a SIP PBX line.

Telnet path: /Setup/Voice- Call- Manager/Users/Analog- User/Users

Possible values:

- Max. 63 characters

Default: Blank

2.33.3.3.2.5 Secret

Password for authentication as a SIP user to any upstream SIP PBX when the analog user's domain is the same as the domain of a SIP PBX line. It is possible for ISDN users to log in to an upstream SIP PBX using a shared password ("Standard password" on the SIP PBX line).

Telnet path: /Setup/Voice- Call- Manager/Users/Analog- User/Users

Possible values:

- Max. 32 characters

Default: Blank

2.33.3.3.2.6 Domain

Domain of an upstream SIP PBX when the analog user is to be logged in as a SIP user. The domain must be configured for a SIP PBX line in order for upstream login to be performed.

Telnet path: /Setup/Voice- Call- Manager/Users/Analog- User/Users

Possible values:

- Max. 63 characters

Default: Blank

2.33.3.3.2.8 CLIR

Switches the transmission of the calling-line identifier on/off.

Telnet path: /Setup/Voice- Call- Manager/Users/Analog-User/Users

Possible values:

- Yes: Transmission of the calling-line identifier is suppressed whatever the setting in the user's device.
- No: Transmission of the calling-line identifier is not suppressed in the device; the settings in the user's terminal device control the transmission of the calling-line identifier.

Default: No

2.33.3.3.2.9 Metering

The metering pulse is used in analog telephone networks to inform callers of the costs of their calls. With appropriate terminal equipment (e.g. telephone with charge display), the metering pulse is filtered out from the overall signal and this information is converted to display the call charge.

Telnet path: /Setup/Voice- Call- Manager/Users/Analog-User/Users

Possible values:

- Yes
- No

Default: No



This option allows the metering pulse to be passed on to the analog user/equipment. It is possible for charge information from the ISDN telephone network to be transferred to an ISDN line and converted into an analog metering pulse.

2.33.3.4 Extensions

Here you can define extended user settings such as call waiting or call transfer.

Telnet path: /Setup/Voice- Call- Manager/Users

2.33.3.4.1 Name

The user settings apply to this telephone number or SIP-ID.

Telnet path: /Setup/Voice- Call- Manager/Users/Extensions

Possible values:

- Max. 64 characters

Default: Blank



Call forwarding can be set up for all local users (SIP, ISDN or analog).

2.33.3.4.10 Active

Activates or deactivates the entry.

Telnet path: /Setup/Voice- Call- Manager/Users/Extensions

Possible values:

- On
- Off

Default: On

2.33.3.4.11 Busy-on-Busy

Prevents a second call from being connected to a terminal device, irrespective of whether CW (call-waiting indication) is active on the device or not; i.e. there is no "call waiting" signal. The second caller hears an engaged tone. This also applies where an internal telephone number supports multiple logins and just one of the possible terminal devices is already in use.

Telnet path: /Setup/Voice- Call- Manager/Users/Extensions

Possible values:

- Yes
- No

Default: No

2.33.3.4.12 CallForward-Set-CallingLine-Id

Use this entry to set which phone number will be signaled when a call is forwarded (CF) - for example from CDIV - alternatively, you can enter your own phone number as a fixed setting.

Telnet path: /Setup/Voice- Call- Manager/Users/Extensions

Possible values:

- Extension-ID:
- Calling-ID: Signals the incoming phone number. When the call is forwarded to a mobile phone, a subscriber will be able to identify the caller's original phone number.
- Custom-ID: Signals the phone number entered under /Setup/Voice- Call- Manager/Users/Extensions/Custom-ID.

Default: Extension-ID:

2.33.3.4.13 Custom ID

Use this entry to set the phone number that will be used for signaling with call forwarding.

Telnet path: /Setup/Voice- Call- Manager/Users/Extensions

Possible values:

- Maximum 64 characters

Default: Blank

This phone number will only be used if the parameter /Setup/Voice- Call- Manager/Users/Extensions/CF-Set-Cln-Id is set to "Custom-ID"

2.33.3.4.2 User modifiable

This activates or deactivates the option for users to configure their settings via the telephone.

Telnet path: /Setup/Voice- Call- Manager/Users/Extensions

Possible values:

- Yes
- No

Default: Yes

2.33.3.4.3 CFU active

Activates or deactivates the immediate forwarding of calls (CFU).

Telnet path: /Setup/Voice- Call- Manager/Users/Extensions

Possible values:

- Yes
- No

Default: No

2.33.3.4.4 CFU target

Target for immediate unconditional call forwarding

Telnet path: /Setup/Voice- Call- Manager/Users/Extensions

Possible values:

- Maximum 64 characters to designate local users, hunt groups or external phone numbers.

Default: Blank

2.33.3.4.5 CFNR active

Activates or deactivates the delayed forwarding of call (after waiting for no reply).

Telnet path: /Setup/Voice- Call- Manager/Users/Extensions

Possible values:

- Yes

- No

Default: No

2.33.3.4.6 CFNR target

Target for call forwarding no reply.

Telnet path: /Setup/Voice- Call- Manager/Users/Extensions

Possible values:

- Maximum 64 characters to designate local users, hunt groups or external phone numbers.

Default: Blank

2.33.3.4.7 CFNR timeout

Wait time for call forwarding on no reply. After this time period the call is forwarded to the target number if the subscriber does not pick up the phone.

Telnet path: /Setup/Voice- Call- Manager/Users/Extensions

Possible values:

- Max. 255 seconds

Default: 15 seconds

2.33.3.4.8 CFB active

Activates or deactivates call forwarding on busy.

Telnet path: /Setup/Voice- Call- Manager/Users/Extensions

Possible values:

- Yes

- No

Default: No

2.33.3.4.9 CFB target

Target for call forwarding on busy.

Telnet path: /Setup/Voice- Call- Manager/Users/Extensions

Possible values:

- Maximum 64 characters to designate local users, hunt groups or external phone numbers.

Default: Blank

2.33.4 Lines

This menu contains line settings for the Voice Call Manager.

Telnet path: /Setup/Voice- Call- Manager

2.33.4.1 SIP provider

This menu contains SIP provider settings for the Voice Call Manager.

Telnet path: /Setup/Voice- Call- Manager/Lines

2.33.4.1.1 Line

The device uses these lines to register with other SIP remote stations (usually SIP providers or remote gateways at SIP PBXs). The connection is made either over the Internet or a VPN tunnel. Up to 16 SIP lines can be entered.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP-Provider

2.33.4.1.1.1 Name

Name of the line; may not be identical to another line that is configured in the device.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP-Provider/Line

Possible values:

- Max. 16 characters

Default: Blank

2.33.4.1.1.10 Active

Activates or deactivates the entry.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP- Provider/Line

Possible values:

- On
- Off

Default: On

2.33.4.1.1.11 Comment

Comment on this entry

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP- Provider/Line

Possible values:

- Max. 64 characters

Default: Blank

2.33.4.1.1.12 Codecs

While the connection is being established, the terminal equipment concerned negotiate which codecs are to be used to compress the voice data. Use the codec filter to restrict the codecs that are permitted and to permit only certain codecs.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP- Provider/Line

Possible values:

- Along with the widely available codecs, some models also support the following codec for the SIP gateway function:
- G.722 - 64 kbps (high-quality codec for ISDN to SIP and vice versa only)
- G.729 - 8 kbps (codec with higher compression for lower bandwidths)
- These codecs are available to the devices LANCOM 1722 VoIP, LANCOM 1723 VoIP, LANCOM 1724 VoIP and LANCOM 1823 VoIP, and also for all models with the LANCOM Advanced VoIP Option.

Default: All



If no common the codecs can be agreed upon, no connection is made.

2.33.4.1.1.13 Codec order

This parameter influences the order in which the codecs are presented during connection establishment.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP- Provider

Possible values:

- Unchanged: Leaves the order of the codecs unchanged
- BestQuality: Changes the order of the codecs that are offered to achieve the best voice quality possible.
- LowestBandwidth: Changes the order of the codecs that are offered to achieve the lowest bandwidth possible.

Default: Unchanged

2.33.4.1.1.14 Routing tag

Routing tag for selecting a certain route in the routing table for connections to this SIP provider.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP- Provider/Line

Possible values:

- Max. 64 numbers

Default: 0

2.33.4.1.1.15 Display name

Name for display on the telephone being called.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP-Provider/Line

Possible values:

- Max. 64 characters

Default: Blank



Normally this value should not be set as incoming calls have a display name set by the SIP provider, and outgoing calls are set with the local client or call source (which may be overwritten by the user settings for display name, if applicable). This settings is often used to transmit additional information (such as the original calling number when calls are forwarded) that may be useful for the person called. In the case of single-line SIP accounts, some providers require an entry that is identical to the display name defined in the registration details, or the SIP ID (e.g. T-Online). This access data is used to register the line (single account, trunk, link, gateway), but not the individual local users with their individual registration details. If individual users (SIP, ISDN, analog) are to register with an upstream device using the data stored there or on the terminal device, then the line type "SIP PBX line" should be selected.

2.33.4.1.16 Registrar

The SIP registrar is the point at the SIP provider that accepts the login with the authentication data for this account.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP-Provider/Line

Possible values:

- Max. 64 characters

Default: Blank



This field can remain empty unless the SIP provider specifies otherwise. The registrar is then determined by sending DNS SRV requests to the configured SIP domain/realm (this is often not the case for SIP services in a corporate network/VPN, i.e. the value must be explicitly set).

2.33.4.1.17 Mode

This selection determines the operating mode of the SIP line.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP-Provider/Line

Possible values:

- Provider: Externally, the line behaves like a typical SIP account with a single public number. The number is registered with the service provider, the registration is refreshed at regular intervals (when (re-)registration has been activated for this SIP provider line). For outgoing calls, the calling-line number is replaced (masked) by the registered number. Incoming calls are sent to the configured internal target number. Only one connection can exist at a time.
- Trunk: Externally, the line acts like an extended SIP account with a main external telephone number and multiple extension numbers. The SIP ID is registered as the main external number with the service provider and the registration is refreshed at regular intervals (when (re-)registration has been activated for this SIP provider line). For outgoing calls, the switchboard number acts as a prefix placed in front of each calling number (sender; SIP: "From:"). For incoming calls, the prefix is removed from the target number (SIP: "To:"). The remaining digits are used as the internal extension number. In case of error (prefix not found, target equals prefix) the call is forwarded to the internal target number as configured. The maximum number of connections at any one time is limited only by the available bandwidth.
- Gateway: Externally the line behaves like a typical SIP account with a single public number, the SIP ID. The number (SIP ID) is registered with the service provider and the registration is refreshed at regular intervals (when (re-)registration has been activated for this SIP provider line). For outgoing calls, the calling-line number (sender) is replaced (masked) by the registered number (SIP ID in SIP: "From:") and sent in a separate field (SIP: "Contact:"). For incoming calls the dialed number (target) is not modified. The maximum number of connections at any one time is limited only by the available bandwidth.
- Link: Externally, the line behaves like a typical SIP account with a single public number (SIP ID). The number is registered with the service provider, the registration is refreshed at regular intervals (when (re-)registration has been activated for this SIP provider line). For outgoing calls, the calling-line number (sender; SIP: "From:") is not modified. For incoming calls, the dialed number (target; SIP: modified. The maximum number of connections at any one time is limited only by the available bandwidth.

Default: Provider



The "Service provider" can be a server in the Internet, an IP PBX, or a voice gateway. Please observe the notices about 'SIP mapping'..

2.33.4.1.1.18 Refer forwarding

Call switching (connect call) between two remote subscribers can be handled by the device itself (media proxy) or it can be passed on to the exchange at the provider if both subscribers can be reached on this SIP provider line (otherwise the media proxy in the LANCOM device assumes responsibility for switching the media streams, for example when connecting between two SIP providers).

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP-Provider/Line

Possible values:

- Yes: Switching is passed on to the provider.
- No: Switching is retained within the device.

Default: No



An overview of the main SIP providers supporting this function is available in the Support area of our Internet site.

2.33.4.1.1.19 Local port

This is the port used by the LANCOM proxy to communicate with the provider.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP-Provider/Line

Possible values:

- 1 to 65536

Default: 0

Special values: 0: Dynamic port selection; the port is automatically selected from the pool of available port numbers.



If line (re-)registration is deactivated, the local port has to be defined with a fixed value, and this also has to be entered at the provider end as the destination port (e.g. when using an unregistered trunk in the company VPN). This ensures that both ends can send SIP signaling.

2.33.4.1.1.2 Domain

SIP domain/realm of the upstream device. Provided the remote device supports DNS service records for SIP, this setting is sufficient to determine the proxy, outbound proxy, port and registrar automatically. This is generally the case for typical SIP provider services.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP-Provider/Line

Possible values:

- Max. 64 characters

Default: Blank

2.33.4.1.1.20 (Re-)registration

This activates the (repeated) registration of the SIP provider line. Registration can also be used for line monitoring.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP-Provider/Line

Possible values:

- Yes
- No

Default: Yes



To use (re-) registration, the line monitoring method must correspondingly be set to "Register" or "Automatic". Registration is repeated after the monitoring interval has expired. If the provider's SIP registrar suggests a different interval, the suggested value is used automatically.

2.33.4.1.1.21 Line-monitoring

Specifies the line monitoring method. Line monitoring checks if a SIP provider line is available. The Call Router can make use of the monitoring status to initiate a change to a backup line. The monitoring method sets the way in which the status is checked.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP-Provider/Line

Possible values:

- Auto: The method is set automatically.
- Disabled: No monitoring; the line is always reported as being available. This setting does not allow the actual line availability to be monitored.
- Register: Monitoring by means of register requests during the registration process. This setting also requires "(Re-)registration" to be activated for this line.
- Options: Monitoring via Options Requests. This involves regular polling of the remote station. Depending on the response the line is considered to be available or unavailable. This setting is well suited for e.g. lines without registration.

Default: Auto

2.33.4.1.1.22 Monitoring interval

The monitoring interval in seconds. This value affects the line monitoring with register request and also the option request. The monitoring interval must be set to at least 60 seconds. This defines the time period that passes before the monitoring method is used again. If (re-) registration is activated, the monitoring interval is also used as the time interval before the next registration.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP-Provider/Line

Possible values:

- Max. 5 numbers

Default: 60

Special values: Values less than 60 seconds are automatically set to 60 seconds.



If the remote station responds to an option request with a different suggested value for the monitoring interval, this is accepted and subsequently applied.

2.33.4.1.1.23 Trusted

Specifies the remote station on this line (provider) as "Trusted Area". In this trusted area, the caller ID is not concealed from the caller, even if this is requested by the settings on the line (CLIR) or in the device. In the event of a connection over a trusted line, the Caller ID is first transmitted in accordance with the selected privacy policy and is only removed in the final exchange before the remote subscriber. This means, for example, that Caller ID can be used for billing purposes within the trusted area. This function is interesting for providers using a VoIP router to extend their own managed networks all the way to the connection for the VoIP equipment.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP-Provider/Line

Possible values:

- Yes: Trusted
- No: Not trusted

Default: Yes



The function is not supported by all providers.

2.33.4.1.1.24 Privacy method

Specifies the method used for transmitting the caller ID in the separate SIP-header field.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP-Provider/Line

Possible values:

- None
- RFC3325: Using P-Preferred-Id/P-Asserted-Id
- IETF-Draft-Sip-Privacy-04: Using RPID (Remote Party ID)

Default: None

2.33.4.1.1.25 Remove FROM user type

Select this option to remove the "user=phone" information from the From field for outgoing calls over a provider line. Some VoIP proxies do not process this information according to the standard and reject the call.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP-Provider/Line/remove- FROM-usertype

Possible values:

- Yes
- No

Default: No

2.33.4.1.1.3 Port

TCP/UDP port that the SIP provider uses as the target port for SIP packets.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP-Provider/Line

Possible values:

- Any available TCP/IP port.

Default: 5060



This port has to be activated in the firewall for the connection to work.

2.33.4.1.1.4 User ID

Telephone number of the SIP account or name of the user (SIP URI).

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP-Provider/Line

Possible values:

- Max. 64 characters

Default: Blank



This access data is used to register the line (single account, trunk, link, gateway), but not the individual local users with their individual registration details. If individual users (SIP, ISDN, analog) are to register with an upstream device using the data stored there or on the terminal device, then the line type "SIP PBX line" should be selected.

2.33.4.1.1.5 Authentication name

Name for authentication to the upstream SIP device (provider/SIP PBX).

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP-Provider/Line

Possible values:

- Max. 64 characters

Default: Blank



This access data is used to register the line (single account, trunk, link, gateway), but not the individual local users with their individual registration details. If individual users (SIP, ISDN, analog) are to register with an upstream device using the data stored there or on the terminal device, then the line type "SIP PBX line" should be selected.

2.33.4.1.1.6 Secret

The password for authentication at the SIP registrar and SIP proxy at the provider. For lines without (re-)registration, the password may be omitted under certain circumstances.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP-Provider/Line

Possible values:

- Max. 64 characters

Default: Blank

2.33.4.1.1.7 Outbound proxy

The SIP provider's outbound proxy accepts all SIP signaling originating from the LANCOM device for the duration of the connection.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP- Provider/Line

Possible values:

■ Max. 64 characters

Default: Blank



This field can remain empty unless the SIP provider specifies otherwise. The outbound proxy is then determined by sending DNS SRV requests to the configured SIP domain/realm (this is often not the case for SIP services in a corporate network/VPN, i.e. the value must be explicitly set).

2.33.4.1.1.8 Cln- Prefix

The call prefix is a number placed in front of the caller number (CLI; SIP "From:") for all incoming calls. This generates unique telephone numbers for return calls.

For example; a number can be added, which the call router analyzes (and subsequently removes) to select the line to be used for the return call.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP- Provider/Line

Possible values:

■ Max. 9 numbers

Default: Blank

2.33.4.1.1.9 Name

The effect of this field depends upon the mode set for the line:

If the line is set to "Single account" mode, all incoming calls on this line with this number as the target (SIP: "To") are transferred to the call router.

If the mode is set to "Trunk", the target number is determined by removing the trunk's switchboard number. If an error occurs, the call will be supplemented with the number entered in this field (SIP: "To") are transferred to the call router.

If mode is set to "Gateway" or "Link" the value entered in this field has no effect.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP- Provider/Line

Possible values:

■ Max. 64 characters

Default: Blank

2.33.4.1.2 Mapping

The entries made under SIP mapping establish a series of rules for number translation to SIP lines in the trunk or gateway mode. Up to 40 mapping rules can be entered.

A SIP line in trunk mode is used for mediating between internal numbers and the range of telephone numbers offered by a SIP account.

For incoming calls, the destination number (called party ID) is modified. The internal number is used if the called party ID matches with the external telephone number.

For outgoing calls, the calling party ID is modified. The external number is used if the calling party ID matches with the internal telephone number.

Telnet path: /Setup/Voice- Call- Manager/Lines/SIP- Provider

2.33.4.1.2.1 SIP provider

Name of the line which is the target of the call number mapping.

Telnet path: /Setup/Voice Call Manager/Lines/SIP- provider/Mapping

Possible values:

■ All defined SIP lines.

Default: Blank

2.33.4.1.2.2 Ext- number/name

Call number within the range of those used by the SIP trunk account or upstream SIP PBX.

Telnet path: /Setup/Voice Call Manager/Lines/SIP- provider/Mapping

Possible values:

- Max. 64 characters

Default: Blank

2.33.4.1.2.3 Number/Name

Telephone number in the range of the LANCOM VoIP router.

Telnet path: /Setup/Voice Call Manager/Lines/SIP-provider/Mapping

Possible values:

- Max. 64 characters

Default: Blank

2.33.4.1.2.4 Length

The value defines the number of digits required for a called number to be considered as complete. It only applies to SIP gateway lines with entries that end in a # symbol.

For an outgoing call, the external called number generated from this entry is automatically regarded as complete according to the defined number of numerals, and then forwarded. This process speeds up the dialing process. Alternatively, the called number is regarded as complete when:

The user concludes the dialed number with a # symbol, or

a precisely matching entry was found in the SIP mapping table without a # symbol, or

the wait time expires.

Telnet path: /Setup/Voice Call Manager/Lines/SIP-provider/Mapping

Possible values:

- Max. 9 numbers

Default: 0

Special values: Setting the length of called number to '0' deactivates premature dialing from the length of called number.

2.33.4.1.2.5 Active

Activates or deactivates the entry.

Telnet path: /Setup/Voice Call Manager/Lines/SIP-provider/Mapping

Possible values:

- On
- Off

Default: On

2.33.4.1.2.6 Comment

Comment on this entry

Telnet path: /Setup/Voice Call Manager/Lines/SIP-provider/Mapping

Possible values:

- Max. 64 characters

Default: Blank

2.33.4.1.2.7 CLIR

The display of your telephone number is suppressed so the person called cannot see it.

Telnet path: /Setup/Voice Call Manager/Lines/SIP-provider/Mapping

Possible values:

- Yes
- No

Default: No

2.33.4.2 SIP-PBX

This menu contains SIP PBX settings for the Voice Call Manager.

Telnet path: /Setup/Voice- Call- Manager/Lines

2.33.4.2.1 SIP- PBX

These lines are used to configure connections to upstream SIP PBXs, which are usually connected via VPN. Up to 4 SIP PBXs can be entered.

Telnet path: /Setup/Voice- Call- Manager/Line/SIP- PBX

2.33.4.2.1.1 Name

Name of the line; may not be identical to another line that is configured in the device.

Telnet path: /Setup/Voice- Call- Manager/Line/SIP- PBX/PBX

Possible values:

- Max. 16 characters

Default: Blank

2.33.4.2.1.10 Codecs

While the connection is being established, the terminal equipment concerned negotiate which codecs are to be used to compress the voice data. Use the codec filter to restrict the codecs that are permitted and to permit only certain codecs.

Telnet path: /Setup/Voice- Call- Manager/Line/SIP- PBX/PBX

Possible values:

- Along with the widely available codecs, some models also support the following codec for the SIP gateway function:
- G.722 - 64 kbps (high-quality codec for ISDN to SIP and vice versa only)
- G.729 - 8 kbps (codec with higher compression for lower bandwidths)
- These codecs are available to the devices LANCOM 1722 VoIP, LANCOM 1723 VoIP, LANCOM 1724 VoIP and LANCOM 1823 VoIP, and also for all models with the LANCOM Advanced VoIP Option.

Default: All



If no common the codecs can be agreed upon, no connection is made.

2.33.4.2.1.11 Codec order

This parameter influences the order in which the codecs are presented during connection establishment.

Telnet path: /Setup/Voice- Call- Manager/Line/SIP- PBX/PBX

Possible values:

- No optimization: Leaves the order of the codecs unchanged
- Best quality: Changes the order of the codecs that are offered to achieve the best voice quality possible.
- Minimum bandwidth: Changes the order of the codecs that are offered to achieve the lowest bandwidth possible.

Default: No optimization

2.33.4.2.1.12 Routing tag

Routing tag for selecting a certain route in the routing table for connections to this SIP PBX.

Telnet path: /Setup/Voice- Call- Manager/Line/SIP- PBX/PBX

Possible values:

- Max. 64 numbers

Default: 0

2.33.4.2.1.13 Registrar

The SIP registrar is the point that accepts the login with the configured authentication data for this account in the SIP PBX.

Telnet path: /Setup/Voice- Call- Manager/Line/SIP- PBX/PBX

Possible values:

- Max. 63 characters

Default: Blank



This field can remain empty unless the SIP provider specifies otherwise. The address of the registrar is resolved over the realm.

2.33.4.2.1.14 Local port

This is the port used by the LANCOM proxy to communicate with the upstream SIP PBX.

Telnet path: /Setup/Voice- Call- Manager/Line/SIP- PBX/PBX

Possible values:

- 1 to 65536

Default: 0

Special values: 0: Dynamic port selection; the port is automatically selected from the pool of available port numbers.



If line (re-)registration is deactivated, the local port has to be defined with a fixed value, and this also has to be entered into the SIP PBX to ensure that both ends can send SIP signaling.

2.33.4.2.1.15 (Re-)registration

This activates the (repeated) registration of the SIP PBX line. Registration can also be used for line monitoring.

Telnet path: /Setup/Voice- Call- Manager/Line/SIP- PBX/PBX

Possible values:

- Yes
- No

Default: Yes



To use (re-) registration, the line monitoring method must correspondingly be set to "Register" or "Automatic". Registration is repeated after the monitoring interval has expired. If the SIP registrar in the SIP PBX suggests a different interval, the suggested value is used automatically.

2.33.4.2.1.16 Line-monitoring

Specifies the line monitoring method. Line monitoring checks if a SIP PBX line is available. The Call Router can make use of the monitoring status to initiate a change to a backup line. The monitoring method sets the way in which the status is checked.

Telnet path: /Setup/Voice- Call- Manager/Line/SIP- PBX/PBX

Possible values:

- Auto: The method is set automatically.
- Disabled: No monitoring; the line is always reported as being available. This setting does not allow the actual line availability to be monitored.
- Register: Monitoring by means of register requests during the registration process. This setting also requires "(Re-)registration" to be activated for this line.
- Options: Monitoring via Options Requests. This involves regular polling of the remote station. Depending on the response the line is considered to be available or unavailable. This setting is well suited for e.g. lines without registration.

Default: Auto

2.33.4.2.1.17 Monitoring interval

The monitoring interval in seconds. This value affects the line monitoring with register request and also the option request. The monitoring interval must be set to at least 60 seconds. This defines the time period that passes before the monitoring method is used again. If (re-) registration is activated, the monitoring interval is also used as the time interval before the next registration.

Telnet path: /Setup/Voice- Call- Manager/Line/SIP- PBX/PBX

Possible values:

- Max. 5 numbers

Default: 60

Special values: Values less than 60 seconds are automatically set to 60 seconds.



If the remote station responds to an option request with a different suggested value for the monitoring interval, this is accepted and subsequently applied.

2.33.4.2.1.18 Trusted

Specifies the remote station on this line (provider) as "Trusted Area". In this trusted area, the caller ID is not concealed from the caller, even if this is requested by the settings on the line (CLIR) or in the device. In the event of a connection over a trusted line, the Caller ID is first transmitted in accordance with the selected privacy policy and is only removed in the final exchange before the remote subscriber. This means, for example, that Caller ID can be used for billing purposes within the trusted area. This function is interesting for providers using a VoIP router to extend their own managed networks all the way to the connection for the VoIP equipment.

Telnet path: /Setup/Voice- Call- Manager/Line/SIP- PBX/PBX

Possible values:

- Yes: Trusted
- No: Not trusted

Default: Yes



Please note that not all providers support this function.

2.33.4.2.1.19 Privacy method

Specifies the method used for transmitting the caller ID in the separate SIP-header field.

Telnet path: /Setup/Voice- Call- Manager/Line/SIP- PBX/PBX

Possible values:

- None
- RFC3325: Using P-Preferred-Id/P-Asserted-Id
- IETF-Draft-Sip-Privacy-04: Using RPID (Remote Party ID)

Default: None

2.33.4.2.1.2 Domain

SIP domain/realm of the upstream SIP PBX.

Telnet path: /Setup/Voice- Call- Manager/Line/SIP- PBX/PBX

Possible values:

- Max. 64 characters

Default: Blank

2.33.4.2.1.3 Port

TCP/UDP port of the upstream SIP PBX to which the LANCOM device sends the SIP packets.

Telnet path: /Setup/Voice- Call- Manager/Line/SIP- PBX/PBX

Possible values:

- Any available TCP/IP port.

Default: 5060



This port has to be activated in the firewall for the connection to work.

2.33.4.2.1.4 Secret

Shared password for registering with the SIP PBX. This password is only required (a) when SIP subscribers have to log in to the PBX who have not been set up as SIP users with their own access data in the SIP user

list or (b) when local SIP authentication is not forced. This means that SIP users can register with the LAN-COM device without a password and can log in to the upstream SIP PBX with a shared password if the SIP user's domain is the same as the domain of a SIP PBX line.

Telnet path: /Setup/Voice- Call- Manager/Line/SIP- PBX/PBX

Possible values:

■ Max. 64 characters

Default: Blank

2.33.4.2.1.5 Outbound proxy

A SIP proxy receives requests from SIP clients and acts as a proxy while the connection is being established.

Telnet path: /Setup/Voice- Call- Manager/Line/SIP- PBX/PBX

Possible values:

■ Max. 64 characters

Default: Blank



This field can remain empty unless the SIP provider specifies otherwise. The address of the proxy is resolved over the realm.

2.33.4.2.1.6 Active

Activates or deactivates the entry.

Telnet path: /Setup/Voice- Call- Manager/Line/SIP- PBX/PBX

Possible values:

■ On

■ Off

Default: On

2.33.4.2.1.7 Comment

Comment on this entry

Telnet path: /Setup/Voice- Call- Manager/Line/SIP- PBX/PBX

Possible values:

■ Max. 64 characters

Default: Blank

2.33.4.2.1.8 Cln- Prefix

The call prefix is a number placed in front of the caller number (CLI; SIP "From:") for all incoming calls. This generates unique telephone numbers for return calls.

For example; a number can be added, which the call router analyzes (and subsequently removes) to select the line to be used for the return call.

Telnet path: /Setup/Voice- Call- Manager/Line/SIP- PBX/PBX

Possible values:

■ Max. 9 numbers

Default: Blank

2.33.4.2.1.9 Line prefix

With outgoing calls using this line, this prefix is placed in front of the calling number to create a complete telephone number that is valid for this line. With incoming calls this prefix is removed, if present.

Telnet path: /Setup/Voice- Call- Manager/Line/SIP- PBX/PBX

Possible values:

■ Max. 9 numbers

Default: Blank

2.33.4.3 ISDN

The ISDN connections are configured over these lines. In addition to the physical ISDN line to be used, a telephone number translation is configured as well. This ensures the internal telephone number or SIP URL is converted to an external ISDN number.

Telnet path: /Setup/Voice- Call- Manager/Lines

2.33.4.3.1 Interfaces

This is where the lines to ISDN exchanges or PBX systems are configured (the router is the terminal device).

Telnet path: /Setup/Voice- Call- Manager/Line/ISDN

2.33.4.3.1.1 Name

This name uniquely identifies the line. It may not be assigned to any other line.

Telnet path: /Setup/Voice- Call- Manager/Line/ISDN/Interfaces

Possible values:

- Max. 64 characters

Default: Blank



Here you can, for example, enter the telephone number for a group that is to receive incoming calls. This allows you to flexibly control which telephones ring for incoming calls, or to transfer calls to a mobile phone number or answering machine after a certain time.

2.33.4.3.1.2 Interface

Interface to which the ISDN subscribers are connected.

Telnet path: /Setup/Voice- Call- Manager/Line/ISDN/Interfaces

Possible values:

- All available ISDN interfaces.

Default: Model dependent.

2.33.4.3.1.3 Domain

Domain in which the calls from/to the ISDN line are managed in LANCOM's SIP world.

Telnet path: /Setup/Voice- Call- Manager/Line/ISDN/Interfaces

Possible values:

- Max. 64 characters

Default: Blank

2.33.4.3.1.4 Cln-Prefix

The call prefix is a number placed in front of the caller number (CLI; SIP "From:") for all incoming calls. This generates unique telephone numbers for return calls.

Telnet path: /Setup/Voice- Call- Manager/Line/ISDN/Interfaces

Possible values:

- Max. 9 numbers

Default: Blank

2.33.4.3.1.5 Active

Activates or deactivates the entry.

Telnet path: /Setup/Voice- Call- Manager/Line/ISDN/Interfaces

Possible values:

- On
- Off

Default: On

2.33.4.3.1.6 Comment

Comment on this entry

Telnet path: /Setup/Voice- Call- Manager/Line/ISDN/Interfaces

Possible values:

■ Max. 64 characters

Default: Blank

2.33.4.3.2 Mapping

ISDN mapping assigns external ISDN telephone numbers (MSN or DDI) to the telephone numbers that are used internally. You can enter up to 64 telephone number assignments.

Telnet path: /Setup/Voice- Call- Manager/Line/ISDN

2.33.4.3.2.1 MSN/DDI

External telephone number of the connection in the ISDN network.

For incoming calls that are directed to this number, the corresponding internal telephone number is entered as the destination number. For outgoing calls, this number is transmitted as the caller's number, unless this has been suppressed.

MSN: Number of the telephone connection

DDI (Direct Dialing in): Telephone extension number if the connection is configured as a point-to-point line.

Telnet path: /Setup/Voice- Call- Manager/Line/ISDN/Mapping

Possible values:

■ Max. 19 numbers

Default: Blank



By using the # character as a placeholder, entire groups of call numbers, e.g. when using extension numbers, can be addressed via a single entry.

2.33.4.3.2.2 Interface

ISDN interface(s) used for connecting terminal devices to the LANCOM VoIP router. These line have to be configured as ISDN-NT.

Telnet path: /Setup/Voice- Call- Manager/Line/ISDN/Mapping

Possible values:

■ All available ISDN interfaces.

Default: Model dependent.

2.33.4.3.2.3 Number/Name

Internal telephone number of the ISDN telephone or name of the user (SIP URL).

For incoming calls, this is the SIP name or internal telephone number of the telephone to which the call from this interface is switched with the corresponding MSN/DDI. For outgoing calls, the SIP name is replaced by the MSN/DDI of the corresponding entry.

Telnet path: /Setup/Voice- Call- Manager/Line/ISDN/Mapping

Possible values:

■ Max. 64 characters

Default: Blank



By using the # character as a placeholder, entire groups of call numbers, e.g. when using extension numbers, can be addressed via a single entry.

2.33.4.3.2.4 CLIR

The display of your telephone number is suppressed so the person called cannot see it.

Telnet path: /Setup/Voice- Call- Manager/Line/ISDN/Mapping

Possible values:

■ Yes

- No

Default: No

2.33.4.3.2.5 Active

Activates or deactivates the entry.

Telnet path: /Setup/Voice- Call- Manager/Line/ISDN/Mapping

Possible values:

- On
- Off

Default: On

2.33.4.3.2.6 Comment

Comment on this entry

Telnet path: /Setup/Voice- Call- Manager/Line/ISDN/Mapping

Possible values:

- Max. 64 characters

Default: Blank

2.33.4.4 Predefined destination

Table with predefined special functions for the destination lines in the call routing entries.

Telnet path: /Setup/Voice- Call- Manager/Lines

2.33.4.4.1 Name

Predefined special functions for the destination lines in the call routing entries.

Telnet path: /Setup/Voice- Call- Manager/Line/Predef- Dest.

Possible values:

- REJECT highlights a blocked telephone number.
- USER forwards the call to local SIP, analog or ISDN subscribers.
- RESTART starts a new pass through the call routing table with the previously formed "number/name". The former "source line" is deleted.

Default: REJECT

USER

RESTART

2.33.4.5 Source filters

Table with predefined source lines to filter calls from local users.

Telnet path: /Setup/Voice- Call- Manager/Lines

2.33.4.5.1 Name

Predefined source lines to filter calls from local users.

Telnet path: /Setup/Voice- Call- Manager/Line/Source- Filters

Possible values:

- USER.ANALOG for calls from a local analog subscribers
- USER.ISDN for calls from a local ISDN subscriber
- USER.SIP for calls from a local SIP subscriber
- USER# for calls from a local subscriber in general

Default: USER.ANALOG

USER.ISDN

USER.SIP

USER#

2.33.4.6 Analog

The analog connections are configured over these lines. In addition to the physical analog line to be used, a telephone number translation is configured as well.

Telnet path: /Setup/Voice- Call- Manager/Lines

2.33.4.6.1 Interfaces

This is where the lines to analog exchanges (external lines) or PBX systems are configured (the router is the terminal device).

Telnet path: /Setup/Voice- Call- Manager/Line/Analog

2.33.4.6.1.1 Name

Name of the line; may not be identical to another line that is configured in the device.

Telnet path: /Setup/Voice- Call- Manager/Line/Analog/Interfaces

Possible values:

■ ANALOG

Default: ANALOG

2.33.4.6.1.10 Caller ID transmission requirements

Apart from selecting the modulation method, different countries and providers also have different time delays in the signaling of the Caller ID over analog lines. The telephone being called expects the Caller ID at a certain time, and so providers should set up their systems accordingly.

Telnet path: /Setup/Voice- Call- Manager/Line/Analog/Interfaces

Possible values:

- Default: With this setting, the values taken are the default values for the country where the device is operated.
- During ringing: The Caller ID is transmitted while the phone is ringing between the first and second ring.
- RP AS: Transmission of the Caller ID is not directly connected with the ringing but is transferred via a special "alerting signal". This alerting signal is a ringing impulse (Ringing Pulse Alerting Signal,
- RP-AS). The Caller ID can be transferred after the ringing impulse.
- Line reversal: Transmission of the Caller ID is not directly connected with the ringing but is transferred via a special "alerting signal". The alarm signal is sent by a brief reversal of polarity in the line (line reversal). The Caller ID can be transferred after the line reversal.

Default: Country-specific default values:

Austria: During-Ringing

Belgium: Ringing Pulse Alerting Signal, RP-AS

France: During-Ringing

Italy: During-Ringing

Switzerland: During-Ringing

The Netherlands: Line reversal

Spain: Ringing Pulse Alerting Signal, RP-AS

United Kingdom: Line reversal

Germany: During-Ringing

2.33.4.6.1.2 Domain

The analog line's domain name used for addressing in SIP.

Telnet path: /Setup/Voice- Call- Manager/Line/Analog/Interfaces

Possible values:

- Max. 64 characters

Default: Blank

2.33.4.6.1.3 Cln-Prefix

The call prefix is a number placed in front of the caller number (CLI; SIP "From:") for all incoming calls on this analog line. This generates unique telephone numbers for return calls.

For example; a number can be added, which the call router analyzes (and subsequently removes) to select the line to be used for the return call.

Telnet path: /Setup/Voice- Call- Manager/Line/Analog/Interfaces

Possible values:

- Max. 9 numbers

Default: Blank

2.33.4.6.1.4 Number/Name

Internal number/SIP URI that each call on this analog line is given as call destination. This number can differ from the telco's actual call number for the analog connection (mapping).

Telnet path: /Setup/Voice- Call- Manager/Line/Analog/Interfaces

Possible values:

- Max. 64 characters

Default: Blank

2.33.4.6.1.5 Active

Activates or deactivates the entry.

Telnet path: /Setup/Voice- Call- Manager/Line/Analog/Interfaces

Possible values:

- On
- Off

Default: On

2.33.4.6.1.6 Comment

Comment on this entry

Telnet path: /Setup/Voice- Call- Manager/Line/Analog/Interfaces

Possible values:

- Max. 64 characters

Default: Blank

2.33.4.6.1.7 Line type

The line type provides a simplified model of an analog line.

Telnet path: /Setup/Voice- Call- Manager/Lines/Analog/Interfaces/Line-type

Possible values:

- Default
- EIA0
- EIA1
- EIA2
- EIA3
- EIA4
- EIA5
- EIA6
- EIA7

Default: Default



The settings for the line type are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.33.4.6.1.8 Central office termination

The Central Office Termination is the complex terminating resistor that terminates the exchange line. This depends on the country of operation.

Telnet path: /Setup/Voice-Call-Manager/Lines/Analog/Interfaces/Central-Office-Termination

Possible values:

- Default
- 220Ohm+820Ohm|115nF
- 200Ohm+560Ohm|100nF
- 270Ohm+750Ohm|150nF
- 370Ohm+620Ohm|310nF
- 220Ohm+1200Ohm|115nF
- 600Ohm
- 220Ohm+820Ohm|120nF
- 300Ohm+1000Ohm|220nF
- 600Ohm+1.5uF
- 150Ohm+510Ohm|47nF
- 1200Ohm+376Ohm|112nF

Default: Default



The settings for the Central Office Termination are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.33.4.6.1.9 Caller-ID signaling

Providers of analog telephone connections support various services including Caller ID transmission, i.e. the caller's number is shown in the display of the telephone being called. This service is also known as Calling Line Identification Presentation (CLIP). Depending on the country and provider, two different methods of modulation are used to transfer the caller ID over the analog line (FSK or DTMF).

Telnet path: /Setup/Voice-Call-Manager/Line/Analog/Interfaces

Possible values:

- Default: With this setting, the values taken are the default values for the country where the device is operated.
- FSK: Transfer of the Caller ID with the Frequency Key Shifting method.
- DTMF: Transfer of the Caller ID with the Dual Tone Multi Frequency method.

Default: Country-specific default values:

The Netherlands: DTMF

All other countries: V.23 (FSK)

2.33.5 Call router

This menu contains call router settings for the Voice Call Manager.

Telnet path: /Setup/Voice-Call-Manager

2.33.5.1 Call routing

Rules can be defined here for redirecting or rejecting calls to certain call targets or lines.

Telnet path: /Setup/Voice-Call-Manager/Call-Router

2.33.5.1.1 Called ID

The called party name or destination telephone number (without domain information) that is called.

Telnet path: /Setup/Voice- Call- Manager/Call-Router/Call- Routing

Possible values:

- Max. 64 characters

Default: Blank

Special values: The # character is used as a placeholder for any character strings. All characters in front of the # are removed, the remaining characters are used in the "Number/name" field instead of the # character to further establish the connection.



Example: The call routing table contains entry '00049#' as the called number/name and '00#' as the number/name. For all calls with a preceding '0' for outside-line access and the complete dialing code for Germany, only the leading '0' for the outside-line access and the leading '0' for the local area dialing code are retained as the number/name; the country ID is removed. So '00049 2405 123456' becomes '0 02405 123456'.

2.33.10.7.15 Comment

Comment on this entry

Telnet path: /Setup/Voice- Call- Manager/Call-Router/Call- Routing

Possible values:

- Max. 64 characters

Default: Blank

2.33.5.1.11 Dest-Id-2

This telephone number is used to establish the connection further if nothing is entered in "number/name" or the corresponding "line" is not available. If no connection can be established using this 2nd call number and the relevant 2nd line, the 3rd call number and 3rd line will be used.

Telnet path: /Setup/Voice- Call- Manager/Call-Router/Call- Routing

Possible values:

- Max. 64 characters

Default: Blank

2.33.5.1.12 Dest-Line-2

The connection is established using this line if the 2nd number is used to establish the connection. The same lines can be dialed as for "line".

Telnet path: /Setup/Voice- Call- Manager/Call-Router/Call- Routing

Possible values:

- Analog
- ISDN
- All defined SIP lines.
- The following special functions can be entered as a destination line:
 - REJECT highlights a blocked telephone number.
 - USER forwards the call to local SIP, analog or ISDN subscribers.
 - RESTART starts a new pass through the call routing table with the previously formed "number/name". The former "source line" is deleted.

Default: Blank

2.33.5.1.13 Dest-Id-3

Similar to the 2nd number.

Telnet path: /Setup/Voice- Call- Manager/Call-Router/Call- Routing

Possible values:

- Max. 64 characters

Default: Blank

2.33.5.1.14 Dest-Line-3

Similar to the 2nd line.

Telnet path: /Setup/Voice- Call-Manager/Call-Router/Call-Routing

Possible values:

- Analog
- ISDN
- All defined SIP lines.
- The following special functions can be entered as a destination line:
- REJECT highlights a blocked telephone number.
- USER forwards the call to local SIP, analog or ISDN subscribers.
- RESTART starts a new pass through the call routing table with the previously formed "number/name". The former "source line" is deleted.

Default: Blank

2.33.5.1.15 Priority

The Call Manager sorts all entries with the same priority automatically, so that the table can be processed through logically from top to bottom. With some entries, however, the sequence of the entries has to be specified (for the telephone number translation, for example). The entries with the highest priority are automatically sorted to the top.

Telnet path: /Setup/Voice- Call-Manager/Call-Router/Call-Routing

Possible values:

- 0 to 999

Default: 0

2.33.5.1.2 Cld-Domain

This entry filters the called domain, the "Called Party Domain". The call router entry is only considered to match if the Called Party Domain for the call matches the domain that is entered here. If nothing is specified, any destination domain is accepted.

Telnet path: /Setup/Voice- Call-Manager/Call-Router/Call-Routing

Possible values:

- Analog
- ISDN
- The internal VoIP domains of the LANCOM VoIP router.
- All domains entered for the SIP and SIP-PBX lines.

Default: Blank

2.33.5.1.3 Calling-Id

This entry filters the calling number/name, the "calling party ID". It is specified as an internal number or as a national or international telephone number. The domain is not specified. No "0" or other character for a line ID is prefixed; the ID is used as if it comes from the line or from internal telephone calls.

The call router entry is only evaluated as matching if the Calling Party ID for the call matches the number that is entered here. After "#", any characters can be accepted.

Telnet path: /Setup/Voice- Call-Manager/Call-Router/Call-Routing

Possible values:

- Internal number
- National
- International call number.
- LOCAL restricts to internal telephone numbers (without a leading "0").
- EMPTY can be used for Calling Party IDs that are not specified.

Default: Blank



If nothing is specified here, any Calling Party ID is accepted.

2.33.5.1.4 Cln-Domain

This entry filters the calling domain. The call router entry is only considered to match if the Calling Domain for the call matches the domain that is entered here. If nothing is specified, each calling domain is accepted.

Telnet path: /Setup/Voice- Call- Manager/Call-Router/Call- Routing

Possible values:

- Analog
- ISDN
- The internal VoIP domains of the LANCOM VoIP router.
- All domains entered for the SIP and SIP-PBX lines.

Default: Blank



SIP telephones usually have several line keys, for which different domains can be configured. With this filter, telephone calls are handled depending on the selection that is made using different line keys.

2.33.5.1.5 Src-Line

This entry filters the source line. The call router entry is only considered to match if the source line for the call matches the line that is entered here. If nothing is specified, any calling line is accepted.

Telnet path: /Setup/Voice- Call- Manager/Call-Router/Call- Routing

Possible values:

- USER.ANALOG for calls from a local analog subscribers
- USER.ISDN for calls from a local ISDN subscriber
- USER.SIP for calls from a local SIP subscriber
- USER# for calls from a local subscriber in general
- All ISDN, SIP and SIP-PBX lines that are entered.

Default: Blank

2.33.5.1.7 Destination-Id-1

This telephone number is used to continue with establishing the connection. If no connection can be established using this telephone number and the corresponding line, then the backup telephone numbers with their associated lines are used

Telnet path: /Setup/Voice- Call- Manager/Call-Router/Call- Routing

Possible values:

- Max. 64 characters

Default: Blank



At least one of the entries "Number/Name", "1st Backup No." or "2nd Backup No." must be filled in. They are evaluated in this sequence. A blank field is skipped.

2.33.5.1.8 Destination-Line-1

The connection is established using the destination line.

ISDN

All defined SIP lines.

The following special functions can be entered as a destination line:

REJECT highlights a blocked telephone number.

USER forwards the call to local SIP or ISDN subscribers.

RESTART starts a new pass through the call routing table with the previously formed "number/name". The former "source line" is deleted.

Telnet path: /Setup/Voice- Call- Manager/Call-Router/Call- Routing

Possible values:

- Analog
- ISDN

- All defined SIP lines.
- The following special functions can be entered as a destination line:
- REJECT highlights a blocked telephone number.
- USER forwards the call to local SIP, analog or ISDN subscribers.
- RESTART starts a new pass through the call routing table with the previously formed "number/name". The former "source line" is deleted.

Default: Blank



This field has to be completed, otherwise the entry is not used.

2.33.5.1.9 Active

The routing entry can be activated, deactivated, or marked as a default entry. All calls that can be resolved using the first passes but not using the call routing table or local subscriber table are then automatically resolved using these default entries. You can use any destination name and destination domain; only the source filters that are set are considered

Telnet path: /Setup/Voice- Call- Manager/Call-Router/Call-Routing

Possible values:

- Active
- Idle
- Default line

Default: Active

2.33.7 Groups

This menu contains user-group settings for the Voice Call Manager.

Telnet path: /Setup/Voice- Call- Manager

2.33.7.1 Groups

Groups are defined here that enable incoming calls to be automatically distributed to two or more subscribers.

Telnet path: /Setup/Voice- Call- Manager/Groups

2.33.7.1.1 Name

The hunt group is available under this telephone number or SIP-ID.

Telnet path: /Setup/Voice- Call- Manager/Groups/Groups

Possible values:

- Max. 64 characters

Default: Blank



The names of hunt groups may not coincide with the names of users (SIP, ISDN, analog).

2.33.7.1.2 Members

Comma-separated list of the members of the hunt group. Members can be users, hunt groups or external telephone numbers, and so there is no limit on scaling.

Telnet path: /Setup/Voice- Call- Manager/Groups/Groups

Possible values:

- Users
- Hunt groups
- External telephone numbers

Default: Blank



A hunt group may not contain itself or any parents in the hierarchical system—recursion through member entries is not possible. However, loops to parents in the structure can be set up via the 'Forwarding target'.

2.33.7.1.3 Distribution method

Sets the type of call distribution.

Telnet path: /Setup/Voice-Call-Manager/Groups/Groups

Possible values:

- **Simultaneous:** The call is signaled to all group members at once. If a member picks up the call within the call-forwarding time, the call is no longer signaled to other group members. If nobody accepts the call within the forwarding time, then the call is switched to its forwarding target.
- **Sequential:** The call is directed to one member of the group after the other. If a group member does not accept the call within the forwarding time, then the call is switched to the next member of the group. If nobody in the group accepts the call within the forwarding time, then the call is switched to its forwarding target.

Default: Simultaneous

2.33.7.1.4 Forwarding time

If an incoming call is not picked up by a group member within the forwarding time, then the call is forwarded according to the distribution method selected:

In the case of simultaneous call distribution, the call is forwarded to the forwarding target.

In case of sequential call distribution, the call is forwarded to the next group member in line. If the group member is the last one in the sequence, then the call is redirected to its forwarding target.

Telnet path: /Setup/Voice-Call-Manager/Groups/Groups

Possible values:

- Max. 255 seconds

Default: 15

Special values: 0 seconds. The call is forwarded immediately to the forwarding target (temporarily jumps a hunt group in a hierarchy).



If all members of the group are busy or unavailable, then the call is redirected to the forwarding target without waiting for the forwarding-time to expire.

2.33.7.1.5 Forwarding target

If none of the group members accepts the call within the forwarding time, then the call is switched to the forwarding target entered here. Forwarding targets can be users, hunt groups or external telephone numbers. Only one forwarding target can be entered.

Telnet path: /Setup/Voice-Call-Manager/Groups/Groups

Possible values:

- Users
- Hunt groups
- External telephone numbers

Default: Blank



If no forwarding target is defined, then the call is rejected as soon as the member list has been worked through, or if all members are busy or unavailable.

The forwarding target only becomes active once the group's forwarding time has expired or if no members are available. Here, too, redirection to a higher level of the hunt-group structure is possible, unlike with the 'Members' entry.

2.33.7.1.6 Active

Activates or deactivates the entry.

Telnet path: /Setup/Voice-Call-Manager/Groups/Groups

Possible values:

- On
- Off

Default: On**2.33.7.1.7 Comment**

Comment on this entry

Telnet path: /Setup/Voice-Call-Manager/Groups/Groups**Possible values:**

- Max. 64 characters

Default: Blank**2.33.8 Logging**

This menu contains logging settings for the Voice Call Manager.

Telnet path: /Setup/Voice-Call-Manager**2.33.8.1 Call data records**

This menu contains logging settings for the Voice Call Manager.

Telnet path: /Setup/Voice-Call-Manager/Logging**2.33.8.1.2 E-mail address**

E-mail address for sending messages.

Telnet path: /Setup/Voice-Call-Manager/Logging/Call-Data-Records**Possible values:**

- Valid e-mail address

Default: Blank**2.33.8.1.1 E-mail notification**

You can optionally receive information about all of the calls made via the LANCOM VoIP router via e-mail. For every call which is connected (internal, external, incoming, outgoing), a message is generated containing information such as the source and target number, start-time and end-time of the call, etc.

Telnet path: /Setup/Voice-Call-Manager/Logging/Call-Data-Records**Possible values:**

- On
- Off

Default: Off

An SMTP account must be set up to make use of this function.

2.33.8.1.3 Syslog

You can also obtain information on all calls made over the LANCOM VoIP router using SYSLOG (facility: accounting; level: info). For every call which is connected (internal, external, incoming, outgoing), a message is generated containing information such as the source and target number, start-time and end-time of the call, etc.

Telnet path: /Setup/Voice-Call-Manager/Logging/Call-Data-Records**Possible values:**

- On
- Off

Default: Off



A syslog client must be set up to make use of this function.

2.34 Printer

This menu contains settings for the printer.

Telnet path: /Setup

2.34.1 Printer

You can adjust setting for the network printer here.

Telnet path: /Setup/Printer

2.34.1.1 Printer

Printer name.

Telnet path: /Setup/Printer/Printer

Possible values:

■ Max. 10 characters

Default: *

2.34.1.2 RawIP port

This port can be used to accept print jobs over RawIP.

Telnet path: /Setup/Printer/Printer

Possible values:

■ Max. 10 characters

Default: 9100

2.34.1.3 LPD port

This port can be used to accept print jobs over LDP.

Telnet path: /Setup/Printer/Printer

Possible values:

■ Max. 10 characters

Default: 515

2.34.1.4 Operating

Activates or deactivates this entry.

Telnet path: /Setup/Printer/Printer

Possible values:

■ Yes: The print server is active.

■ No: The print server is not active.

Default: No

2.34.1.5 Bidirectional

This parameter enables or disables the bi-directional mode of the printer.

Telnet path: /Setup/Printer/Printer



The bidirectional model of the printer is intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.34.1.6 Reset on open

If this option is activated the device will send a reset command to the printer before opening a printer session.

Telnet path: /Setup/Printer/Printer

Possible values:

- Yes
- No

Default: No



Activate this option if the connection to the printer does not work as expected.

2.34.2 Access list

Here you define the networks that have access to the printer.

Telnet path: /Setup/Printer

2.34.2.1 IP address

IP address of the network with clients requiring access to the printer.

Telnet path: Setup/Printer/Access-list

Possible values:

- Valid IP address.

Default: 00.0.0

2.34.2.2 IP netmask

Netmask of the permitted networks.

Telnet path: Setup/Printer/Access-list

Possible values:

- Valid IP address.

Default: 00.0.0

2.34.2.3 Routing tag

If you specify a routing tag for this access rule, the only packets that will be accepted have received the same tag in the firewall or they are from a network with the corresponding interface tag. If the routing tag is 0, access attempts from suitable IP addresses are accepted every time.

Telnet path: /Setup/Printer/Access-list/Rtg-tag

Possible values:

- Max. 5 characters

Default: Blank



It follows that the use of routing tags only makes sense in combination with the appropriate accompanying rules in the firewall or tagged networks.

2.35 ECHO server

This menu contains the configuration of the ECHO server.

Telnet path: /Setup

2.35.1 Operating

The echo server is used to monitor the line quality by measuring RTT and jitter.

Telnet path: /Setup/ECHO-Server

Possible values:

- Yes
- No

Default: No

2.35.3 TCP timeout

If a TCP session to an ECHO server is inactive for 10 (default) seconds, the server disconnects. Normally TCP clears up "dormant" connections by itself, but this takes far longer.

Telnet path: /Setup/ECHO-Server

Possible values:

- Max. 10 characters

Default: 10

2.35.2 Access table

This table defines the access rights for using the ECHO server.

Telnet path: /Setup/ECHO-Server

2.35.2.1 IP address

IP address of remote device.

Telnet path: /Setup/ECHO-server/Access-table

Possible values:

- Valid IP address.

2.35.2.2 Netmask

IP address of remote device.

Telnet path: /Setup/ECHO-server/Access-table

Possible values:

- Valid IP address.

2.35.2.3 Protocol

Protocol used for measuring.

Telnet path: /Setup/ECHO-server/Access-table

Possible values:

- None

- TCP
- UDP
- TCP+UDP

2.35.2.4 Operating

Activates or deactivates this entry in the table.

Telnet path: /Setup/ECHO-server/Access-table

Possible values:

- Yes
- No

Default: No

2.35.2.5 Comment

Comment on this entry.

Telnet path: /Setup/ECHO-server/Access-table

2.36 Performance monitoring

This menu contains the configuration of the performance monitoring.

Telnet path: /Setup

2.36.2 RttMonAdmin

This table displays information about the type of measurements.

Telnet path: /Setup/Performance-Monitoring

2.36.2.1 Index

Shared index for the measurement

Telnet path: /Setup/Performance-Monitoring/RttMonAdmin

2.36.2.4 Type

Measurement type.

Telnet path: /Setup/Performance-Monitoring/RttMonAdmin

2.36.2.6 Frequency

Time in milliseconds until the measurement is repeated. Is the only parameter that can be modified while the status is active. In this case only 0 is allowed in order to prevent further iterations.

Telnet path: /Setup/Performance-Monitoring/RttMonAdmin

2.36.2.7 Timeout

Measurement timeout in milliseconds. The timeout value must be smaller than the time until measurement is repeated.

Telnet path: /Setup/Performance-Monitoring/RttMonAdmin

2.36.2.9 Status

Measurement status

Telnet path: /Setup/Performance-Monitoring/RttMonAdmin

Possible values:

- Active: Measurement is in progress. This value can only be set if the Status value is Not_In_Service. No measurement parameters can be modified while the Status is active.
- Not_In_Service: All parameters required have been set; no measurement is currently in progress.
- Not_Ready: Not all parameters required have been set.
- Create: Create a table row. SNMP Set is used to create a table row by setting the desired index to Create. When configuration is performed from the menu system the Status must also first be set to Create. When a new table row is created, the appropriate rows in the other tables are created automatically.
- Destroy: Delete a table row. This is only possible when the status is not Active. The appropriate rows in the other tables are deleted automatically.

2.36.3 RttMonEchoAdmin

This table displays information about the the measurements.

Telnet path: /Setup/Performance-Monitoring

2.36.3.1 Protocol

Protocol to be used

Telnet path: /Setup/Performance-Monitoring/RttMonEchoAdmin

2.36.3.17 Interval

Time between two measurement packets in milliseconds

Telnet path: /Setup/Performance-Monitoring/RttMonEchoAdmin

2.36.3.18 Packet count

Number of measurement packets per measurement

Telnet path: /Setup/Performance-Monitoring/RttMonEchoAdmin

2.36.3.2 Destination address

Address of the responder

Telnet path: /Setup/Performance-Monitoring/RttMonEchoAdmin

Possible values:

- Valid IP address.

2.36.3,255 Index

Shared index for the measurement

Telnet path: /Setup/Performance-Monitoring/RttMonEchoAdmin

2.36.3.3 Packet size

Length of the measurement packets in bytes. Packets are padded out to the minimum length required by the measurement.

Telnet path: /Setup/Performance-Monitoring/RttMonEchoAdmin

2.36.3.5 Destination port

Destination port. Currently ignored

Telnet path: /Setup/Performance-Monitoring/RttMonEchoAdmin

2.36.4 RttMonStatistics

This table displays performance monitoring statistics.

Telnet path: /Setup/Performance-Monitoring

2.36.4.10 Jitter-Min-Pos-SD

Minimum positive jitter value from sender to responder in uSec

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.11 Jitter-Max-Pos-SD

Maximum positive jitter value from sender to responder in uSec

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.12 Jitter-Count-Pos-SD

Number of positive jitter values determined from sender to responder

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.13 Jitter-Sum-Pos-SD

Sum of all positive jitter values from sender to responder in uSec

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.16 Jitter-Min-Pos-DS

Minimum positive jitter value from responder to sender in uSec

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.17 Jitter-Max-Pos-DS

Maximum positive jitter value from responder to sender in uSec

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.18 Jitter-Count-Pos-DS

Number of positive jitter values determined from responder to sender

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.19 Jitter-Sum-Pos-DS

Sum of all positive jitter values from responder to sender in uSec

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.2 Completions

Number of measurements performed.

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.22 Jitter-Min-Neg-SD

Minimum negative jitter value from sender to responder in uSec, absolute value

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.23 Jitter-Max-Neg-SD

Maximum negative jitter value from sender to responder in uSec, absolute value

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.24 Jitter-Count-Neg-SD

Number of negative jitter values determined from sender to responder

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.25 Jitter-Sum-Neg-SD

Sum of all negative jitter values from sender to responder in uSec, absolute value

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4,255 Index

Shared index for the measurement

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.28 Jitter-Min-Neg-DS

Minimum negative jitter value from responder to sender in uSec, absolute value

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.29 Jitter-Max-Neg-DS

Maximum negative jitter value from responder to sender in uSec, absolute value

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.30 Jitter-Count-Neg-DS

Number of negative jitter values determined from responder to sender

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.31 Jitter-Sum-Neg-DS

Sum of all negative jitter values from responder to sender in uSec, absolute value

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.34 Packet-Loss-SD

Number of packets lost from sender to responder

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.35 Packet-Loss-DS

Number of packets lost from responder to sender

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.4 RTT-Count

Total number of RTT values determined

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.5 RTT-Sum

Sum of all RTT values determined

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.62 Average-Jitter

Average of all absolute jitter values

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.63 Average-Jitter-SD

Average of all absolute jitter values from sender to responder

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.64 Average-Jitter-DS

Average of all absolute jitter values from responder to sender

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.8 RTT-Min

Minimum roundtrip time in uSec

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.9 RTT-Max

Maximum roundtrip time in uSec

Telnet path: /Setup/Performance-Monitoring/RttMonStatistics

2.37 WLAN management

This menu is used to configure WLAN management for WLAN controllers.

2.37.6 Autoaccept AP

Enables the WLAN controller to provide all new access points with a configuration, even those not in possession of a valid certificate.

Enables the WLAN controller to provide a certificate to all new access points without a valid certificate. One of two conditions must be fulfilled for this:

- A configuration is entered into the AP table for the access point under its MAC address.
- The option 'Automatically provide APs with the default configuration' is enabled.

Telnet path: /Setup/WLAN-Management

Possible values:

- Yes
- No

Default: No



Combining the settings for auto-accept and default configuration can cater for a variety of different situations for the setup and operation of access points:

Auto accept ON, default configuration ON: Rollout phase: Use this combination only if you can be sure that no unintended access points are connected with the LAN and thus accepted into the WLAN infrastructure.

Auto accept ON, default configuration OFF: Controlled rollout phase: Use this combination if you have entered all of the approved access points into the AP table along with their MAC addresses, assuming that these are to be automatically accepted into the WLAN infrastructure.

Auto accept OFF, default configuration OFF: Normal operation: No new access points will be accepted into the WLAN infrastructure without the administrator's approval.

2.37.7 Accept AP

Do command to accept new APs. The MAC address must be specified as a parameter. Optionally, a profile name can be specified after the MAC address.

Telnet path: /Setup/WLAN-Management

Possible values:

- Syntax: Do accept-AP [-c] <WTP-MAC> [<Profile>]
- -c: Do not generate config entry

Default: Blank

2.37.9 Disconnect AP

Do command to disconnect APs. The MAC address must be specified as a parameter.

Telnet path: /Setup/WLAN-Management

Possible values:

- Syntax: Do Disconnect-AP <WTP-MAC>

Default: Blank

2.37.5 CAPWAP port

Port number for the CAPWAP service

Telnet path: /Setup/WLAN-Management

Possible values:

■ 0 to 65535

Default: 1027



Cannot be configured with LANconfig

2.37.8 Provide default configuration

This enables the WLAN controller to assign a default configuration to every new (i.e. those without a valid certificate) even if no explicit configuration has been stored for it. In combination with auto-accept, the WLAN controller can accept all managed-mode access points which are found in the WLAN infrastructure managed by it (up to the maximum number of access points that can be managed by one).

Telnet path: /Setup/WLAN-Management

Possible values:

■ Yes

■ No

Default: No



This option can also lead to the acceptance of unintended access points into the WLAN infrastructure. For this reason this option should only be activated during the start-up phase when setting up a centrally managed WLAN infrastructure.

2.37.31 Interval for status table cleanup

The WLAN controller regularly cleans up the status tables for the background scans and for the wireless clients. During this cleanup, the WLAN controller removes all entries that are older than the interval in minutes defined here.

Telnet path: /Setup/WLAN-Management/Interval-for-status-table-cleanup

Possible values:

■ Max. 11 numerical characters

Default: 1440 minutes

2.37.33 License limit

This value indicates the maximum possible number of licenses for the WLAN controller that you can use on this device.

Telnet path: /Setup/WLAN-Management/License-limit



This value is for your information only. You cannot change it.

2.37.32 License count

This value indicates the current number of licenses for the WLAN controller that you can use on this device.

Telnet path: /Setup/WLAN-Management/License-Count



This value is for your information only. You cannot change it.

2.37.19 Start automatic radio field optimization

Launches RF optimization automatically. Optimization may be limited to one AP by specifying its MAC address as a parameter.

Telnet path: /Setup/WLAN-Management

Possible values:

- Syntax: Do start-automatic-radio-field-optimization [<WTP-MAC>]

Default: Blank

2.37.30 Synch. WTP password

Activating this function sets the main device password for the access point each time it registers. This ensures that the password is synchronized with that of the WLAN controller. If this function is deactivated, the main device password will only be set if the access point has no password when it registers. Once a password is set, it will not be overwritten.

Telnet path: /Setup/WLAN-Management/Synch.-WTP-Password

Possible values:

- Yes
- No

Default: Yes

2.37.1 AP configuration

This menu contains the settings for the access point configuration.

Telnet path: /Setup/WLAN-Management

Default: Blank

2.37.1.7 Control connection encryption default

Encryption of communications over the control channel. Without encryption the control data is exchanged as plain text. In both cases authentication is by certificate.

Telnet path: /Setup/WLAN-management/AP-configuration

Possible values:

- DTLS
- No

Default: DTLS (1)

2.37.1.8 Country default

The country in which the access points are to be operated. This information is used to define country-specific settings such as the permitted channels, etc.

Telnet path: /Setup/WLAN-management/AP-configuration

Possible values:

- Albania
- Argentina
- Australia
- Austria
- Bahrain
- Bangladesh
- Belarus
- Belgium
- Bosnia-Herzegovina
- Brazil
- Brunei-Daressalam
- Bulgaria
- Canada

- Chile
- China
- Colombia
- Costa- Rica
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Ecuador
- Egalistan
- Egypt
- Estonia
- Finland
- France
- Germany
- Ghana
- Greece
- Guatemala
- Honduras
- Hong- Kong
- Hungary
- Iceland
- India
- Indonesia
- Ireland
- Israel
- Italy
- Japan
- Jordan
- South Korea
- Kuwait
- Latvia
- Lebanon
- Liechtenstein
- Lithuania
- Luxembourg
- Macao
- Macedonia
- Malaysia
- Malta
- Mexico
- Moldavia
- Morocco
- Netherlands
- New Zealand
- Nicaragua
- Norway
- Oman
- Pakistan
- Panama
- Paraguay
- Peru

- Philippines
 - Poland
 - Portugal
 - Puerto-Rico
 - Qatar
 - Romania
 - Russia
 - Saudi Arabia
 - Singapore
 - Slovakia
 - Slovenia
 - South Africa
 - Spain
 - Sweden
 - Switzerland
 - Taiwan
 - Tanzania
 - Thailand
 - Tunisia
 - Turkey
 - Uganda
 - Ukraine
 - United Arab Emirates
 - Great Britain
 - United States FCC
 - Uruguay
 - Venezuela
- Default:** Germany (276)

2.37.1.5 WLAN module 1 default

Frequency of the first WLAN module. This parameter can also be used to deactivate the WLAN module.

Telnet path: /Setup/WLAN-management/AP-configuration

Possible values:

- 2.4GHz
- 5GHz
- Off

Default: 2.4GHz

2.37.1.6 WLAN module 2 default

Frequency of the second WLAN module. This parameter can also be used to deactivate the WLAN module.

Telnet path: /Setup/WLAN-management/AP-configuration

Possible values:

- 2.4GHz
- 5GHz
- Off

Default: 5GHz

2.37.1.1 Network profiles

Here you define the logical WLAN networks for activation and operation via the associated access points (APs).

Telnet path: /Setup/WLAN-management/AP-configuration

2.37.1.1.1 Name

Name of the logical WLAN network under which the settings are saved. This name is only used for internal administration of logical networks.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

■ Max. 31 ASCII characters

Default: Blank

2.37.1.1.2 Parent name

A LANCOM WLAN controller is capable of managing a large number of different access points at different locations. However, WLAN profiles include settings that are not equally suitable for every type of access point that can be managed. For example, there are differences between the country settings and the device properties.

In order to avoid having to maintain multiple redundant WLAN profiles to cater for different countries or device types, it is possible for the logical WLAN networks to "inherit" properties from other entries.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

■ Max. 31 ASCII characters

Default: Blank

2.37.1.1.3 Local values

Specifies which logical wireless LAN parameters are taken over during inheritance from the parent element. All non-inherited parameters can be set locally for this profile.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

■ Bit field as HEX number. Set bits specify the columns to be inherited. Select from the list of logical WLAN networks (GUI).

Default: All values are taken over from parent elements.

2.37.1.1.21 SSID

Define a unique SSID (the network name) for each of the logical wireless LANs required. Only WLAN clients that have the same SSID can register with this wireless network.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

■ Max. 32 characters

Default: BLANK

2.37.1.1.4 Operating

Switches the logical WLAN on or off separately.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

■ On

■ Off

Default: On

2.37.1.1.30 VLAN mode

This item allows you to select the VLAN mode for this WLAN network (SSID).

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- tagged: The access point marks the packets of this SSID with the ID configured under 2.37.1.1.34 VLAN ID.
- untagged: The access point forwards the packets of this SSID without any VLAN ID.

Default: untagged

The access point only uses the VLAN settings for the logical WLAN if you activate the VLAN module in the access point (in the physical WLAN parameters). The setting 'untagged' for a specific WLAN allows you to operate in a wireless LAN without VLAN, even if VLAN is otherwise activated.

2.37.1.1.5 VLAN-ID

VLAN ID for this logical WLAN network

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles**Possible values:**

- 0 to 4094

Default: 0**Special values:** 0: Switches off the use of VLAN with this WLAN network.

0

2.37.1.1.6 Encryption

Selects the encryption method and, for WEP, the key length that is to be used to encrypt data packets on the WLAN.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles**Possible values:**

- 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
- None

Default: 802.11i-WPA-PSK (0)

Please consider that not all wireless cards support all encryption methods.

2.37.1.1.7 WPA1 session key type

Here you select the methods which are to be made available for generating WPA session keys and group key. There is a choice of the Temporal Key Integrity Protocol (TKIP), the Advanced Encryption Standard (AES), or both.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles**Possible values:**

- TKIP/AES
- AES
- TKIP

Default: TKIP/AES**2.37.1.1.27 WPA2 session key types**

Here you select the methods which are to be made available for generating WPA session keys and group key. There is a choice of the Temporal Key Integrity Protocol (TKIP), the Advanced Encryption Standard (AES), or both.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles**Possible values:**

- TKIP/AES
- AES
- TKIP

Default: TKIP/AES

2.37.1.1.8 WPA version

Data in this logical WLAN will be encrypted with this WPA version.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- WPA1/2
- WPA1
- WPA2

Default: WPA1/2 (0)

2.37.1.1.9 Key

You can enter the key or passphrase as an ASCII character string. An option for WEP is to enter a hexadecimal number by adding a leading '0x'. The following lengths result for the formats used: Method, length WPA-PSK 8-63 ASCII characters WEP152 (128 bit) 16 ASCII or 32 HEX characters WEP128 (bit 104) 13 ASCII or 26 HEX characters WEP64 (bit 40) 5 ASCII or 10 HEX characters

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- ASCII character string or hexadecimal number

Default: Blank

2.37.109.1 Radio band

Selecting the frequency band determines whether the wireless LAN adapter operates in the 2.4 GHz or 5 GHz band, which in turn determines the available radio channels.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- 2.4GHz/5GHz
- 2.4GHz
- 5GHz

Default: 2.4GHz/5GHz

2.37.1.1.11 Continuation

The time in minutes that a managed-mode access point continues to operate in its current configuration.

The configuration is provided to the access point by the WLAN controller and is optionally stored in flash memory (in an area that is not accessible to LANconfig or other tools). Should the connection to the WLAN controller be interrupted, the access points will continue to operate with the configuration stored in flash for the time period entered here. The access point can also continue to work with this flash configuration after a local power outage.

If there is still no connection to the WLAN controller after this time period has expired then the flash configuration is deleted and the access point goes out of operation. As soon as the WLAN controller can be reached again, the configuration is transmitted again from the WLAN controller to the access point.

This option enables an access point to continue operating even if the connection to the WLAN controller is temporarily interrupted. Furthermore this represents an effective measure against theft as all security-related configuration parameters are automatically deleted after this time has expired.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- 0 to 9999

Default: 0

Special values: 0: Switches the WLAN module off the moment that the connection to the Controller is lost. With this setting, the configuration provided by the WLAN controller is not stored in flash memory but in RAM, meaning that a power outage causes the configuration to be lost immediately.

9999: Continues working indefinitely with the current configuration, even if the WLAN controller is permanently unavailable. The WLAN configuration in the flash memory is only deleted after a reset.



All other WLAN network parameters correspond to those for the standard configuration of access points.



If the access point establishes a backup connection to a secondary WLAN controller, then the countdown to the expiry of standalone operation is halted. The access point and its WLAN networks remain active as long as it has a connection to a WLAN controller.



Please note that the configuration in flash memory is deleted only after expiry of the time for standalone operation, and not when the power is lost!

2.37.1.1.12 Min Tx rate

Normally the access point negotiates the data transmission speeds continuously and dynamically with the connected WLAN clients. The access point adjusts the transmission speeds to the reception conditions. As an alternative, you can set fixed values for the minimum transmission speed if you wish to prevent the dynamic speed adjustment.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- 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

Normally the access point negotiates the data transmission speeds continuously and dynamically with the connected WLAN clients. The access point adjusts the transmission speeds to the reception conditions. As an alternative, you can set fixed value for the maximum transmission speed if you wish to prevent the dynamic speed adjustment.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- 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 Basic rate

The defined broadcast rate should allow the slowest clients to connect to the WLAN even under poor reception conditions. A higher value should only be set here if all clients in this logical WLAN can be reached "faster".

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- 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 preamble

Normally, the clients in 802.11b mode negotiate the length of the preamble with the access point. "Long preamble" should only be set when the clients require this setting to be fixed.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- Auto
- Long

Default: Auto

2.37.1.1.16 MAC filter

The MAC addresses of the clients allowed to associate with an access point are stored in the MAC filter list. The 'MAC filter' switch allows the use of the MAC filter list to be switched off for individual logical networks.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- Yes
- No

Default: No



Use of the MAC filter list is required for logical networks in which the clients register via LEPS with an individual passphrase. The passphrase used by LEPS is also entered into the MAC filter list. The

MAC filter list is always consulted for registrations with an individual passphrase, even if this option is deactivated.

2.37.1.1.17 Client-bridge support

Whereas address adjustment allows only the MAC address of a directly connected device to be visible to the access point, client-bridge support provides transparency; all MAC addresses of the LAN stations behind the client stations are transferred.

Furthermore, the three MAC addresses usual in client mode are not used for this operating mode (in this example for server, access point and client station), but rather four addresses as with point-to-point connections (the fourth is the MAC address of the station in the LAN of the client station). The fully transparent connection of a LAN to the client station allows targeted transmission of data packets in the WLAN and hence functions such as TFTP downloads, initiated by a broadcast.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- Yes: Activates client-bridge support for this logical WLAN.
- No: Deactivates client-bridge support for this logical WLAN.
- Exclusive: Only accepts clients that also support the client-bridge mode.

Default: No



Client-bridge mode can only be used between two LANCOM devices.

2.37.1.1.18 Maximum stations

Here you set the maximum number of clients that may associate with this access point. Additional clients wanting to associate will be rejected.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- 0 to 65535

Default: 0

2.37.1.1.19 SSID broadcast

You can operate your wireless LAN either in public or private mode. A wireless LAN in public mode can be contacted by any mobile station in the area. Your wireless LAN is put into private mode by activating the closed network function. In this operation mode, mobile stations that do not know the network name (SSID) are excluded from taking part in the wireless LAN.

Activate the closed network mode if you wish to prevent WLAN clients using the SSID 'ANY' from registering with your network.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- Yes
- No

Default: Yes

2.37.1.1.22 Min. HT MCS

A specific MCS number denotes a unique combination from the modulation of the individual carriers (BPSK, QPSK, 16QAM, 64QAM), coding rate (i.e. proportion of error correction bits in the raw data) and number of spatial streams. 802.11n uses this term instead of the term "data rate" used in older wireless LAN standards because data rate is no longer an unambiguous description.

Selecting the MCS therefore specifies the minimum and maximum modulation parameters to be used. Within these limits, the appropriate MCS is selected when the connection is established depending on the current conditions and may be adapted during the connection if required. This also defines the maximum attainable data throughput. You can find a list with the values for the different MCS in the reference manual.

The first digit specifies the modulation parameters for one spatial stream, the second digit specifies the modulation parameters for two spatial streams.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- 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 the default setting the station automatically selects the best possible MCS for each stream, based on the conditions of each channel. If interference arises during operation and the channel conditions change, for example due to movement of the transmitter or signal deterioration, the MCS is dynamically adjusted to suit the new conditions.

2.37.1.1.23 Max. HT MCS

A specific MCS number denotes a unique combination from the modulation of the individual carriers (BPSK, QPSK, 16QAM, 64QAM), coding rate (i.e. proportion of error correction bits in the raw data) and number of spatial streams. 802.11n uses this term instead of the term "data rate" used in older wireless LAN standards because data rate is no longer an unambiguous description.

Selecting the MCS therefore specifies the minimum and maximum modulation parameters to be used. Within these limits, the appropriate MCS is selected when the connection is established depending on the current conditions and may be adapted during the connection if required. This also defines the maximum attainable data throughput. You can find a list with the values for the different MCS in the reference manual.

The first digit specifies the modulation parameters for one spatial stream, the second digit specifies the modulation parameters for two spatial streams.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- 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 the default setting the station automatically selects the best possible MCS for each stream, based on the conditions of each channel. If interference arises during operation and the channel conditions change, for example due to movement of the transmitter or signal deterioration, the MCS is dynamically adjusted to suit the new conditions.

2.37.1.1.24 Short guard interval

This option is used to reduce the transmission pause between two signals from 0.8 μ s (default) to 0.4 μ s (short guard interval). This increases the effective time available for data transmission and thus the data throughput. However, the wireless LAN system becomes more liable to disruption that can be caused by interference between two consecutive signals.

The short guard interval is activated in automatic mode provided the operating conditions allow this. Alternatively the short guard mode can be switched off.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- Auto
- No

Default: Auto

2.37.1.1.25 Maximum spatial streams

The spatial multiplexing function allows several separate data streams to be transmitted over separate antennas in order to increase data throughput. The use of this function is only recommended when the remote device can process the data streams with corresponding antennas.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- Auto
- One
- Two

Default: Auto

Special values:

- **Auto:** With the 'Auto' setting all spatial streams that are supported by the wireless LAN module in question are used.

2.37.1.1.26 Send aggregates

Frame aggregation is used to combine several data packets (frames) into one large packet and transmit them together. This method serves to reduce the packet overhead, and the data throughput increases.

Frame aggregation is not suitable when working with mobile receivers or time-critical data transmissions such as voice over IP.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- Yes
- No

Default: Yes

2.37.1.1.28 RADIUS accounting activated

This is where you can activate RADIUS accounting for this logical WLAN network.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- Yes, No

Default: No



The access points supporting the logical WLAN network as configured by the WLAN controller must have an LCOS firmware version 8.00 or higher.

2.37.1.1.30 VLAN mode

This item allows you to select the VLAN mode for this WLAN network (SSID).

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- tagged: The access point marks the packets of this SSID with the ID configured under 2.37.1.1.34 VLAN ID.
- untagged: The access point forwards the packets of this SSID without any VLAN ID.

Default: untagged



The access point only uses the VLAN settings for the logical WLAN if you activate the VLAN module in the access point (in the physical WLAN parameters). The setting 'untagged' for a specific WLAN allows you to operate in a wireless LAN without VLAN, even if VLAN is otherwise activated.

2.37.1.1.32 Connect SSID to

Here you can select the logical interface used by the access point to transfer the payload data from this WLAN network (SSID).

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- LAN: The access point forwards payload data from this WLAN network via the bridge to its own local LAN interface. In this case, configure how the data packets are to be further processed by using appropriate routes directly on the access point, for example through a separate Internet connection.
- WLC-TUNNEL-1 to WLC-TUNNEL-x (model dependent): The access point forwards the payload data from this WLAN network via one of the virtual interfaces to the WLAN controller (WLC tunnel). In this case, configure how the data packets are to be further processed by using appropriate routes centrally on the WLAN controller, for example through a shared Internet connection.

Default: LAN



Forwarding payload data from multiple SSIDs to the WLAN controller increases the CPU load and bandwidth demands of the central devices. Consider the performance requirements of central WLAN management that uses layer-3 tunneling.



For each access point you can connect up to 7 SSIDs with a WLC tunnel. For each access point, the WLAN controller connects the WLC tunnel and its associated SSID to an available bridge group. Since one of the eight available bridge groups is reserved for other purposes, 7 bridge groups remain for assigning the WC-tunnel.

2.37.1.1.33 Inter-station traffic

Depending on the application, it may be required that the WLAN clients connected to an access point can—or expressly cannot—communicate with other clients. The setting that decides whether clients within an SSID can exchange data with one another has to be set separately for each logical WLAN.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- Yes
- No

Default: Yes

2.37.1.1.34 VLAN ID

This item allows you to set the VLAN ID for this logical WLAN network. When the VLAN mode is set to 'tagged', the access point transmits the data from this WLAN network (SSID) with the VLAN ID set here.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- 2 to 4094

Default: 2

2.37.1.10 Predef. intranets

This table lists the predefined AP intranets.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Predef.-Intranets



The settings for the predefined intranets are used exclusively for internal communications between the device and LANconfig. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.37.1.10.1 Name

This is the name of the predefined AP intranet.

Telnet path: /Setup/WLAN-Management/AP-Configuration/WLAN-Module-2-Default/Name



The settings for the predefined intranets are used exclusively for internal communications between the device and LANconfig. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

2.37.1.2 Radio profiles

Here you define the physical WLAN parameters which apply to all of the logical WLAN networks that share a managed access point.

Telnet path: /Setup/WLAN-management/AP-configuration

2.37.1.2.1 Name

Unique name for this combination of physical WLAN parameters.

Telnet path: /Setup/WLAN management/AP-Configuration/Radioprofiles

Possible values:

■ Max. 31 ASCII characters

Default: Blank

2.37.1.2.10 DTIM period

This value defines the number of beacons which are collected before multicasts are broadcast. Higher values enable longer client sleep intervals, but worsen the latency times.

Telnet path: /Setup/WLAN management/AP-Configuration/Radioprofiles

Possible values:

■ 0 to 255

Default: 0

2.37.1.2.11 Background scan

In order to identify other access points within the device's local radio range, the LANCOM Wireless router can record the beacons received (management frames) and store them in the scan table. Since this recording occurs in the background in addition to the access points' "normal" radio activity, it is called a "background scan".

If a value is entered here, the LANCOM wireless router searches the active band for currently unused frequencies to find available access points. This value is the time interval between search cycles.

LANCOM wireless routers in access point mode normally use the background scan function for rogue AP detection. This scan interval should correspond to the time span within which rogue access points should be recognized, e.g. 1 hour.

Conversely, LANCOM wireless routers in client mode generally use the background scan function to improve mobile WLAN client roaming. In order to achieve fast roaming, the scan time is limited here, for example, to 260 seconds.

Telnet path: /Setup/WLAN management/AP-Configuration/Radioprofiles

Possible values:

■ 0 to 4294967296

Default: 0

Special values: 0: When the background scan time is '0' the background scanning function is deactivated.

2.37.1.2.12 Antenna gain

Where the transmission power of an antennae exceeds the levels permitted in the country of operation, the power must be attenuated accordingly.

The field 'Antenna gain' is for the gain of the antenna minus the actual cable loss. This value for true antenna gain is dynamically used to calculate and emit the maximum permissible power with regards to other parameters such as country, data rate and frequency band.

In contrast to this, the entry in the field 'Tx power reduction' causes a static reduction in the power by the value entered, and ignores the other parameters. .

Telnet path: /Setup/WLAN management/AP-Configuration/Radioprofiles

Possible values:

- Minus 128 to 127

Default: 0**2.37.1.2.13 Tx power reduction**

In contrast to antenna gain, the entry in the field 'Tx power reduction' causes a static reduction in the power by the value entered, and ignores the other parameters.

Telnet path: /Setup/WLAN management/AP-Configuration/Radioprofiles**Possible values:**

- 0 to 255

Default: 0

The transmission power reduction simply reduces the emitted power. The reception sensitivity (reception antenna gain) remains unaffected. This option is useful, for example, where large distances have to be bridged by radio when using shorter cables. The reception antenna gain can be increased without exceeding the legal limits on transmission power. This leads to an improvement in the maximum possible range and, in particular, the highest possible data transfer rates.

2.37.1.2.14 Mgmt-VLAN-Id

VLAN ID for the management network.

Telnet path: /Setup/WLAN management/AP-Configuration/Radioprofiles**Possible values:**

- 0 to 4094

Default: 0**Special values:** 0: Switches the use of VLAN off.

1: Switches the use of VLAN on; the management network remains untagged, however.

2 to 4094: Switches the use of VLAN on; the management network uses the VLAN ID set here.



All other physical WLAN parameters correspond to those for the standard configuration of access points.



The Management VLAN ID must (!) be set to a value not equal to zero so that VLANs can be used over the WLAN networks. This also applies when the management network itself is not to be tagged with VLAN IDs (Mgmt-VLANID=1). VLAN activation only applies to WLAN networks which are connected by means of these physical WLAN parameters.

2.37.1.2.16 Indoor-only operation

You can specify whether indoor-operation only is to be allowed.

Telnet path: /Setup/WLAN-Management/AP-Configuration/WLAN-Module-2-Default/Indoor-Only-Operation**Possible values:**

- Yes
- No

Default: No**2.37.1.2.2 Parent name**

A LANCOM WLAN controller is capable of managing a large number of different access points at different locations. However, WLAN profiles include settings that are not equally suitable for every type of access point that can be managed. For example, there are differences between the country settings and the device properties.

In order to avoid having to maintain multiple redundant WLAN profiles to cater for different countries or device types, it is possible for the physical WLAN parameters to "inherit" properties from other entries.

Telnet path: /Setup/WLAN management/AP-Configuration/Radioprofiles**Possible values:**

- Max. 31 ASCII characters

Default: Blank

2.37.1.2.3 Local values

Specifies which physical wireless LAN parameters are taken over during inheritance from the parent element. All non-inherited parameters can be set locally for this profile.

Telnet path: /Setup/WLAN management/AP- Configuration/Radioprofiles

Possible values:

- Bit field as HEX number. Set bits specify the columns to be inherited. Select from the list of logical WLAN networks (GUI).

Default: All values are taken over from parent elements.

2.37.1.2.4 Country

The device needs to be set with the country where it is operating in order for the WLAN to use the parameters approved for the location.

Telnet path: /Setup/WLAN management/AP- Configuration/Radioprofiles

Possible values:

- Albania
- Argentina
- Australia
- Austria
- Bahrain
- Bangladesh
- Belarus
- Belgium
- Bosnia-Herzegovina
- Brazil
- Brunei-Daressalam
- Bulgaria
- Canada
- Chile
- China
- Colombia
- Costa-Rica
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Ecuador
- Egalistan
- Egypt
- Estonia
- Finland
- France
- Germany
- Ghana
- Greece
- Guatemala
- Honduras
- Hong-Kong
- Hungary
- Iceland
- India

- Indonesia
- Ireland
- Israel
- Italy
- Japan
- Jordan
- South Korea
- Kuwait
- Latvia
- Lebanon
- Liechtenstein
- Lithuania
- Luxembourg
- Macao
- Macedonia
- Malaysia
- Malta
- Mexico
- Moldavia
- Morocco
- Netherlands
- New Zealand
- Nicaragua
- Norway
- Oman
- Pakistan
- Panama
- Paraguay
- Peru
- Philippines
- Poland
- Portugal
- Puerto-Rico
- Qatar
- Romania
- Russia
- Saudi Arabia
- Singapore
- Slovakia
- Slovenia
- South Africa
- Spain
- Sweden
- Switzerland
- Taiwan
- Tanzania
- Thailand
- Tunisia
- Turkey
- Uganda
- Ukraine
- United Arab Emirates

- Great Britain
- United States FCC
- Uruguay
- Venezuela

Default: Default

Special values: Default: Makes use of the encryption method defined in the 'Options' area.

2.37.1.2.5 Channel list

As standard the access points can use all of the channels permitted in the country of operation. To limit the selection to certain channel, the desired channels can be entered here as a comma-separated list. Ranges can also be defined (e.g. '7–9').

Telnet path: /Setup/WLAN management/AP-Configuration/Radioprofiles

Possible values:

- Comma-separated list with max. 48 characters

Default: Blank

2.37.1.2.6 2.4- GHz mode

In the 2.4 GHz band, there are two different wireless standards: The IEEE 802.11b standard with a transmission speed of up to 11 Mbps and the IEEE 802.11g standard offering up to 54 Mbps. If 2.4 GHz is selected as the operating frequency, the transmission speed can be selected in addition.

The 802.11g/b compatibility mode offers the highest possible speeds and yet also offers the 802.11b standard so that slower clients are not excluded. In this mode, the WLAN card in the access point principally works with the faster standard and falls back on the slower mode should a client of this type log into the WLAN. In the '2Mbit compatible' mode, the access point supports older 802.11b cards with a maximum transmission speed of 2 Mbps.

Telnet path: /Setup/WLAN management/AP-Configuration/Radioprofiles

Possible values:

- 11bg mixed
- 11b only
- 11g only
- 108Mbps
- 11bgn mixed
- 11gn mixed
- Greenfield

Default: 11bg mixed (0)



Please observe that clients supporting only the slower standards may not be able to register with the WLAN if the speeds set here are higher.

2.37.1.2.7 5GHz mode

Using two neighboring, vacant channels for wireless transmissions can increase the transfer speeds in Turbo Mode up to 108 Mbps.

Telnet path: /Setup/WLAN management/AP-Configuration/Radioprofiles

Possible values:

- Normal
- 108Mbps
- 11an mixed
- Greenfield

Default: Normal

2.37.1.2.8 Subbands

In the 5-GHz band, it is also possible to select a subband, which is linked to certain radio channels and maximum transmission powers.

Telnet path: /Setup/WLAN management/AP-Configuration/Radioprofiles

Possible values:

- 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**

With the extension to the 802.11 standard, 802.11e, Quality of Service can be provided for transfers via WLAN. Among others, 802.11e supports the prioritization of certain data-packet types. This extension is an important basis for the use of voice applications in WLANs (Voice over WLAN, VoWLAN). The WiFi alliance certifies products that support Quality of Service according to 802.11e, and refer to WMM (WiFi Multimedia, formerly known as WME or Wireless Multimedia Extension). WMM defines four categories (voice, video, best effort and background) which make up separate queues to be used for prioritization. The 802.11e standard sets priorities by referring to the VLAN tags or, in the absence of these, by the DiffServ fields of IP packets. Delay times (jitter) are kept below 2 milliseconds, a magnitude which is inaudible to the human ear. 802.11e controls access to the transfer medium with EDCF, the Enhanced Distributed Coordination Function.

Telnet path: /Setup/WLAN management/AP-Configuration/Radioprofiles**Possible values:**

- Yes
- No

Default: No

Priorities can only be set if the WLAN client and the access point both support 802.11e or WMM, and also if the applications are able to mark the data packets with the corresponding priorities.

2.37.1.2.17 Activate VLAN module of managed APs

Use this item to activate or deactivate the VLAN module in the managed access points. If VLAN is switched off, all VLAN settings in the logical network are ignored.

Telnet path: /Setup/WLAN management/AP-Configuration/Radioprofiles**Possible values:**

- Yes
- No

Default: No**2.37.1.2.18 Management VLAN mode**

VLAN mode for the management network. VLAN is only used if the VLAN module in the access point is enabled. The management network can be operated untagged even if VLAN is activated.

Telnet path: /Setup/WLAN management/AP-Configuration/Radioprofiles**Possible values:**

- untagged: The access point's management packets are not marked with a VLAN ID.
- tagged: The access point's management packets are marked with the VLAN ID that is configured in this radio profile as the management VLAN ID.

Default: untagged**2.37.1.2.14 Management VLAN ID**

VLAN ID for the management network. The management VLAN ID is used for tagging the management network which is used for communications between the WLAN controller and the access points. VLAN is only used if the VLAN module in the access point is enabled. The management network can be operated without tagging even if VLAN is enabled by selecting the corresponding setting for the management VLAN mode. The VLAN ID '1' is reserved internally for this.

Telnet path: /Setup/WLAN management/AP-Configuration/Radioprofiles

Possible values:

■ 2 to 4094

Default: 2

2.37.1.3 Common profiles

Here you define entire WLAN profiles that summarize all of the WLAN settings which can be used on the managed APs. This includes for example up to 16 logical WLAN networks and a set of physical WLAN parameters.

Telnet path: /Setup/WLAN-management/AP-configuration

2.37.1.3.1 Name

Name of the profile under which the settings are saved.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Commonprofiles

Possible values:

■ Max. 31 ASCII characters

Default: Blank

2.37.1.3.2 Networks

List of the logical WLAN networks that are assigned via this profile.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Commonprofiles

Possible values:

■ Max. 251 ASCII characters, multiple values separated by commas.

Default: Blank



From this list, access points use only the first eight entries that are compatible with their own hardware. This means that eight WLAN networks for purely 2.4-GHz operations and eight for purely 5-GHz operations can be defined in a profile. Consequently, each LANCOM access point—be it a model offering 2.4-GHz or 5-GHz support—can choose from a maximum of eight logical WLAN networks.

2.37.1.3.3 AP parameters

A set of physical parameters to be used by the access point WLAN modules.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Commonprofiles

Possible values:

■ Select from the list of physical WLAN parameters (GUI) or max. 31 ASCII characters

Default: Blank

2.37.1.3.4 Controller

A list of WLAN controllers that the access points should attempt to connect with. The access point starts searching for a WLAN controller with a broadcast. Defining alternative WLAN controllers is worthwhile when a broadcast cannot reach all WLAN controllers (e.g. if the WLAN controller is located in another network).

Telnet path: /Setup/WLAN-Management/AP-Configuration/Commonprofiles

Possible values:

■ IP addresses, multiple values separated by commas. Maximum 159 characters, i.e. 9 to 10 entries depending on the length of the IP addresses.

Default: Blank

2.37.1.4 Access points

Here you define the access points that are to be managed from this WLAN Controller (WLC). At the same time you assign the WLAN profile to the AP.

Telnet path: /Setup/WLAN-management/AP-configuration

2.37.1.4.1 MAC address

MAC address of the access point

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access-Points

Possible values:

■ Valid MAC address

Default: Blank

Special values: FFFFFFFF: Defines the default configuration

2.37.1.4.2 Name

Name of the access point in managed mode.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access-Points

Possible values:

■ Max. 16 ASCII characters

Default: Blank

2.37.1.4.3 Location

Location of the access point in managed mode.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access-Points

Possible values:

■ Max. 251 ASCII characters

Default: Blank

2.37.1 Operating

Activates or deactivates this entry.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access-Points

Possible values:

■ Yes

■ No

Default: Yes

2.37.1.4.4 Profile

This entry sets the WLAN profile that is to be used by this access point.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access-Points

Possible values:

■ Select from the list of defined WLAN profiles, max. 31 ASCII characters.

Default: Blank

2.37.1.4.6 Control connection encryption

Encryption of communications over the control channel. Without encryption the control data is exchanged as plain text. In both cases authentication is by certificate.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access-Points

Possible values:

■ default

■ DTLS

■ No

Default: Default

Special values: Default: Makes use of the encryption method defined in the 'Options' area.

2.37.1.4.7 WLAN module 1

Frequency of the first WLAN module. This parameter can also be used to deactivate the WLAN module.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access-Points

Possible values:

- default
- 2.4 GHz
- 5 GHz
- Off

Default: Default

Special values: Default: Makes use of the encryption method defined in the 'Options' area.

2.37.1.4.15 Allow 40MHz

A wireless LAN module normally uses a frequency range of 20 MHz in which data to be transmitted is modulated to the carrier signals. 802.11a/b/g use 48 carrier signals in a 20MHz channel. The use of double the frequency range of 40 MHz means that 96 carrier signals can be used, resulting in a doubling of the data throughput.

802.11n can use 52 carrier signals in one 20 MHz channel for modulation and up to 108 in a 40 MHz channel. The use of the 40 MHz option for 802.11n therefore means a performance gain of more than double.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access-Points

Possible values:

- Auto
- No

Default: Auto

2.37.1.4.16 Antenna mask

LANCOM access points with 802.11 support can use up to three antennas for transmitting and receiving data. Depending on the application the use of the antennas can be set.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access-Points

Possible values:

- 1+2+3: When using the device in access point mode to connect wireless LAN clients it is generally recommended to use all three antennas in parallel in order to achieve good network coverage.
- 1+3: Antenna ports 1 and 3 are used for 2 parallel data streams for example in point to point connections with an appropriate dual slant antenna. The third antenna port is deactivated.
- 1: For applications with only one antenna (for example an outdoor application with just one antenna) the antenna is connected to port 1 and ports 2 and 3 are deactivated
- Auto: Automatic antenna selection

Default: Auto

Special values: Auto: The 'Auto' setting means that all available antennas are used.

2.37.1.4.9 Module 1 channel list

The radio channel selects a portion of the conceivable frequency band for data transfer.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access-Points

Possible values:

- Comma-separated list with max. 48 characters

Default: Blank



In the 2.4-GHz band, two separate wireless networks must be at least three channels apart to avoid interference.

2.37.1.4.20 Module 1 ant. gain

This item allows you to specify the antenna gain factor (in dBi) minus attenuation of the cable and (if applicable) lightning protection. Based on this, and depending on the country where the system is operated and the frequency band, the base station calculates the maximum permitted transmission power.

If the field is left blank, the default setting defined in the configuration profile of relevant WLAN profile will be used.

Transmission power can be reduced to a minimum of 0.5 dBm in the 2.4-GHz band or 6.5 dBm in the 5-GHz band. This limits the maximum value that can be added to 17.5 dBi in the 2.4-GHz band and 11.5 dBi in the 5-GHz band. Please ensure that your combination of antenna, cable and lightning-protection complies with the legal requirements of the country where the system is operated.

The receiver's sensitivity is unaffected by this.

Example: AirLancer O-18a: Antenna gain: 18dBi, cable attenuation: 4dB --> Value to be entered = 18dBi - 4dB = 14dBi.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access Points/Module-1-Ant.-Gain

Possible values:

■ 0 to 999 dBi

Default: Blank



The current transmission power is displayed by the device's web interface or by telnet under 'Status->WLAN statistics->WLAN parameters->Transmission power' or with LANconfig under 'System information->WLAN card->Transmission power'.

2.37.1.4.22 Module 1 TX reduct.

If you use an antenna with a high amplification factor, you can use this entry to attenuate the transmission power of your base station to the transmission power permitted in your country in the frequency band in question.

If the field is left blank, the default setting defined in the configuration profile of relevant WLAN profile will be used.

Transmission power can be reduced to a minimum of 0.5 dBm in the 2.4-GHz band or 6.5 dBm in the 5-GHz band. This limits the maximum value that can be added to 17.5 dBi in the 2.4-GHz band and 11.5 dBi in the 5-GHz band. Please ensure that your combination of antenna, cable and lightning-protection complies with the legal requirements of the country where the system is operated.

The receiver's sensitivity is unaffected by this.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access-Points

Possible values:

■ 0 to 999 dBi

Default: Blank



The current transmission power is displayed by the device's web interface or by telnet under 'Status->WLAN statistics->WLAN parameters->Transmission power' or with LANconfig under 'System information->WLAN card->Transmission power'.

2.37.1.4.8 WLAN module 2

Frequency of the second WLAN module. This parameter can also be used to deactivate the WLAN module.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access-Points

Possible values:

■ default

■ 2.4 GHz

■ 5 GHz

■ Off

Default: Default

Special values: Default: Makes use of the encryption method defined in the 'Options' area.

2.37.1.4.20 Module 2 ant. gain

This item allows you to specify the antenna gain factor (in dBi) minus attenuation of the cable and (if applicable) lightning protection. Based on this, and depending on the country where the system is operated and the frequency band, the base station calculates the maximum permitted transmission power.

If the field is left blank, the default setting defined in the configuration profile of relevant WLAN profile will be used.

Transmission power can be reduced to a minimum of 0.5 dBm in the 2.4-GHz band or 6.5 dBm in the 5-GHz band. This limits the maximum value that can be added to 17.5 dBi in the 2.4-GHz band and 11.5 dBi in the 5-GHz band. Please ensure that your combination of antenna, cable and lightning-protection complies with the legal requirements of the country where the system is operated.

The receiver's sensitivity is unaffected by this.

Example: AirLancer O-18a: Antenna gain: 18dBi, cable attenuation: 4dB --> Value to be entered = 18dBi - 4dB = 14dBi.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access Points/Module-2-Ant.-Gain

Possible values:

■ 0 to 999 dBi

Default: Blank



The current transmission power is displayed by the device's web interface or by telnet under 'Status->WLAN statistics->WLAN parameters->Transmission power' or with LANconfig under 'System information->WLAN card->Transmission power'.

2.37.1.4.10 Module 2 channel list

The radio channel selects a portion of the conceivable frequency band for data transfer.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access-Points

Possible values:

■ Comma-separated list with max. 48 characters

Default: Blank



In the 2.4-GHz band, two separate wireless networks must be at least three channels apart to avoid interference.

2.37.1.4.22 Module 2 TX reduct.

If you use an antenna with a high amplification factor, you can use this entry to attenuate the transmission power of your base station to the transmission power permitted in your country in the frequency band in question.

If the field is left blank, the default setting defined in the configuration profile of relevant WLAN profile will be used.

Transmission power can be reduced to a minimum of 0.5 dBm in the 2.4-GHz band or 6.5 dBm in the 5-GHz band. This limits the maximum value that can be added to 17.5 dBi in the 2.4-GHz band and 11.5 dBi in the 5-GHz band. Please ensure that your combination of antenna, cable and lightning-protection complies with the legal requirements of the country where the system is operated.

The receiver's sensitivity is unaffected by this.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access-Points

Possible values:

■ 0 to 999 dBi

Default: Blank



The current transmission power is displayed by the device's web interface or by telnet under 'Status->WLAN statistics->WLAN parameters->Transmission power' or with LANconfig under 'System information->WLAN card->Transmission power'.

2.37.1.4.12 IP address

Static IP address for the AP if DHCP cannot be /should not be used.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access-Points

Possible values:

- Valid IP address.

Default: Blank

2.37.1.4.13 Netmask

Static netmask if DHCP cannot be /should not be used.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access-Points

Possible values:

- Valid IP address.

Default: Blank



Cannot be configured with LANconfig

2.37.1.4.14 Gateway

Static IP address of the gateway if DHCP cannot be /should not be used.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access-Points

Possible values:

- Valid IP address.

Default: Blank



Cannot be configured with LANconfig

2.37.1.4.17 AP intranet

This references a line in the AP intranet table.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access-Points

Possible values:

- Max. 31 ASCII characters

Default: Blank

2.37.1.4.18 Manage firmware

This allows the automatic firmware upload to be disabled for this AP. This is also automatically disabled by the controller in the case of certain errors. The reason for automatic deactivation is displayed in the column "Manage firmware additional information".

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access-Points

Possible values:

- Yes
- No

Default: Yes



Cannot be configured with LANconfig

2.37.1.4.19 Manage firmware additional information

This allows the automatic firmware upload to be disabled for this AP. This is also automatically disabled by the controller in the case of certain errors. The reason for automatic deactivation is displayed in the column "Manage firmware additional information".

Telnet path: /Setup/WLAN-Management/AP-Configuration/Access-Points

Possible values:

- Blank
- Disabled_due_to_error_during_update
- Disabled_by_manual_upload

Default: Blank



Cannot be configured with LANconfig

2.37.1.9 MAC address

If necessary, define IP parameter profiles here for use in the access point table if certain access points have IP addresses that were not assigned by DHCP.

Telnet path: /Setup/WLAN-management/AP-configuration

2.37.1.9.1 Name

Name of the intranet where APs are operated. This name is only used for internal administration of intra-networks.

Possible values:

- Max. 31 ASCII characters

Default: Blank

2.37.1.9.2 Parent name

A LANCOM WLAN controller is capable of managing a large number of different access points at different locations. However, WLAN profiles include settings that are not equally suitable for every type of access point that can be managed. For example, there are differences between the country settings and the device properties.

In order to avoid having to maintain multiple redundant WLAN profiles, it is possible for the intranets to "inherit" selected properties from other entries.

Possible values:

- Max. 31 ASCII characters

Default: Blank

2.37.1.9.3 Local values

Specifies which intranet parameters are taken over during inheritance from the parent element. All non-inherited parameters can be set locally for this profile.

Possible values:

- Bit field as HEX number. Set bits specify the columns to be inherited. Select from the list of intranets (GUI).

Default: 0

2.37.1.9.4 Domain name

Domain name used by the access point when resolving WLC addresses.

Possible values:

- Max. 63 ASCII characters

Default: Blank

2.37.1.9.5 Netmask

Static netmask if DHCP cannot be /should not be used.

Possible values:

- Valid IP address.

Default: Blank

2.37.1.9.6 Gateway

Static IP address of the gateway if DHCP cannot be /should not be used.

Possible values:

- Valid IP address.

Default: Blank

2.37.1.9.7 Primary DNS server

Static IP address of the first DNS server if DHCP cannot be /should not be used.

Possible values:

- Valid IP address.

Default: Blank

2.37.1.9.8 Secondary DNS server

Static IP address of the second DNS server if DHCP cannot be /should not be used.

Possible values:

- Valid IP address.

Default: Blank

2.37.1.12 DSCP for control packets

This item allows you to set the prioritization of control packets by DiffServ (Differentiated Services).

Telnet path: /Setup/WLAN-management/AP-configuration

Possible values:

- 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 for data packets

This item allows you to set the prioritization of data packets by DiffServ (Differentiated Services).

Telnet path: /Setup/WLAN-management/AP-configuration

Possible values:

- 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 networks

This table contains the settings for the transmission of CAPWAP multicast packets over the bridge interfaces. When a WLAN controller receives a broadcast or multicast packet from a network belonging to a certain SSID, it has to forward this packet to all access points that work with that SSID. The WLAN controller has two ways to reach all of these access points:

- The WLAN controller copies the packet and sends it as a unicast to the relevant access points. The replication of packets increases the CPU load on the controller and the necessary bandwidths, which negatively impacts performance especially of WAN connections.
- The WLAN controller sends the packet as a multicast. In this case, a single packet only has to be transmitted. However, multicast packets sent from a controller only reach those access points in its own broadcast domain. Access points at the other end of a routed WAN link cannot receive multicast packets from the controller.



The forwarding of multicast packets depends on the routers operated on the WAN route.

The WLAN controller regularly sends keep-alive multicast packets to the multicast group. If an access point responds to these packets, the controller is able to reach this access point with multicast packets. For all other access points, the controller copies the multicast packets it receives and sends them as a unicast to the appropriate access points.

If the transmission of CAPWAP multicast packets has been activated and a valid multicast IP address with port has been defined for the bridge interface, the device forwards the incoming broadcast and multicast packets as a multicast to this address.

To ensure that the information about associated WLAN clients and their multicast group memberships is kept up to date even when they switch between access points, devices operating multicast simultaneously activate IGMP snooping for continuous updates to the information on multicast structure.

In applications featuring multiple WLAN controllers, multicast packets can lead to loops. In order to avoid loops due to multicasts when using the bridge, the WLAN controller applies the following measures:

- The WLAN controller ignores CAPWAP multicast packets. When working with a WLC data tunnel, the controller sends these packets as unicasts.
- The WLAN controller does not forward packets that carry a CAPWAP multicast address as the recipient.
- The WLAN controller automatically enables IGMP snooping on all managed access points if CAPWAP works with multicast.

2.37.1.14.1 Bridge interface

This item allows you to select a bridge interface for the multicast settings.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Multicast-Networks

Possible values:

- Select one of the defined bridge interfaces

2.37.1.14.2 Operating

This option activates or disables the use of CAPWAP multicast packets for this bridge interface.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Multicast-Networks

Possible values:

- Yes
- No

Default: No

2.37.1.14.3 Multicast address

Use this item to select an IP address to which the device sends CAPWAP multicast packets for the selected bridge interface.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Multicast-Networks

Possible values:

- Maximum 15 characters to define a valid IP address

Default: 233.252.124.1 to 233.252.124.32 (IP addresses from the unassigned range)

2.37.1.14.4 Multicast port

This item allows you to select a port for transmitting CAPWAP multicast packets over the selected bridge interface.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Multicast-Networks

Possible values:

- Maximum 5 numbers to define a valid port number

Default: 20000 to 20031

2.37.1.14.5 Loopback address

This is where you can configure an optional sender address to be used instead of the one otherwise automatically selected for the destination address.

If you have configured loopback addresses, you can specify them here as sender address.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Multicast-Networks

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LB0 to LBF for the 16 loopback addresses
- Any valid IP address

Default: 00.0.0



If the list of IP networks or loopback addresses contains an entry named 'DMZ' then the associated IP address will be used. Name of a loopback address.

2.37.10 Notification

This menu contains the configuration of the notification system of the WLAN management.

Telnet path: /Setup/WLAN-Management

2.37.10.1 E-mail

Activates notification by e-mail.

Telnet path: /Setup/WLAN-Management/Notification

Possible values:

- Yes
- No

Default: No

2.37.10.3 E-mail receiver

Information about events in the WLAN controller is sent to this e-mail address.

Telnet path: /Setup/WLAN-Management/Notification

Possible values:

- Valid e-mail address with up to 63 ASCII characters

Default: Blank



An SMTP account must be set up to make use of e-mail messaging.

2.37.10.5 Send SNMP trap for station table event

Here you specify when you receive information about events relating to entries in the station table.

Telnet path: /Setup/WLAN management/Notification/Send-SNMP-Trap-for-Station-Table-Event

Possible values:

- ☐ Add/remove_entry
- ☐ All_events

Default: Add/remove_entry

2.37.10.2 Syslog

Activates notification by SYSLOG.

Telnet path: /Setup/WLAN-Management/Notification

Possible values:

- ☐ Yes
- ☐ No

Default: No

2.37.10.4 Advanced

Here you define the events that you wish to be informed of.

Telnet path: /Setup/WLAN-Management/Notification

2.37.10.4.1 Name

Selects the events that trigger notification.

Telnet path: /Setup/WLAN-Management/Notification/Advanced

Possible values:

- ☐ E-mail
- ☐ Syslog

Default: Blank

Special values: Value is fixed

2.37.10.4.2 Active radios

Activates notification about active access points.

Telnet path: /Setup/WLAN-Management/Notification/Advanced

Possible values:

- ☐ Yes
- ☐ No

Default: No

2.37.10.4.3 Missing AP

Activates notification about lost access points.

Telnet path: /Setup/WLAN-Management/Notification/Advanced

Possible values:

- ☐ Yes
- ☐ No

Default: No

2.37.10.4.4 New AP

Activates notification about new access points.

Telnet path: /Setup/WLAN-Management/Notification/Advanced

Possible values:

- Yes
- No

Default: No

2.37.34 WLC cluster

This menu contains the settings for the data connections and status connections between multiple WLAN controllers.

Telnet path: /Setup/WLAN-Management

2.37.34.4 WLC discovery

This table allows you to enable or disable the automatic search for further WLCs separately for each IP network.

Telnet path: /Setup/WLAN-Management/WLC-Cluster

2.37.34.4.1 Network

Select one of the IP networks defined in the device, in which you want to automatically search for additional WLAN controllers.

Telnet path: /Setup/WLAN-Management/WLC-Cluster/WLC-Discovery**Possible values:**

- Select from the list of defined IP networks (maximum 16 characters).
- No

Default: INTRANET: no, DMZ: no

2.37.34.4.2 Operating

Use this option to enable or disable the automatic search for other WLAN controllers in the selected IP network.

Telnet path: /Setup/WLAN-Management/WLC-Cluster/WLC-Discovery**Possible values:**

- Yes
- No

Default: INTRANET: yes, DMZ: no

The automatic search for other WLAN controllers is one way of establishing the data tunnel between two WLCs. If you disable this option, the WLAN controller cannot automatically establish a data channel to another WLC over this network, even if the use of data tunnels in general has been enabled. As an alternative, you can define the remote sites in the static WLC list.

2.37.34.3 Static WLC list

This table is used to define additional WLAN controllers as remote sites to which a connection can be established. The controller initially establishes a control tunnel to this remote site. If you have activated the option for the data tunnel, the controller then automatically establishes a data tunnel to this remote site.

Telnet path: /Setup/WLAN-Management/WLC-Cluster

The two WLAN controllers can only establish a data tunnel when the devices meet the following requirements:

- You have defined the respective remote sites in both devices.
- Both controllers have a certificate from the same CA.

2.37.34.3.1 IP address

This item defines the IP address of another WLAN controller to which this controller can establish a data tunnel.

Telnet path: /Setup/WLAN-Management/WLC-Cluster/Static-WLC-List



The two WLAN controllers can only establish a data tunnel when the devices meet the following requirements:

- For both devices you have defined the respective remote sites, either statically or using the automatic search.
- Both controllers have a certificate from the same CA.

2.37.34.3.2 Loopback address

This is where you can configure an optional sender address to be used instead of the one otherwise automatically selected for the destination address.

If you have configured loopback addresses, you can specify them here as sender address.

Telnet path: /Setup/WLAN-Management/WLC-Cluster/Static-WLC-List

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LBO to LBF for the 16 loopback addresses
- Any valid IP address

Default: 00.0.0



If the list of IP networks or loopback addresses contains an entry named 'DMZ' then the associated IP address will be used. Name of a loopback address.

2.37.34.2 WLC data tunnel active

This option activates or disables the use of data tunnels between multiple WLAN controllers.

Telnet path: /Setup/WLAN-Management

Possible values:

- Yes
- No

Default: No

2.37.27 Central firmware management

This menu contains the configuration of central firmware management.

Telnet path: /Setup/WLAN-Management

2.37.27.15 Firmware version management

Table with device type, MAC address and firmware version for the precise control of the firmware files in use.

Telnet path: /Setup/WLAN-Management/Central-Firmware-Management

2.37.27.15.2 Device

Select here the type of device that the firmware version specified here is to be used for.

Telnet path: /Setup/WLAN-Management/Central-Firmware-Management/Firmware-Version-Management

Possible values:

- All, or a selection from the list of available devices.

Default: All devices

2.37.27.15.3 MAC address

Select here the device (identified by its MAC address) that the firmware version specified here is to be used for.

Telnet path: /Setup/WLAN-Management/Central-Firmware-Management/Firmware-Version-Management

Possible values:

- Valid MAC address

Default: Blank

2.37.27.15.4 Version

Firmware version that is to be used for the devices or device types specified here.

Telnet path: /Setup/WLAN-Management/Central-Firmware-Management/Firmware-Version-Management

Possible values:

- Firmware version in the form X.XX

Default: Blank

2.37.27.16 Script management

Table with the name of the script file and a WLAN profile for allocating the script to a WLAN profile.

Configuring a wireless router and access point in the "Managed" mode is handled via WLAN profiles. A script can be used for setting those detailed parameters in managed devices that are not handled by the pre-defined parameters in a WLAN profile. Distribution is also handled by WLAN profiles to ensure that the wireless routers and access points with the same WLC configuration also use the same script.

As only one script file can be defined per WLAN profile, versioning is not possible here. However, when distributing a script to a wireless router or access point, an MD5 checksum of the script file is saved. This checksum allows the WLAN Controller to determine whether the script file has to be transmitted again in case a new or altered script has the same file name.

Telnet path: /Setup/WLAN-Management/Central-Firmware-Management

2.37.27.16.1 Profile

Select here the WLAN profile that the script file specified here should be used for.

Telnet path: /Setup/WLAN-Management/Central-Firmware-Management/Script-Management

Possible values:

- Select from the list of defined WLAN profiles, maximum 31 ASCII characters.

Default: Blank

2.37.27.16.2 Name

Name of the script file to be used.

Telnet path: /Setup/WLAN-Management/Central-Firmware-Management/Script-Management

Possible values:

- File name in the form *.lcs, max. 63 ASCII characters

Default: Blank

2.37.27.11 Firmware repository URL

Directory where the latest firmware files are stored

Telnet path: /Setup/WLAN-Management/Central-Firmware-Management

Possible values:

- URL in the form Server/Directory or http://Server/Directory

Default: Blank

2.37.27.25 Firmware loopback address

This is where you can configure an optional sender address to be used instead of the one otherwise automatically selected for the destination address.

Telnet path: /Setup/WLAN-Management/Central-Firmware-Management

Possible values:

- Name of a defined IP network.
- 'INT' for the IP address in the first network with the setting 'Intranet'.
- 'DMZ' for the IP address in the first network with the setting 'DMZ'.
- Name of a loopback address.
- Any other IP address.

Default: Blank



If the list of IP networks or loopback addresses contains an entry named 'DMZ' then the associated IP address will be used.

2.37.27.14 Maximum number of loaded firmwares

Maximum number of firmware versions in memory

Telnet path: /Setup/WLAN-Management/Central-Firmware-Management

Possible values:

- 1 to 10

Default: 5

2.37.27.12 Script repository URL

The path to the directory with the script files.

Telnet path: /Setup/WLAN-Management/Central-Firmware-Management

Possible values:

- URL in the form Server/Directory or http://Server/Directory

Default: Blank

2.37.27.26 Script loopback address

This is where you can configure an optional sender address to be used instead of the one otherwise automatically selected for the destination address.

Telnet path: /Setup/WLAN-Management/Central-Firmware-Management

Possible values:

- Name of a defined IP network.
- 'INT' for the IP address in the first network with the setting 'Intranet'.
- 'DMZ' for the IP address in the first network with the setting 'DMZ'.
- Name of a loopback address.
- Any other IP address.

Default: Blank



If the list of IP networks or loopback addresses contains an entry named 'DMZ' then the associated IP address will be used.

2.37.27.13 Update firmware and script information

Launches an update process for the available firmware and script information

Telnet path: /Setup/WLAN-Management/Central-Firmware-Management

Possible values:

- Syntax: Do update-firmware-and-script-information



Do command

2.37.27.18 Reboot updated APs

Reboot updated APs.

Telnet path: /Setup/WLAN-Management/Central-Firmware-Management

Possible values:

- Syntax: Do Reboot-updated-APs



Do command

2.37.17 RADIUS server

By default, the WLAN Controller handles the forwarding of requests to the RADIUS server for account and access administration. In order for the APs to be able to communicate directly with the corresponding RADIUS server, you have to specify further settings here.

Telnet path: /Setup/WLAN-Management

2.37.17.1 Type

Type of RADIUS application

Telnet path: /Setup/WLAN-Management/RADIUS-Server

Possible values:

- Account
- Access

Default: Blank

Special values: Value is fixed



Cannot be configured with LANconfig

2.37.17.2 IP address

IP address of the RADIUS server that is communicated to the AP in order for it to reach the RADIUS server. If no value is entered the controller's IP address is taken as default.

Telnet path: /Setup/WLAN-Management/RADIUS-Server

Possible values:

- Valid IP address.

Default: Blank



Cannot be configured with LANconfig

2.37.17.3 Port

Port number of the RADIUS server that is communicated to the AP in order for it to reach the RADIUS server. This value will be ignored if no IP address is configured as the controller itself will be used as the RADIUS server.

Telnet path: /Setup/WLAN-Management/RADIUS-Server

Possible values:

- Port-Number

Default: Blank



Cannot be configured with LANconfig

2.37.17.4 Secret

Password for the RADIUS service. If no IP address is specified the controller will generate a random password that the AP then uses to register with RADIUS server in the controller.

Telnet path: /Setup/WLAN-Management/RADIUS-Server

Possible values:

- Max. 31 ASCII characters

Default: Blank



Cannot be configured with LANconfig

2.37.20 Access list

You can limit the data traffic between the wireless LAN and your local network by activating MAC address checks for individual logical WLAN networks. Enter all of the stations which are to be able to access these logical networks into the following table.

Telnet path: /Setup/WLAN-Management

2.37.20.1 MAC address

Enter the MAC address of a station.

Telnet path: /Setup/WLAN-Management/Access-List

Possible values:

- Valid MAC address

Default: Blank



Every network card has its own MAC address that is unique in the world. The address is a 12-character hexadecimal number (e.g. 00A057010203). This address can generally be found printed on the network card.

2.37.20.2 Name

You can enter any name you wish and a comment for any station.

This enables you to assign MAC addresses more easily to specific stations or users.

Telnet path: /Setup/WLAN-Management/Access-List

Possible values:

- Max. 32 characters

Default: Blank

2.37.20.3 Comment

Comment on this entry

Telnet path: /Setup/WLAN-Management/Access-List

Possible values:

■ Max. 30 characters

Default: Blank

2.37.20.4 WPA passphrase

Here you may enter a separate passphrase for each physical address (MAC address) that is used in a 802.11i/WPA/AES-PSK-secured network. If no separate passphrase is specified for this MAC address, the passphrases stored in the '802.11i/WEP' area will be used for each logical wireless LAN network.

Telnet path: /Setup/WLAN-Management/Access-List

Possible values:

■ ASCII character string with a length of 8 to 63 characters

Default: Blank

Special values: 0



This field has no significance for networks secured by WEP.

2.37.20.5 Tx limit

Bandwidth restriction for registering WLAN clients. A client communicates its own settings to the base station when logging in. The base station uses these values to set the minimum bandwidth.

Telnet path: /Setup/WLAN-Management/Access-List

Possible values:

■ 0 to 65535 kbps

Default: 0

Special values: 0: No limit



The significance of the Rx and Tx values depends on the device's operating mode. In this case, as an access point, Rx stands for "Send data" and Tx stands for "Receive data".

2.37.20.6 Rx limit

Bandwidth restriction for registering WLAN clients.

A client communicates its own settings to the base station when logging in. The base station uses these values to set the minimum bandwidth.

Telnet path: /Setup/WLAN-Management/Access-List

Possible values:

■ 0 to 65535 kbps

Default: 0

Special values: 0: No limit



The significance of the Rx and Tx values depends on the device's operating mode. In this case, as an access point, Rx stands for "Send data" and Tx stands for "Receive data".

2.37.20.7 VLAN-ID

This VLAN ID is assigned to packets that are received from the client with the MAC address entered here.

Telnet path: /Setup/WLAN-Management/Access-List

Possible values:

■ 0 to 4096

Default: 0

2.39 Certificates

This menu contains the configuration of the certificates.

Telnet path: /Setup

2.39.1 SCEP client

This menu contains the configuration of the SCEP client.

Telnet path: /Setup/Certificates

2.39.1.1 Operating

Switches SCEP on or off.

Telnet path: /Setup/Certificates/SCEP-Client

Possible values:

■ Yes

■ No

Default: No

Special values: No

2.39.1.9 Update

Manually triggers a request for a new system certificate, irrespective of the remaining validity period (lease). A new key pair is generated at the same time.

Telnet path: /Setup/Certificates/SCEP-Client

2.39.1.12 Check pending requests interval

Interval in seconds for checks on outstanding certificate requests.

Telnet path: /Setup/Certificates/SCEP-Client

Possible values:

■ Max. 10 characters

Default: 101

2.39.1.10 Clear SCEP file system

Starts a clean-up of the SCEP file system.

Deleted are: RA certificates, pending certificate requests, new and inactive CA certificates, new and inactive private keys.

Retained are: System certificates currently in use for VPN operations, associated private keys, and the CA certificates currently in use for VPN operations.

Telnet path: /Setup/Certificates/SCEP-Client

2.39.1.3 CA certificate-update before expiration

Preparation time in days for the timely retrieval of new RA/CA certificates.

Telnet path: /Setup/Certificates/SCEP-Client

Possible values:

■ Max. 10 characters

Default: 3

2.39.1.8 Reinitialization

Starts the manual reinitialization of the SCEP parameters. As with the standard SCEP initialization, the necessary RA and CA certificates are retrieved from the CA and stored within the file system in the LANCOM Wireless such that they are not yet ready for use in VPN operations. If the available system certificate fits to the retrieved CA certificate, then the system certificate, CA certificate and the device's private key can be used for VPN operations. If the existing system certificates do not fit to the retrieved CA certificate, then the next step is for the SCEP server to submit a new certificate request. Only once a new system certificate that fits to the retrieved CA certificate has been issued and retrieved can the system certificate, CA certificate and the device's private key can be used for VPN operations.

Telnet path: /Setup/Certificates/SCEP-Client

2.39.1.2 CA certificate-update before expiration

Preparation time in days for the timely retrieval of new RA/CA certificates.

Telnet path: /Setup/Certificates/SCEP-Client

Possible values:

■ Max. 10 characters

Default: Blank

2.39.1.13 Trace level

The output of trace messages for the SCEP client trace can be restricted to contain certain content only. The specified value defines the amount of detail of the packets in the trace.

Telnet path: /Setup/Certificates/SCEP-Client

Possible values:

■ All: All trace messages, including information and debug messages

■ Reduced: Error and alert messages only

■ Only errors: Error messages only

Default:

All

2.39.1.11 Retry after error interval

Interval in seconds between retries after errors of any type.

Telnet path: /Setup/Certificates/SCEP-Client

Possible values:

■ Max. 10 characters

Default: 22

2.39.1.7 Certificates

Here you can configure certificates or add new ones.

Telnet path: /Setup/Certificates/SCEP-Client

2.39.1.7.1 Name

The certificate's configuration name.

Telnet path: /Setup/Certificates/SCEP-client/Certificates

Possible values:

■ Max. 16 characters

Default: Blank

2.39.1.7.2 CADN

Distinguished name of the CA. With this parameter the CAs are assigned to system certificates (and vice versa) on the one hand. On the other hand this parameter is also important for evaluating whether received or available certificates match with the configuration.

Telnet path: /Setup/Certificates/SCEP-client/Certificates

Possible values:

■ Max. 251 characters

Default: Blank

2.39.1.7.3 Subject

Distinguished name of the subject of the requester.

Telnet path: /Setup/Certificates/SCEP-client/Certificates

Possible values:

■ Max. 251 characters

Default: Blank

2.39.1.7.4 Challenge password

Password (for the automatic issue of device certificates on the SCEP server).

Telnet path: /Setup/Certificates/SCEP-client/Certificates

Possible values:

■ Max. 251 characters

Default: Blank

2.39.1.7.5 SubjectAltName

Further information about the requester, e.g. domain or IP address.

Telnet path: /Setup/Certificates/SCEP-client/Certificates

Possible values:

■ Max. 251 characters

Default: Blank

2.39.1.7.6 Key usage

Any comma-separated combination of: digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign, cRLSign, encipherOnly, decipherOnly, critical (possible but not recommended)

Telnet path: /Setup/Certificates/SCEP-client/Certificates

Possible values:

■ Max. 251 characters

Default: Blank

2.39.1.7.7 Device certificate keylength

The length of the key to be generated for the device itself.

Telnet path: /Setup/Certificates/SCEP-client/Certificates

Possible values:

- 31 or better

Default: 0

2.39.1.7.8 Application

Indicates the intended application of the specified certificates. The certificates entered here are only queried for the corresponding application.

Telnet path: /Setup/Certificates/SCEP-client/Certificates

Possible values:

- VPN

Default: VPN

2.39.1.7.9 Extended key usage

Any comma-separated combination of: Critical, serverAuth, clientAuth, codeSigning, emailProtection, timeStamping, msCodeInd, msCodeCom, msCTLSign, msSGC, msEFS, nsSGC, 1.3.6.1.5.5.7.3.18 for WLAN controllers, 1.3.6.1.5.5.7.3.19 for access points in managed mode

Telnet path: /Setup/Certificates/SCEP-client/Certificates

Possible values:

- Max. 251 characters

Default: Blank

2.39.1.14 CAs

This table is used to define the available CAs.

Telnet path: /Setup/Certificates/SCEP-Client/CAs

2.39.1.14.1 Name

Enter a name that identifies this configuration.

Telnet path: /Setup/Certificates/SCEP-Client/Certificates/Name

Possible values: Max. 16 alphanumerical characters

Default: Blank

2.39.1.14.11 Loopback address

Enter a loopback address.

Telnet path: /Setup/Certificates/SCEP-Client/Certificates/Loopback-Addr.

Possible values: Max. 16 characters

Default: Blank

2.39.1.14.2 URL

This is where the enrollment URL is entered. The router must contact the certificate authority (CA) to request a certificate. The URL required tends to differ from one provider to another, and it is commonly specified in the documentation of the CA. Example: <http://postman/certsrv/mscep/mscep.dll>

Telnet path: /Setup/Certificates/SCEP-Client/Certificates/URL

Possible values:

- Max. 251 alphanumerical characters

Default: Blank

2.39.1.14.3 DN

The distinguished name must be entered here. With this parameter the CAs are assigned to system certificates (and vice versa) on the one hand. On the other hand this parameter is also important for evaluating whether received or available certificates match with the configuration. Separated by commas or forward slashes, this is a list where the name, department, state and country can be specified for the gateway. The following are examples of how an entry might appear: CN=myCACN, DC=mscep, DC=ca, C=DE, ST=berlin, O=myOrg /CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE

Telnet path: /Setup/Certificates/SCEP-Client/Certificates/DN

Possible values:

- Max. 251 alphanumerical characters

Default: Blank

2.39.1.14.4 Encryption algorithm

The encryption algorithm is specified here as used by the SCEP protocol (Simple Certificate Enrollment Protocol). This algorithm has to be supported by the Certificate Authority (CA) and by the client. Three methods are available:

Telnet path: /Setup/Certificates/SCEP-Client/Certificates/Enc-Alg

Possible values:

- **DES** - Data-Encryption-Standard: The DES algorithm uses a 64-bit key. This is the SCEP standard encryption. DES is an algorithm developed by the National Bureau of Standards (NBS) in the USA. The DES algorithm uses a 64-bit key which allows combinations of a substitution cipher, transposition cipher and exclusive-OR (XOR) operations. The 64-bit block size consists of an effective key length of 56 bits and 8 parity bits. The algorithm is based on the Lucifer cipher. This method was published in 1974, became a standard known as ANSI X3.92-1981, and is also specified by the ISO as ISO 8227. It has been in use for a number of years where sensitive data is found, such as in the capital markets and on Smartcards, and can be described as an international quasi-standard.
- **3DES** - Triple DES: This is an improved method of DES encryption using 2 keys of 64-bits in length.
- **BLOWFISH**: The BLOWFISH algorithm works with a variable key length of between 32 and 448 bits. It is a fast and highly secure algorithm. It has major advantages over other symmetrical methods such as DES and 3DES. Blowfish, developed by Bruce Schneier in 1993, is a symmetrical encryption method with a fast and highly secure algorithm, in particular in combination with 32-bit computers. This method works with a 64-bit block length and a variable key length of between 32 and 448 bits. Blowfish is highly efficient, works with XOR links and additions on 32-bit words. It is viewed as secure and offers big advantages over other symmetrical methods such as DES and 3DES.
- **AES128**: The Advanced Encryption Standard (AES) has a variable block size of 128, 192 or 256 bits and a variable key length of 128, 192 or 256 bits, providing a very high level of security.

Default: des



If possible you should employ one of the last two methods (3DES or BLOWFISH) as long as these are supported by the CA and all clients. The default value here is DES encryption to ensure interoperability.

2.39.1.14.5 Identifier

An additional identifier can be specified here. This value is required by some web servers to identify the CA.

Telnet path: /Setup/Certificates/SCEP-Client/Certificates/Identifier

Possible values:

- Max. 251 alphanumerical characters

Default: Blank

2.39.2 SCEP-CA

This menu contains the settings for SCEP-CA.

Telnet path: /Setup/Certificates/SCEP-Client

2.39.2.1 SCEP operating

Activates or deactivates the SCEP client.

Telnet path: /Setup/Certificates/SCEP-CA/SCEP-Operating

Possible values:

- Yes
- No

Default: No

2.39.2.7 Fingerprint algorithm

Here you select the fingerprint algorithm that the Certificate Authority (CA) uses to calculate the signature's fingerprint. This method must be supported by the CA and the client. The fingerprint is a hash value of data (key, certificate, etc.), i.e. a short number string that can be used to check the integrity of the data.

Telnet path: /Setup/Certificates/SCEP-CA/Fingerprint-Algorithm

Possible values:

- MD5: Message Digest Algorithm 5 generates a 128-bit hash value
- SHA1: Secure Hash Algorithm 1 generates a 160-bit hash value

Default: MD5

2.39.2.4 RA auto-approve

With this option, new requests are signed with this assuming that a system certificate is available. The option must be activated both at the client and at the Certificate Authority (CA server). In this case the client is authenticated at the CA by the certificate alone and without exchange of a challenge password.

Telnet path: /Setup/Certificates/SCEP-CA/RA-Autoapprove

Possible values:

- Yes
- No

Default: Yes

2.39.2.9 Reinitialize

Use this command to reinitialize the CA. The device checks the configuration and the certificates, and if necessary it updates the corresponding values and files.

Run this command when the CA is not running because of a configuration error. This initiates a new check after a change of configuration.

Telnet path: /Setup/Certificates/SCEP-CA/Reinitialize

2.39.2.6 Signature algorithm

Here you select the signature algorithm used by the Certificate Authority (CA) to sign the certificate. This method must be supported by the CA and the certificate recipient (client) as the client uses this signature to check the integrity of the certificate. Two cryptographic hash functions are relatively widespread.

Telnet path: /Setup/Certificates/SCEP-CA/Signature-Algorithm

Possible values:

- No
- **SHA1** - Secure Hash Algorithm 1 generates a 160-bit hash value. These are used to calculate a unique checksum for any data. Generally this data makes up messages. It is practically impossible to come across two messages with exactly the same SHA value. The length of the hash value in the SHA algorithm is 160 bits.
- **MD5** (default) - Message Digest Algorithm 5 generates a 128-bit hash value. MD5 was developed in 1991 by Ronald L. Rivest. The results reveal no conclusive information about the key. This method takes a message of any length to generate a 128-bit message digest, which is attached to the unencrypted message. The recipient compares the message digest with that determined from the information.

Default: Off

2.39.2.3 Encryption algorithm

The encryption algorithm is specified here as used by the SCEP protocol (Simple Certificate Enrollment Protocol). This algorithm has to be supported by the Certificate Authority (CA) and by the client.

Telnet path: /Setup/Certificates/SCEP-CA/Encryption-Algorithm

Possible values:

- **DES:** Data Encryption Standard: The DES algorithm uses a 64-bit key. This is the SCEP standard encryption.
- **3DES:** Triple DES: This is an improved method of DES encryption using 2 keys of 64-bits in length.
- **BLOWFISH:** The BLOWFISH algorithm works with a variable key length of between 32 and 448 bits. It is a fast and highly secure algorithm. It has major advantages over other symmetrical methods such as DES and 3DES.
- **AES128:** The Advanced Encryption Standard (AES) has a variable block size of 128, 192 or 256 bits and a variable key length of 128, 192 or 256 bits, providing a very high level of security.

Default: DES

2.39.2.2 CA certificates

This menu contains the settings for CA certificates.

Telnet path: /Setup/Certificates/SCEP-Client/CAs

2.39.2.2.3 Alternative name

An alternative 'Subject Name' can be entered here.

Examples: Critical, DNS:host.company.de IP:10.10.10.10 DNS:host.company.de, IP:10.10.10.10
UFQDN:email:name@company.de

Telnet path: /Setup/Certificates/SCEP-CA/CA-certificates/Alternative-name

2.39.2.2.1 CA distinguished name

The distinguished name must be entered here. With this parameter the CAs are assigned to system certificates (and vice versa) on the one hand. On the other hand this parameter is also important for evaluating whether received or available certificates match with the configuration. Separated by commas or forward slashes, this is a list where the name, department, state and country can be specified for the gateway. The following are examples of how an entry might appear: CN=myCACN, DC=mscep, DC=ca, C=DE, ST=berlin, O=myOrg /CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE

Telnet path: /Setup/Certificates/SCEP-CA/CA certificates/CA-Distinguished-Name

Possible values:

- Max. 251 characters

Default: Blank

2.39.2.2.6 CA certificate update before

Enter the time period for the 'Update before expiry' in days.

Telnet path: /Setup/Certificates/SCEP-CA/CA-certificates/Validity-Period

Possible values:

■ Max. 2 numerical characters

Default: 4

2.39.2.2.9 Create new CA certificates

Run this command if you have changed the configuration of the CA.

The CA only creates new certificates automatically when the old ones have expired or none are available. If you decide to change the key length, the name, or other values of the CA certificate, this command enables you to recreate the corresponding certificate files.

Telnet path: /Setup/Certificates/SCEP-CA/CA-certificates/Create-new-CA-certificates

2.39.2.2.10 Create PKCS12 backup files

To restore the CA or RA, the relevant root certificates with private keys will be required that are generated automatically when the WLAN Controller is started.

To ensure that this confidential information remains protected even when exported from the device, it is initially stored to a password-protected PKCS12 container.

The command "Create-PKCS12-Backup-Files" starts the export. Enter the passphrase when prompted to enter a parameter.

Telnet path: /Setup/Certificates/SCEP-CA/CA-certificates/Create-PKCS12-Backup-Files

2.39.2.2.5 Validity period

Here you enter the certificate's validity period in days.

Telnet path: /Setup/Certificates/SCEP-CA/CA-certificates/Validity-Period

Possible values:

■ Max. 5 numerical characters

Default: 1100

2.39.2.2.8 RA distinguished name

The distinguished name must be entered here. With this parameter the CAs are assigned to system certificates (and vice versa) on the one hand. On the other hand this parameter is also important for evaluating whether received or available certificates match with the configuration. Separated by commas or forward slashes, this is a list where the name, department, state and country can be specified for the gateway. The following are examples of how an entry might appear: CN=myCACN, DC=mscep, DC=ca, C=DE, ST=berlin, O=myOrg /CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE

Telnet path: /Setup/Certificates/SCEP-CA/CA-certificates/RA-Distinguished-Name

Possible values:

■ Max. 251 characters

Default: Blank

2.39.2.2.4 RSA key length

The key length must be entered here. This value specifies the length of new keys in bits.

Telnet path: /Setup/Certificates/SCEP-CA/CA-certificates/RSA-key-length

Possible values:

■ 1024

■ 2048

■ 3072

■ 4096

■ 8192

Default: 2048



The time taken for calculation depends on the performance available from the system; the greater the number of bits, the longer it takes.

2.39.2.2.11 Restore certificates from backup

In case of a backup event, this command restores the two PKCS12 files with their respective root certificates and the private keys from the CA and/or RA.

Telnet path: /Setup/Certificates/SCEP-CA/CA-certificates/Restore-certificates-from-Backup

2.39.2.5 Client certificates

This menu contains the settings for client certificates.

Telnet path: /Setup/Certificates/SCEP-Client/Certificates

2.39.2.5.4 General challenge password

An additional 'password' can be entered here, which is transmitted to the CA. This can be used by default to authenticate revocation requests. If CAs operate Microsoft-SCEP (mscep), the one-time passwords issued by the CA can be entered here for the authentication of requests.

Telnet path: /Setup/Certificates/SCEP-CA/Client-Certificates/General-Challenge-Password

Possible values:

■ Max. 16 characters

Default: XuL[ksKcC3+'%PA2

2.39.2.5.1 Validity period

Here you determine the validity period of the certificate in days.

Telnet path: /Setup/Certificates/SCEP-CA/CA-certificates/Validity-Period

Possible values:

■ Max. 5 numerical characters

Default: 365

2.39.2.5.3 Challenge passwords

This table provides an overview of the challenge passwords.

Telnet path: /Setup/Certificates/SCEP-CA/Client-Certificates/Validity-Period

2.39.2.5.3.1 Index

Enter the index for the challenge password here.

Telnet path: /Setup/Certificates/SCEP-CA/Client-Certificates/Validity-Period/Index

Possible values:

■ Max. 10 numerical characters

Default: Blank

2.39.2.5.3.2 Subject distinguished name

The distinguished name must be entered here. With this parameter the CAs are assigned to system certificates (and vice versa) on the one hand. On the other hand this parameter is also important for evaluating whether received or available certificates match with the configuration. Separated by commas or forward slashes, this is a list where the name, department, state and country can be specified for the gateway. The following are examples of how an entry might appear: CN=myCACN, DC=mscep, DC=ca, C=DE, ST=berlin, O=myOrg /CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE

Telnet path: /Setup/Certificates/SCEP-CA/Client-Certificates/Challenge-Passwords/Subject-Distinguished-Name

Possible values:

- Max. 251 characters

Default: Blank**2.39.2.5.3.3 MAC address**

Enter the MAC address of the client whose password is to be managed by the challenge-password table.

Telnet path: /Setup/Certificates/SCEP-CA/Client-Certificates/Validity-Period/MAC-Address**Possible values:**

- Maximum 12 alphanumerical characters

Default: Blank**2.39.2.5.3.4 Challenge**

Enter the challenge (password) for the client here.

Telnet path: /Setup/Certificates/SCEP-CA/Client-Certificates/Validity-Period/Challenge**Possible values:**

- Maximum 16 alphanumerical characters

Default: Blank**2.39.2.5.3.5 Validity**

Enter the validity period of passwords in days.

Telnet path: /Setup/Certificates/SCEP-CA/Client-Certificates/Validity-Period/Validity-Period**Possible values:**

- Max. 5 characters

Default: 365 days**2.39.2.8 Certificate revocation lists**

This item contains the certificate revocation lists.

Telnet path: /Setup/Certificates/SCEP-CA/Certificate-Revocation-Lists**2.39.2.8.2 CRL distribution point hostname**

Enter here the update interval in seconds for creating a new CRL. The lower limit for this is 600 seconds.

Telnet path: /Setup/Certificates/SCEP-CA/Certificate-Revocation-Lists/CRL-Distribution-Point-Hostname**Possible values:**

- Max. 63 numerical characters

Default: 600**2.39.2.8.3 Create new CRL**

Normally, the CA automatically creates a new certificate revocation list (CRL) when the old CRL expires or when the contents of the CRL changes (due to SCEP operations).

Run this command if you have revoked a certificate in the certificate status list.

Telnet path: /Setup/Certificates/SCEP-CA/Certificate-Revocation-Lists/Create-New-CRL**2.39.2.8.1 Update interval**

Enter here the update interval in seconds for creating a new CRL. The lower limit for this is 600 seconds. .

Telnet path: /Setup/Certificates/SCEP-CA/Certificate-Revocation-Lists/CRL-Update-Interval**Possible values:**

- Max. 63 numerical characters

Default: 86,400

2.39.2.10 Notification

This menu contains the settings for the notification of events relating to certificates.

Telnet path: /Setup/Certificates/SCEP-CA/Logging

2.39.2.10.1 E-mail

The setting here determines whether a notification is sent when an event occurs.

Telnet path: /Setup/Certificates/SCEP-CA/Logging/E-Mail

Possible values:

- No
- Yes

Default: No

2.39.2.10.1 E-mail receiver

Here you enter the e-mail address to which a notification is sent when an event occurs.

Telnet path: /Setup/Certificates/SCEP-CA/Logging/E-Mail

Possible values:

- Maximum 63 alphanumerical characters

Default: Blank

2.39.2.10.4 Send backup reminder

If this function is activated, a reminder about the need to make a backup is sent automatically to the e-mail address entered here.

Telnet path: /Setup/Certificates/SCEP-CA/Logging/Send-Backup-Reminder

Possible values:

- No
- Yes

Default: No

2.39.2.10.2 Syslog

This item activates the logging function based on notifications via Syslog.

Telnet path: /Setup/Certificates/SCEP-CA/Logging/Syslog

Possible values:

- No
- Yes

Default: No



To make use of this function, the Syslog client in the device needs to be configured accordingly.

2.39.3 CRLs

This menu contains the configuration of the CRLs.

Telnet path: /Setup/Certificates

2.39.3.1 Operating

Enabled: During the certificate check, the CRL (if available) will be considered as well.

Telnet path: /Setup/Certificates/CRLs

Possible values:

- Yes
- No

Default: No

If this option is activated but no valid CRL is available (e.g. if the server can't be reached), then all connections will be rejected and existing connections will be interrupted.

2.39.3.5 Prefetch period

The time period after which periodic attempts are made to retrieve a new CRL. Useful for the early retrieval of CRLs published at irregular intervals. The entry '0' disables regular retrieval.

Telnet path: /Setup/Certificates/CRLs**Possible values:**

- Max. 10 characters

Default: 0

If with regular updates the CRL cannot be retrieved, no further attempts will be started until the next regular attempt.

2.39.3.7 Refresh CRL now

Reads the current CRL from the URL specified in the root certificate, or from the alternative URL (if this function is set up).

Telnet path: /Setup/Certificates/CRLs

2.39.3.6 Validity exceedance

Even after expiry of the CRL, certificate-based connections will continue to be accepted for the period defined here. This tolerance period can prevent the unintentional rejection or interruption of connections if the CRL server should be temporarily unavailable.

Telnet path: /Setup/Certificates/CRLs**Possible values:**

- Max. 10 characters

Default: 0

Special values: Within the time period defined here, even certificates in the CRL which have expired can still be used to maintain or establish a connection.



In the time period defined here, even expired certificates can be used to maintain or re-establish a connection.

2.39.3.4 Update before expiry

The point in time prior to expiry of the CRL when the new CRL can be loaded. This value is increased by a random value to prevent server overload from multiple simultaneous queries. Once within this time frame, any coinciding regular planned updates will be stopped.

Telnet path: /Setup/Certificates/CRLs**Possible values:**

- Max. 10 characters

Default: 300



If the first attempt to load the CRL fails, new attempts are made at regular short intervals.

2.39.3.9 Loopback address

Here you can optionally define a sender address for display to the recipient instead of the automatically generated address.

Telnet path: /Setup/Certificates/CRLs/Loopback-Address

Possible values:

- Name of the IP network whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LBO – LBF for the 16 loopback addresses
- Any valid IP address

Default: Blank



If there is an interface called "DMZ", its address will be taken if you have selected "DMZ".

2.39.3.8 Alternative URL table

This table contains the list of alternative URLs.

The address where a certificate revocation list (CRL) can be collected is normally defined in the certificate (as `crlDistributionPoint`). LCOS has a table where alternative CRLs can be specified. After a system start the CRLs are automatically collected from these URLs. These are used in addition to the lists offered by the certificates.

Telnet path: /Setup/Certificates/CRLs/Alternative-URL-Table

2.39.3.8.1 Alternative URL

Here you enter the alternative URL where a CRL can be collected.

Telnet path: /Setup/Certificates/CRLs/Alternative-URL-Table/Alternative-URL

Possible values:

- Any valid URL with max. 251 characters.

Default: Blank

2.39.6 OCSP client

This menu contains the settings for the OCSP client.

Telnet path: /Setup/Certificates

2.39.6.1 CA profile table

This table contains information on the Certificate Authorities (CAs), whose certificates are evaluated by the OCSP client by sending a request to an OCSP responder.

Telnet path: /Setup/Certificates/OCSP-Client

2.39.6.1.1 Profile name

Enter here the name of a CA profile to be used by the OCSP client for a particular CA.

Telnet path: /Setup/Certificates/OCSP-Client/Ca-Profile-Table

Possible values:

- Maximum 32 alphanumerical characters

Default: Blank

2.39.6.1.2 CA distinguished name

Enter the distinguished name of the CA, whose certificates are evaluated by the OSCP client with this profile name.

Telnet path: /Setup/Certificates/OCSP-Client/Ca-Profile-Table

Possible values:

- Maximum 251 alphanumerical characters

Default: Blank

2.39.6.1.3 Prefer AIA

Certificates used for establishing VPN connections optionally include the URL of the relevant OSCP responder in the field Authority Info Access (AIA). This item defines whether the OSCP client prefers to use the URL from this entry in the CA profile table or the URL from the AIA field, if available.

Telnet path: /Setup/Certificates/OCSP-Client/Ca-Profile-Table

Possible values:

- No: The OSCP client always uses the URL from this CA-profile table entry and ignores the URL in the AIA field.
- Yes: The OSCP client uses the URL from the AIA field (if specified) and ignores the URL from this CA profile table entry.

Default: No

2.39.6.1.4 Responder profile name

This item selects the responder profile used by the OSCP client to evaluate certificates from this CA.

Telnet path: /Setup/Certificates/OCSP-Client/Ca-Profile-Table

Possible values:

- Select from the list of profile names in the table 2.39.6.2 Responder profile table, maximum 32 alphanumeric characters.

Default: Blank



If the field for the responder profile name is left empty, the machine evaluates the certificates from the CA defined here not with OSCP, but with the help of a CRL.

2.39.6.1.5 Source interface

This is where you can configure an optional sender address to be used instead of the one otherwise automatically selected for the destination address.

If you have configured loopback addresses, you can specify them here as sender address.

Telnet path: /Setup/Certificates/OCSP-Client/Ca-Profile-Table

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LB0 to LBF for the 16 loopback addresses
- Any valid IP address

Default: 00.0.0



If the list of IP networks or loopback addresses contains an entry named 'DMZ' then the associated IP address will be used. Name of a loopback address.

2.39.6.1.6 Certificate evaluation

This item defines how the device behaves if certificate evaluation fails. During connection establishment, the OSCP client first queries the OSCP responder about the validity of the certificate. If the certificate is about to expire, the OSCP client automatically repeats the query about the validity before the certificate expires.

Telnet path: /Setup/Certificates/OCSP-Client/Ca-Profile-Table

Possible values:

- Strict: If the OCSP responder reports that the certificate used during connection establishment is not valid, the device does not establish a connection to the remote site. If during an ongoing connection the OCSP responder does not confirm a new request in good time before the certificate's expiry, the device will cut the connection.
- Loose: If the OCSP responder reports that the certificate used during connection establishment is not valid, the device will still establish a connection to the remote site. Even if during an ongoing connection the OCSP responder does not confirm a new request in good time before the certificate's expiry, the device will not cut the connection.

Default: Strict

If necessary, you can log and review the results of certificate evaluation by the OCSP responder with SYSLOG, SNMP traps and relevant traces.

2.39.6.1.7 Syslog events

The OCSP client can optionally generate SYSLOG messages with information on the results of certificate checks by the OCSP responder.

Telnet path: /Setup/Certificates/OCSP-Client/Ca-Profile-Table**Possible values:**

- Yes: The OCSP client generates SYSLOG messages
- No: The OCSP client does not generate SYSLOG messages

Default: Yes**2.39.6.2 Responder profile table**

This table contains information on the Certificate Authorities (CAs), whose certificates are evaluated by the OCSP client by sending a request to an OCSP responder.

Telnet path: /Setup/Certificates/OCSP-Client**2.39.6.2.1 Profile name**

Enter here the name of an OCSP-responder profile to be referenced by the OCSP client in the CA profile table.

Telnet path: /Setup/Certificates/OCSP-Client/Ca-Profile-Table**Possible values:**

- Maximum 32 alphanumerical characters

Default: Blank**2.39.6.2.2 URL**

Enter the URL for the OCSP client to access the OCSP responder.

Telnet path: /Setup/Certificates/OCSP-Client/Ca-Profile-Table**Possible values:**

- Valid URL with a maximum of 251 alphanumeric characters

Default: Blank**2.40 GPS**

This item contains the GPS settings.

Telnet path: /Setup/GPS**2.40.1 Operating**

Activate or deactivate the GPS function here. You can activate the GPS module independently of the location verification function, for example to monitor the current positional coordinates with LANmonitor.

Telnet path: /Setup/GPS/Operating

Possible values:

- No
- Yes

Default: No

2.41 UTM

You can adjust the UTM settings here.

Telnet path: /Setup/

2.41.2 Content filter

The settings for the content filter are located here.

Telnet path: /Setup/UTM/

2.41.2.1 Operating

This is where you can activate the content filter.

Telnet path: /Setup/UTM/Content-Filter/Operating**Possible values:**

- Yes: Activates the content filter.
- No: Deactivates the content filter.

Default:

- No

2.41.2.2 Global settings

NEW

The global settings for the content filter are located here.

Telnet path: /Setup/UTM/Content-Filter/

2.41.2.2.1 Admin e-mail

An SMTP client must be defined if you wish to use the e-mail notification function. You can use the client in the device, or another client of your choice.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings

No e-mail will be sent if no e-mail recipient is defined,.

2.41.2.2.5 Action on error

This is where you can determine what should happen when an error occurs. For example, if the rating server cannot be contacted, this setting either allows the user to surf without restrictions or access to the web is blocked entirely.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings**Possible values:**

- Block, pass

Default: Block

2.41.2.2.6 Action on license expiration

The license to use the LANCOM Content Filter is valid for a certain period. You will be reminded of the license expiry date 30 days, one week and one day before it actually expires (at the e-mail address configured in LANconfig: Log & Trace > General).

This is where you can specify what should happen when the license expires (i.e. block everything or allow everything through). After the license expires, this setting either allows the user to surf the web without restrictions, or access to the web is blocked entirely.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings

Possible values:

- Block, pass

Default: Block

2.41.2.2.6 Action on license exceedance

This is where you can determine what should happen when the licensed number of users is exceeded. Users are identified by their IP address. The system keeps count of the IP addresses that connect via the LANCOM Content Filter. When the eleventh user establishes a connection with a 10-user license, no further checking is performed by the LANCOM Content Filter. Depending on this setting, the unlicensed user can either surf the web without restrictions, or access to the web is blocked entirely.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings

Possible values:

- Block, pass

Default: Block



The users of the content filter are automatically removed from the user list when no connection has been made from the IP address concerned via the content filter for 24 hours.

2.41.2.2.17 Save to flashrom

Activate this option for the category statistics to be stored to the flash ROM.

This ensures that the data are not lost even if the device is switched off or suffers a power outage.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/Save-to-Flashrom

Possible values:

- Yes: Activates storage to the flash ROM.
- No: Deactivates storage to the flash ROM.

Default: No

2.41.2.2.22 Loopback to use on override



This parameter is no longer used as of LCOS 8.50.

This is where you can configure an optional sender address for the override URL to be used instead of the one that would normally be automatically selected for this target address. If you have configured loopback addresses, you can specify them here as sender address.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings

English description: Loopback-To-Use-On-Override

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ (Note: If there is an interface named "DMZ", its address will be taken).
- LB0 ... LBF for the 16 loopback addresses
- GUEST
- Any IP address in the form x.x.x.x

Default: Blank



The sender address specified here is used unmasked for every remote station.

2.41.2.2.12 Loopback to use on blocking

This is where you can configure an optional sender address for the blocked URL to be used instead of the one that would normally be automatically selected for this target address. If you have configured loopback addresses, you can specify them here as sender address.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ (Note: If there is an interface named "DMZ", its address will be taken).
- LBO ... LBF for the 16 loopback addresses
- GUEST
- Any IP address in the form x.x.x.x

Default: Blank



The sender address specified here is used unmasked for every remote station.

2.41.2.2.13 Override active

This is where you can activate the override function and make further related settings.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings

Possible values:

- Yes, No

Default: No

2.41.2.2.14 Override duration

The override duration can be restricted here. When the period expires, any attempt to access the same domain and/or category will be blocked again. Clicking on the override button once more allows the web site to be accessed again for the duration of the override and, depending on the settings, the administrator will be notified once more.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/

Possible values:

- 1-1440 (minutes)
- Max. 4 characters

Default: 5 minutes

2.41.2.2.15 Override type

This is where you can set the type of override. It can be allowed for the domain, for the category of web site to be blocked, or for both.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings

Possible values:

- Category: For the duration of the override, all URLs are allowed that fall under the affected categories (as well as those which would already have been allowed even without the override).
- Domain: For the duration of the override all URLs in this domain are allowed, irrespective of the categories they belong to.
- Category-and-Domain: For the duration of the override, all URLs are allowed that belong to this domain and also to the allowed categories. This is the highest restriction.

Default: Category-and-Domain

2.41.2.2.24 Proxy connections limit

This setting is for the maximum allowable number of simultaneous proxy connections. This limits the load that can be placed on the system. A notification is sent if this number should be exceeded.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/Proxy-Connections-Limit

Possible values:

- 0 to 999999 connections

Default: Varies from device to device

2.41.2.2.21 URL to show on override



This parameter is no longer used as of LCOS 8.50.

This is where you can enter the address of an alternative URL. In the event of an override, the URL entered here will be displayed instead of the usual web site. You can use this external HTML page to display your company's corporate design, for example, or to perform functions such as JavaScript routines, etc. You can also use the same tags here as used in the override text. If you do not make any entry here, the default page stored in the device will be displayed..

Telnet path: /Setup/UTM/Content-Filter/Global-Settings

Possible values:

- Valid URL address

Default: Blank

2.41.2.2.11 URL to show on blocking

This is where you can enter the address of an alternative URL. If access is blocked, the URL entered here will be displayed instead of the requested web site. You can use this external HTML page to display your company's corporate design, for example, or to perform functions such as JavaScript routines, etc. You can also use the same HTML tags here as used in the blocking text. If you do not make any entry here, the default page stored in the device will be displayed..

Telnet path: /Setup/UTM/Content-Filter/Global-Settings

Possible values:

- Valid URL address

Default: Blank

2.41.2.2.25 Processing timeout in ms

Specifies the maximum time in milliseconds that the proxy can take for processing. A timeout error page is displayed if this time is exceeded.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/Processing-Timeout-in-ms

Possible values:

- 0 to 999999 milliseconds

Default:

- 3000 milliseconds

Special values:

- The value 0 sets no time limit. Values less than 100 milliseconds make no sense.

2.41.2.2.9 Notification

This is where you define how you wish to receive notification of specific events. Notification can be made by e-mail, SNMP or SYSLOG. You can specify that messages for different events should be output in different ways.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/

Error:

- For SYSLOG: Source "System", priority "Alarm".
- Default: SYSLOG notification

License exceedance:

- For SYSLOG: Source "Admin", priority "Alarm".
- Default: E-MAIL, SNMP and SYSLOG notification

License expiry:

- For SYSLOG: Source "Admin", priority "Alarm".
- Default: E-MAIL, SNMP and SYSLOG notification

Override:

- For SYSLOG: Source "Router", priority "Alarm".
- Default: No notification

Proxy limit:

- For SYSLOG: Source "Router", priority "Info".
- Default: SYSLOG notification

2.41.2.2.9.1 Cause

Here you choose one of the predefined values for the cause for notification.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/Notification

2.41.2.2.9.2 E-mail

You can specify whether you want to receive notification by e-mail here.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/Notification

Possible values:

- Yes
- No

Default: Differs according to the cause.

2.41.2.2.9.3 SNMP

You can specify whether you want to receive notification by SNMP here.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/Notification

Possible values:

- Yes, No

Default: Differs according to the cause.

2.41.2.2.9.4 Syslog

You can specify whether you want to receive notification by SYSLOG here.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/Notification

Possible values:

- Yes
- No

Default: Differs according to the cause.

2.41.2.2.10 Block text

This is where you can define text to be displayed when blocking occurs. Different blocking texts can be defined for different languages. The display of blocking text is controlled by the language setting transmitted by the browser (user agent).

Telnet path: /Setup/UTM/Content-Filter/Global-Settings

2.41.2.2.10.1 Language

Entering the appropriate country code here ensures that users receive all messages in their browser's preset language. If the country code set in the browser is found here, the matching text will be displayed.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/Block-Text

You can add any other language.

Examples of the country code:

- de-DE: German-Germany
- de-CH: German-Switzerland
- de-AT: German-Austria
- en-GB: English-Great Britain
- en-US: English-USA



The content filter processes only the first part of the country code to the '-', i.e. "en", "en-GB" and "en-US" are identical to the content filter. The content filter is not case-sensitive. If the country code

set in the browser is not found in this table, or if the text stored under that country code is deleted, the predefined default text ("default") will be used. You can modify the default text.

Possible values:

10 alphanumerical characters

Default:

Blank

2.41.2.2.10.2 Text

Enter the text that you wish to use as blocking text for this language.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/Block-Text

Possible values:

- 254 alphanumerical characters

Default:

Blank

Special values:

You can also use special tags for blocking text if you wish to display different pages depending on the reason why the web site was blocked (e.g. forbidden category or entry in the blacklist).

The following tags can be used as tag values:

- <CF-URL/> for the forbidden URL
- <CF-HOST/> or <CF-DOMAIN/> displays the host or the domain for the allowed URL. The tags are of equal value and their use is optional.
- <CF-CATEGORIES/> for the list of categories why the web site was blocked
- <CF-PROFILE/> for the profile name
- <CF-DURATION/> displays the override duration in minutes.
- <CF-OVERRIDEURL/> for the URL used to activate the URL (this can be integrated in a simple <a> tag or in a button)
- <CF-LINK/> adds a link for activating the override
- <CF-BUTTON/> for a button for activating the override

You can use a tag with attributes to display or hide parts of the HTML document: <CF-IF att1 att2> ... </CF-IF>.

Possible attributes are:

- BLACKLIST: If the site was blocked because it is in the profile blacklist
- FORBIDDEN: If the site was blocked due to one of its categories
- CATEGORY: When the override type is "Category" and the override was successful
- ERR: If an error has occurred.

Since there are separate text tables for the blocking page and the error page, this tag only makes sense if you have configured an alternative URL to show on blocking.

- OVERRIDEOK: If users have been allowed an override (in this case, the page should display an appropriate button)

If several attributes are defined in one tag, the section will be displayed if at least one of these conditions is met. All tags and attributes can be abbreviated to the first two letters (e.g. CF-CA or CF-IF BL). This is necessary as the blocking text may only contain a maximum of 254 characters.

Example:

- <CF-URL/> is blocked because it matches the categories <CF-CA/>.</p><p>Your content profile is <CF-PR/>.</p><p><CF-IF OVERRIDEOK></p><p><CF-BU/></CF-IF>



The tags described here can also be used in external HTML pages (alternative URLs to show on blocking).

2.41.2.2.19 Error text

This is where you can define text to be displayed when an error occurs.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings

2.41.2.2.19.1 Language

Entering the appropriate country code here ensures that users receive all messages in their browser's preset language. If the country code set in the browser is found here, the matching text will be displayed.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/Error-Text

You can add any other language.

Examples of the country code:

- de-DE: German-Germany
- de-CH: German-Switzerland
- de-AT: German-Austria
- en-GB: English-Great Britain
- en-US: English-USA



The content filter processes only the first part of the country code to the '-', i.e. "en", "en-GB" and "en-US" are identical to the content filter. The content filter is not case-sensitive. If the country code set in the browser is not found in this table, or if the text stored under that country code is deleted, the predefined default text ("default") will be used. You can modify the default text.

Possible values:

10 alphanumerical characters

Default:

Blank

2.41.2.2.19.2 Text

Enter the text that you wish to use as error text for this language.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/Error-Text

Possible values:

254 alphanumerical characters

Default:

Blank

Special values:

You can also use HTML tags for the error text.

The following empty element tags can be used as tag values:

- <CF-URL/> for the forbidden URL
- <CF-HOST/> or <CF-DOMAIN/> displays the host or the domain for the forbidden URL. The tags are of equal value and their use is optional.
- <CF-DURATION/> displays the override duration in minutes.
- <CF-PROFILE/> for the profile name
- <CF-ERROR/> for the error message

You can use a tag with attributes to display or hide parts of the HTML document: <CF-IF att1 att2> ... </CF-IF>.

Possible attributes are:

- CHECKERROR: The error occurred while checking the URL
- OVERRIDEERROR: The error occurred while approving an override

Example:

<CF-URL/> is blocked because an error has occurred:</p><p><CF-ERROR/>

<CF-URL>: Blocked URL <CF-HOST> or <CF-DOMAIN>: Host part of the blocked URL <CF-PROFILE>: User content-filter profile <CF-DURATION>: Override time in minutes <CF-ERROR>: Error message <CF-IF> to </CF-IF>: Conditional evaluation of the following parameters with the logical OR: CHECKERROR: The error occurred while checking the URL (as earlier) OVERRIDE ERROR: The error occurred while approving an override

2.41.2.2.20 Override text

This is where you can define text that is displayed to users confirming an override.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings

2.41.2.2.20.1 Language

Entering the appropriate country code here ensures that users receive all messages in their browser's preset language. If the country code set in the browser is found here, the matching text will be displayed.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/Override-Text

You can add any other language.

Examples of the country code:

- de-DE: German-Germany
- de-CH: German-Switzerland
- de-AT: German-Austria
- en-GB: English-Great Britain
- en-US: English-USA



The content filter processes only the first part of the country code to the '-', i.e. "en", "en-GB" and "en-US" are identical to the content filter. The content filter is not case-sensitive. If the country code set in the browser is not found in this table, or if the text stored under that country code is deleted, the predefined default text ("default") will be used. You can modify the default text.

Possible values:

10 alphanumerical characters

Default:

Blank

2.41.2.2.20.2 Text

Enter the text that you wish to use as override text for this language.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/Override-Text

Possible values:

- 254 alphanumerical characters

Default:

Blank

Special values:

You can also use HTML tags for blocking text if you wish to display different pages depending on the reason why the web site was blocked (e.g. forbidden category or entry in the blacklist).

The following tags can be used as tag values:

- <CF-URL/> for the originally forbidden URL that is now allowed
- <CF-CATEGORIES/> for the list of categories that have now been allowed as a result of the override (except if domain override is specified).
- <CF-BUTTON/> displays an override button that forwards the browser to the original URL.
- <CF-BUTTON/> displays an override link that forwards the browser to the original URL.
- <CF-HOST/> or <CF-DOMAIN/> displays the host or the domain for the allowed URL. The tags are of equal value and their use is optional.
- <CF-ERROR/> generates an error message in the event that the override fails.
- <CF-DURATION/> displays the override duration in minutes.

You can use a tag with attributes to display or hide parts of the HTML document: <CF-IF att1 att2> ... </CF-IF>.

Attributes can be:

- BLACKLIST: If the site was blocked because it is in the profile blacklist
- FORBIDDEN: If the site was blocked due to one of its categories
- CATEGORY: When the override type is "Category" and the override was successful
- DOMAIN: When the override type is "Domain" and the override was successful
- BOTH: When the override type is "Category-and-Domain" and the override was successful
- ERROR: When the override fails

- OK: When either CATEGORY or DOMAIN or BOTH are applicable

If several attributes are defined in one tag, the section should be displayed if at least one of these conditions is met. All tags and attributes can be abbreviated to the first two letters (e.g. CF-CA or CF-IF BL). This is necessary as the blocking text may only contain a maximum of 254 characters.

Example:

```
<CF-IF CA BO>The categories <CF-CAT/> are</CF-IF><CF-IF BO> in the domain <CF-DO/></CF-IF><CF-IF DO>The domain <CF-DO/> is</CF-IF><CF-IF OK> released for <CF-DU/> minutes.</p><p><CF-LI/></CF-IF><CF-IF ERR>Override error:</p><p><CF-ERR/></CF-IF>
```

2.41.2.2.23 Snapshot

This is where you can activate the content filter snapshot and determine when and how often it should be taken. The snapshot copies the category statistics table to the last snapshot table, overwriting the old contents of the snapshot table. The category statistics values are then reset to 0.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings

2.41.2.2.23.1 Active

This is where you can activate the content filter snapshot and determine when and how often it should be taken. The snapshot copies the category statistics table to the last snapshot table, overwriting the old contents of the snapshot table. The category statistics values are then reset to 0.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/Snapshot/Active

Possible values:

- Yes: Activates the snapshot.
- No: Deactivates the snapshot.

Default:

- Yes

2.41.2.2.23.4 Day

For monthly snapshots, set the day of the month when the snapshot should be taken.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/Snapshot

Possible values:

Max. 2 characters

Default:

1



It is advisable to select a number between 1 and 28 in order to ensure that it occurs every month.

2.41.2.2.23.2 Type

Here you decide whether the snapshot should be taken monthly, weekly or daily.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/Snapshot

Possible values

Monthly, weekly, daily

Default:

Monthly

2.41.2.2.23.5 Weekday

For weekly snapshots, set the day of the week when the snapshot should be taken.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/Snapshot

Possible values:

Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday

Default: Sunday

2.41.2.2.23.3 Time

If you require a daily snapshot, then enter here the time of day for the snapshot in hours and minutes.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/Snapshot

Possible values:

- Max. 5 characters
- Format HH:MM

Default:

00:00

2.41.2.2.21 URL to show on error

This is where you can enter an alternative URL. In the event of an error, the URL entered here will be displayed instead of the usual web site. You can use this external HTML page to display your company's corporate design, for example, or to perform functions such as JavaScript routines, etc. You can also use the same tags here as used in the override text. If you do not make any entry here, the default page stored in the device will be displayed..

Telnet path: /Setup/UTM/Content-Filter/Global-Settings

Possible values:

- Valid URL address

Default: Blank

2.41.2.2.21 Loopback to use on error

This is where you can configure an optional sender address for the error URL to be used instead of the one that would normally be automatically selected for this target address. If you have configured loopback addresses, you can specify them here as sender address.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings

English description: Loopback-To-Use-On-Override

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ (Note: If there is an interface named "DMZ", its address will be taken).
- LBO ... LBF for the 16 loopback addresses
- GUEST
- Any IP address in the form x.x.x.x

Default: Blank



The sender address specified here is used unmasked for every remote station.

2.41.2.3 Profiles

The profile settings for the content filter are located here.

2.41.2.3.1 Profiles

This is where you can create content filter profiles that are used to check web sites for prohibited content. A content filter profile always has a name and, for various time periods, it activates the desired category profile and, optionally, a blacklist and a whitelist.

Telnet path: /Setup/UTM/Content-Filter/Profiles

In order to provide different configurations for the various timeframes, several content-filter profile entries are created with the same name. The content filter profile is thus made up of the sum of all entries with the same name.

The firewall refers to this content-filter profile.



Please note that you must make corresponding settings in the firewall in order to use the profiles in the LANCOM Content Filter.

2.41.2.3.1.1 Name

Enter the name of the content filter profile to be used for referencing in the firewall.

Telnet path: /Setup/UTM/Content-Filter/Profiles

Possible values:

- Name of a profile
- Maximum 31 characters

Default:

Blank

2.41.2.3.1.2 Timeframe

Select the timeframe for the content filter profile. The timeframes "ALWAYS" and "NEVER" are predefined. You can configure other timeframes under: /Setup/Time/Timeframe.

A content-filter profile may have several lines with different timeframes.

Telnet path: /Setup/UTM/Content-Filter/Profiles

Possible values:

- Always
- Never
- Name of a timeframe profile
- Maximum 31 characters

Default: Blank



If timeframes overlap when multiple entries are used for a content filter profile, all pages contained in one of the active entries will be blocked for that period of time. If a period remains undefined when several entries are used for a content filter profile, access to all web sites is unchecked for this period.

2.41.2.3.1.3 Whitelist

Select the whitelist that applies to this content filtering profile. Enter a new name or select an existing entry from the whitelist table.

Telnet path: /Setup/UTM/Content-Filter/Profiles

Possible values:

- Name of an existing whitelist
- Maximum 31 characters

Default: Blank

2.41.2.3.1.4 Blacklist

Select the blacklist that applies to this content filtering profile. Enter a new name or select an existing entry from the blacklist table.

Telnet path: /Setup/UTM/Content-Filter/Profiles

Possible values:

- Name of an existing blacklist
- Maximum 31 characters

Default: Blank

2.41.2.3.1.5 Category profile

Select the category profile that applies to this content filtering profile. Enter a new name or select an existing entry from the table of category profiles.

Telnet path: /Setup/UTM/Content-Filter/Profiles

Possible values:

- Name of a category profile
- Maximum 31 characters

Default: Blank

2.41.2.3.2 Whitelists

This is where you can configure web sites to which access is to be allowed.

Telnet path: /Setup/UTM/Content-Filter/Profiles



Entries for the allowed web sites may contain up to 252 characters. To define longer whitelist entries, a number of entries can use a special, shared name. Enter the name of the whitelist followed by a # character and any suffix. For example, you create three whitelist entries called "MyWhitelist#1", "MyWhitelist#2" and "MyWhitelist#3". In the content filtering profile, you can reference this extended whitelist with the name "MyWhitelist".

2.41.2.3.2.1 Name

Enter the name of the whitelist for referencing from the content-filter profile.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Whitelists

Possible values:

- Name of a whitelist
- Maximum 31 characters

Default:

Blank

2.41.2.3.2.2 Whitelist

This is where you can configure web sites which are to be checked locally and then accepted.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Whitelists

Possible values:

- Valid URL address(es)
- Maximum 252 characters

The following wildcard characters may be used:

- * for any combination of more than one character (e.g. www.lancom.* encompasses the web sites www.lancom.de, www.lancom.eu, www.lancom.es, etc.)
- ? for any one character (e.g. www.lancom.e* encompasses the web sites www.lancom.eu, www.lancom.es)



Please enter the URL without the leading http://. Please note that in the case of many URLs a forward slash is automatically added as a suffix to the URL, e.g. www.mycompany.de/. For this reason it is advisable to enter the URL as: www.mycompany.de*.

Individual URLs are separated by a blank.

Default:

Blank

2.41.2.3.3 Blacklists

This is where you can configure those web sites that are to be blocked.

Telnet path: /Setup/UTM/Content-Filter/Profiles



Entries for the forbidden web sites may contain up to 252 characters. To define longer blacklist entries, a number of entries can use a special, shared name. Enter the name of the blacklist followed by a # character and any suffix. For example, you create three blacklist entries called "MyBlacklist#1", "MyBlacklist#2" and "MyBlacklist#3". In the content filtering profile, you can reference this extended blacklist with the name "MyBlacklist".

2.41.2.3.3.1 Name

Enter the name of the blacklist for referencing from the content-filter profile.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Blacklists

Possible values:

- Blacklist name

- Maximum 31 characters

Default:

Blank

2.41.2.3.3.2 Blacklist

Access to the URLs entered here will be forbidden by the blacklist.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Blacklists

Possible values:

- Valid URL address(es)
- Maximum 252 characters

The following wildcard characters may be used:

- * for any combination of more than one character (e.g. www.lancom.* encompasses the web sites www.lancom.de, www.lancom.eu, www.lancom.es, etc.)
- ? for any one character (e.g. www.lancom.e* encompasses the web sites www.lancom.eu, www.lancom.es)



Please enter the URL without the leading http://. Please note that in the case of many URLs a forward slash is automatically added as a suffix to the URL, e.g. www.mycompany.de/. For this reason it is advisable to enter the URL as: www.mycompany.de*.

Individual URLs are separated by a blank.

Default:

Blank

2.41.2.3.4 Category profiles

Here you create a category profile and determine which categories or groups should be used to rate web sites for each category profile. You can allow or forbid the individual categories or activate the override function for each group.

Telnet path: /Setup/UTM/Content-Filter/Profiles

2.41.2.3.4.1 Name

The name of the category profile for referencing from the content-filter profile is entered here.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

Possible values:

- Name of a category profile
- Maximum 31 characters

Default:

Blank

2.41.2.3.4.100 Unknown

Here you can specify how the content filter is to treat URLs that are unknown to the rating server, and thus are as yet uncategorized.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

Possible values:

Allowed, forbidden, override

Default: Allowed



The category profile must subsequently be assigned to a content-filter profile (together with a time-frame) to become active.

2.41.2.3.4.101 Pornography/Erotic/Sex

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.103 Swimwear/Lingerie

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.104 Shopping

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.105 Auctions/Classified_Ads

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.106 Governmental/Non-Profit_Organizations

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.108 Cities/Regions/Countries

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.109 Education

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.110 Political_Parties

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.111 Religion/Spirituality

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.113 Illegal_Activities

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.114 Computer_Crime/Warez/Hacking

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.115 Political_Extreme/Hate/Discrimination

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.117 Violence/Extreme

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.118 Gambling/Lottery

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.119 Computer_Games

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.120 Toys

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.121 Cinema/Television/Social_Media

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.122 Recreational_Facilities/Theme_Parks

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.123 Arts/Museums/Theaters

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.124 Music/Radio_Broadcast

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.125 Literature/Books

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.126 Humor/Cartoons

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.127 News/Magazines

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.128 Webmail/Unified_Messaging

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.129 Chat

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.130 Blogs/Bulletin_Boards

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.131 Mobile_Telephony

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.132 Digital_Postcards

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.133 Search_Engines/Web_Catalogs/Portals

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.134 Software/Hardware

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.135 Communication_Services

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.136 IT_Security/IT_Information

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.137 Web_Site_Translation

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.138 Anonymous_Proxies

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.139 Illegal_Drugs

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.140 Alcohol/Tobacco

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.143 Dating/Networks

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.144 Restaurants/Entertainment_Venues

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.145 Travel

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.146 Fashion/Cosmetics/Jewelry

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.147 Sports

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.148 Architecture/Construction/Furniture

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.149 Environment/Climate/Pets

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.150 Personal_Web_Sites

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.151 Job_Search

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.152 Finance/Investment

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.154 Banking

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.155 Vehicles

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.156 Weapons/Military

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.157 Medicine/Health/Self-Help

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.158 Abortion

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.160 Spam_URLs

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.161 Malware

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.162 Phishing_URLs

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.163 Instant_Messaging

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.167 General_Business

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.174 Banner_Advertisements

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.41.2.3.4.180 Web_Storage

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

Allowed, forbidden, override

Default:

Allowed

2.42 ADSL

Asymmetrical Digital Subscriber Line - transmission process for high-speed data transmission over normal telephone lines. With ADSL, transmissions (downstream) of up to 6 Mbps can be implemented over normal telephone lines; for bidirectional transmission there is a second frequency band with transmission speeds of up to 640 kbps (upstream) - hence the name "asymmetric".

Telnet path: /Setup

2.42.1 Trace mode

The trace mode determines whether values issued by the ADSL trace also include internal status values (extended) or the line status (simple) only.

Telnet path: /Setup/ADSL/Trace-Mode

Possible values:

- Simple
- Extended

Default: Extended



The default value is 'Simple' as of firmware version 8.20.

2.42.4 Monitoring time (h)

This parameter specifies the monitoring time in hours.

Line failures (2.42.3 Line-Failures) and monitoring time are a part of the ADSL-auto mode. Together they indicate how many line failures are allowed within a certain time to accept a line code as functional and stable.

In case of line failures, the first loss of sync is not counted if it occurs within the first minute. If the permitted number of line failures exceeds the monitoring period, the device selects another line code.

Telnet path: /Setup/ADSL/Monitoring-Time(h)

Possible values:

- Max. 5 numerical characters

Default: 24



If you set the line code in the configuration, the device ignores this setting.

2.42.3 Line failures

This parameter specifies the maximum allowed number of line failures.

Line failures and monitoring time (2.42.4 Monitoring-Time(h)) are part of the ADSL-auto mode. Together they indicate how many line failures are allowed within a certain time to accept a line code as functional and stable.

In case of line failures, the first loss of sync is not counted if it occurs within the first minute. If the permitted number of line failures exceeds the monitoring period, the device selects another line code.

Telnet path: /Setup/ADSL/Line-failures

Possible values:

- Max. 2 numerical characters

Default: 1



If you set the line code in the configuration, the device ignores this setting.

2.52 COM ports

This menu contains the configuration of the COM ports.

Telnet path: /Setup

2.52.1 Devices

The serial interfaces in the LANCOM can be used for various applications, for example for the COM port server or as a WAN interface. The Devices table allows individual serial devices to be assigned to certain applications.

Telnet path: /Setup/COM-Ports

2.52.1.1 Device type

Selects a serial interface from the list of those available in the device.

Telnet path: /Setup/COM-Ports/Devices

Possible values:

- All available serial interfaces.

Default: Outband

2.52.1.4 Service

Activation of the port in the COM port server.

Telnet path: /Setup/COM-Ports/Devices

Possible values:

- WAN
- COM-port server

Default: WAN

2.52.2 COM-port server

This menu contains the configuration of the COM-port server.

Telnet path: /Setup/COM-Ports

2.52.2.1 Operational

This table activates the COM port server at a port of a certain serial interface. Add an entry to this table to start a new instance of the COM port server. Delete an entry to stop the corresponding server instance.

Telnet path: /Setup/COM-Ports/COM-Port-Server

2.52.2.1.1 Device type

Selects a serial interface from the list of those available in the device.

Telnet path: /Setup/COM-Ports/COM-Port-Server/Device-Type

Possible values:

- All available serial interfaces.

Default: Outband

2.52.2.1.2 Port number

Some serial devices such as the CardBus have more than one serial port. Enter the port number that is to be used for the COM port server on the serial interface.

Telnet path: /Setup/COM-Ports/COM-Port-Server/Device-Type

Possible values:

■ Max. 10 characters

Default: 0

Special values: 0 for serial interfaces with just one port, e.g. outband.

2.52.2.1.4 Operating

Activates the COM port server on the selected port of the selected interface.

Telnet path: /Setup/COM-Ports/COM-Port-Server/Device-Type

Possible values:

■ Yes

■ No

Default: No

2.52.2.2 COM-port settings

This table contains the settings for data transmission over the serial interface.

Please note that all of these parameters can be overwritten by the remote site if the RFC2217 negotiation is active. Current settings can be viewed in the status menu.

Telnet path: /Setup/COM-Ports/COM-Port-Server

2.52.2.2.1 Device type

Selects a serial interface from the list of those available in the device.

Telnet path: LCOS Menu Tree/Setup/COM-Ports/COM-Port-Server/COM-Port-Settings

Possible values:

■ All available serial interfaces.

Default: Outband

2.52.2.2.10 Ready data timeout

The timeout switches the port back to the not-ready status if no data is received. This function is deactivated when timeout is set to zero. In this case the port is always ready if the data mode is selected.

Telnet path: LCOS Menu Tree/Setup/COM-Ports/COM-Port-Server/COM-Port-Settings

Possible values:

■ Max. 10 characters

Default: 0

Special values: 0 switches the Ready-data-timeout off.

2.52.2.2.2 Port number

Some serial devices such as the CardBus have more than one serial port. Enter the port number that is to be used for the COM port server on the serial interface.

Telnet path: LCOS Menu Tree/Setup/COM-Ports/COM-Port-Server/COM-Port-Settings

Possible values:

■ Max. 10 characters

Default: 0

Special values: 0 for serial interfaces with just one port, e.g. outband.

2.52.2.2.4 Bit rate

Bitrate used on the COM port

Telnet path: LCOS Menu Tree/Setup/COM-Ports/COM-Port-Server/COM-Port-Settings

Possible values:

- 110 to 230400

Default: 9600**2.52.2.2.5 Data bits**

Number of data bits.

Telnet path: LCOS Menu Tree/Setup/COM-Ports/COM-Port-Server/COM-Port-Settings**Possible values:**

- 7
- 8

Default: 8**2.52.2.2.6 Parity**

The checking technique used on the COM port.

Telnet path: LCOS Menu Tree/Setup/COM-Ports/COM-Port-Server/COM-Port-Settings**Possible values:**

- None
- Even
- Odd

Default: None**2.52.2.2.7 Stop bits**

Number of stop bits.

Telnet path: LCOS Menu Tree/Setup/COM-Ports/COM-Port-Server/COM-Port-Settings**Possible values:**

- 1
- 2

Default: 1**2.52.2.2.8 Handshake**

The data-flow control used on the COM port.

Telnet path: LCOS Menu Tree/Setup/COM-Ports/COM-Port-Server/COM-Port-Settings**Possible values:**

- none
- RTS/CTS

Default: RTS/CTS**2.52.2.2.9 Ready condition**

The ready condition is an important property of any serial port. The COM port server transmits no data between the serial port and the network if the status is not "ready". Apart from that, in the client mode the act of switching between the ready and not-ready status is used to establish and terminate TCP connections. The readiness of the port can be checked in two different ways. In DTR mode (default) only the DTR handshake is monitored. The serial interface is considered to be ready for as long as the DTR line is active. In data mode, the serial interface is considered to be active for as long as it receives data. If no data is received during the timeout period, the port reverts to its not-ready status.

Telnet path: LCOS Menu Tree/Setup/COM-Ports/COM-Port-Server/COM-Port-Settings**Possible values:**

- DTR
- Data

Default: DTR

2.52.2.3 Network settings

This table contains all settings that define the behavior of the COM port in the network.

Please note that all of these parameters can be overwritten by the remote site if the RFC2217 negotiation is active. Current settings can be viewed in the status menu.

Telnet path: /Setup/COM-Ports/COM-Port-Server

2.52.2.3.1 Device type

Selects a serial interface from the list of those available in the device.

Telnet path: /Setup/COM-Ports/COM-Port-Server/Network-Settings

Possible values:

- All available serial interfaces.

Default: Outband

2.52.2.3.10 Newline conversion

Here you select the character to be output by the serial port when binary mode is activated.

This setting is independent of the application communicating via the serial port. If the port is connected to another LANCOM device, you can either enter CRLF here or just CR. This is because the outband interface of these devices expects a "carriage return" for the automatic determination of data-transfer speed. However, some Unix applications interpret CRLF as a prohibited double line feed character. In these cases enter either CR or LF.

Telnet path: /Setup/COM-Ports/COM-Port-Server/Network-Settings

Possible values:

- CRLF
- CR
- LF

Default:

CRLF



This setting is only relevant if binary mode is deactivated for this port.

2.52.2.3.11 Assume binary mode

Some network devices connected to a serial COM port transmit data structures which may be interpreted as control characters (CR/LF – carriage return / line feed). In the default setting, the COM-ports in LANCOM devices process this information to control the data flow. "Binary mode" instructs a COM port to forward the data in binary format and ignore any control characters.

Telnet path: /Setup/COM-Ports/COM-Port-Server/Network-Settings

Possible values:

- Yes
- No

Default: No

2.52.2.3.12 TCP retransmit timeout

Maximum time for the retransmission timeout. This timeout defines the interval between checking TCP-connection status and reporting the result to the application using the TCP connection.

Telnet path: /Setup/COM-Ports/COM-Port-Server/Network-Settings

Possible values:

- 0 to 99 seconds
- Maximum 2 characters

Special values:

- 0 activates the RFC 1122 default value (60 seconds).

Default:

- 0



The maximum duration of the TCP-connection check is the product of TCP-retransmit-count and TCP-retry-count. The TCP application is only informed after the timeout for all attempts has expired. With the default values of 60 seconds timeout and max. 5 attempts, it can take up to 300 seconds before the application is informed about an inactive TCP connection.

2.52.2.3.13 TCP retry count

The maximum number of attempts for checking TCP-connection status and reporting the result to the application using the TCP connection.

Telnet path: /Setup/COM-Ports/COM-Port-Server/Network-Settings

Possible values:

- 0 to 9
- Maximum 1 characters

Special values:

- 0 activates the RFC 1122 default value (5 attempts).

Default:

- 0



The maximum duration of the TCP-connection check is the product of TCP-retransmit-count and TCP-retry-count. The TCP application is only informed after the timeout for all attempts has expired. With the default values of 60 seconds timeout and max. 5 attempts, it can take up to 300 seconds before the application is informed about an inactive TCP connection.

2.52.2.3.14 TCP keepalive

The RFC 1122 sets down a method of checking the availability of TCP connections, called TCP keepalive. An inactive transmitter queries the receive status from the remote station. If the TCP session to the remote site is available, then the remote responds with its receive status. If the TCP session to the remote site is not available, then the query is repeated for as long as it takes for the remote to respond with its receive status (after which a longer interval comes into play). As long as the basic connection functions, but the TCP session to the remote station is not available, then the remote station sends an RST packet which triggers the establishment of the TCP session by the requesting application.

Telnet path: /Setup/COM-Ports/COM-Port-Server/Network-Settings

Possible values:

- Inactive: TCP keepalive is not used.
- Active: TCP keepalive is active; only RST packets cause the disconnection of TCP sessions.
- Proactive: TCP keepalive is active, but the request for the receive status from the remote site is only repeated for the number of times defined under "TCP retry count". If this number of requests expires without a response with the receive status, then the TCP sessions is classified as "not available" and the application is informed. If an RST packet is received during the wait time, the TCP session will be disconnected prematurely.

Default:

- Inactive



The setting "active" is recommended for server applications.

2.52.2.3.15 TCP keepalive interval

This value defines the interval between sending requests for receive status if the first request is not affirmed. The associated timeout is defined as being interval/3 (max. 75 sec.).

Telnet path: /Setup/COM-Ports/COM-Port-Server/Network-Settings

Possible values:

- Maximum 10 characters.

Default:

- 0

Special values:

- 0 activates the RFC 1122 default values (interval 7200 seconds, timeout 75 seconds).

2.52.2.3.2 Port number

Some serial devices such as the CardBus have more than one serial port. Enter the port number that is to be used for the COM port server on the serial interface.

Telnet path: /Setup/COM-Ports/COM-Port-Server/Network-Settings

Possible values:

- Max. 10 characters

Default: 0

Special values: 0 for serial interfaces with just one port, e.g. outband.

2.52.2.3.4 TCP mode

Each instance of the COM port server in server mode monitors the specified listen port for incoming TCP connections. Just one active connection is permitted per instance. All other connection requests are refused. In client mode, the instance attempts to establish a TCP connection via a defined port to the specified remote site, as soon as the port is ready. The TCP connection is closed again as soon as the port becomes unavailable. In both cases a LANCOM closes any open connections when the device is restarted.

Telnet path: /Setup/COM-Ports/COM-Port-Server/Network-Settings

Possible values:

- Server
- Client

Default: Server

2.52.2.3.5 Listen port

The TCP port where the COM port in TCP server mode expects incoming connections.

Telnet path: /Setup/COM-Ports/COM-Port-Server/Network-Settings

Possible values:

- Max. 10 characters

Default: 0

2.52.2.3.6 Connect host name

The COM port in TCP client mode establishes a connection to this host as soon as the port is in "Ready" status.

Telnet path: /Setup/COM-Ports/COM-Port-Server/Network-Settings

Possible values:

- DNS-Name
- IP address

Default: Blank

2.52.2.3.7 Connect port

The COM port in TCP client mode uses this TCP port to establish a connection as soon as the port is in "Ready" state.

Telnet path: /Setup/COM-Ports/COM-Port-Server/Network-Settings

Possible values:

- Max. 10 characters

Default: 0

2.52.2.3.8 Loopback address

The COM port can be reached at this address. This is its own IP address that is given as the source address when establishing connections. This is used to define the IP route to be used for the connection.

Telnet path: /Setup/COM-Ports/COM-Port-Server/Network-Settings

Possible values:

- Max. 16 characters

Default: Blank

2.52.2.3.9 RFC2217 extensions

The RFC2217 extensions can be activated for both TCP modes. With these extensions activated, the LANCOM uses the IAC DO COM-PORT-OPTION sequence to signal that it will accept Telnet control sequences. The COM port subsequently works with the corresponding options; the configured default values are overwritten. The port also attempts to negotiate the local echo and line mode for Telnet. Using the RFC2217 extensions with incompatible remote sites is not critical. Unexpected characters may be displayed at the remote site. A side effect of using the RFC2217 extensions may be that the port regularly carries out an alive check as Telnet NOPs are transmitted to the remote site.

Telnet path: /Setup/COM-Ports/COM-Port-Server/Network-Settings

Possible values:

- Yes
- No

Default: Yes

2.52.3 WAN

This menu contains the configuration of the Wide Area Network (WAN).

Telnet path: /Setup/COM-Ports

2.52.3.1 Devices

The table with WAN devices is a status table only. All Hotplug devices (connected via USB or CardBus) enter themselves into this table.

Telnet path: /Setup/COM-Ports/WAN

2.52.3.1.1 Device type

List of serial interfaces available in the device.

Telnet path: /Setup/COM-Ports/WAN/Devices

Possible values:

- All available serial interfaces.

2.52.3.1.3 Operating

Status of connected device.

Telnet path: /Setup/COM-Ports/WAN/Devices

Possible values:

- Yes
- No

2.53 Temperature monitor

The settings for the temperature monitor are located here.

Telnet path: /Setup/Temperature-Monitor

2.53.1 Upper-limit degrees

When the temperature set here is exceeded, the device sends an SNMP trap of the type "trpTempMonOver-Temp".

Telnet path: /Setup/Temperature-Monitor/Upper-Limit-Degrees

Possible values:

- 0 – 127 ° Celsius

Default: 70

2.53.2 Lower-limit degrees

When the temperature drops below that set here, the device sends an SNMP trap of the type "trpTempMonUnderTemp".

Telnet path: /Setup/Temperature-Monitor/Upper-Limit-Degrees

Possible values:

■ 0 – 127 ° Celsius

Default: 0

2.54 TACACS

2.54.3 Accounting

WEBconfig: /Setup/Tacacs+

Activates accounting via TACACS+ server. If TACACS+ accounting is activated, all accounting data is transmitted via TACACS+ protocol to the configured TACACS+ server.

Possible values: Activated, deactivated

Default: Deactivated



TACACS+ accounting will only activate if the defined TACACS+ server is available.

2.54.1 Authentication

WEBconfig: /Setup/Tacacs+

WEBconfig English: LCOS Menu Tree/Setup/TACACS+

Activates authentication via TACACS+ server. If TACACS+ authentication is activated, all authentication data is transmitted via TACACS+ protocol to the configured TACACS+ server.

Possible values: Activated, deactivated

Default: Deactivated



TACACS+ authentication will only activate if the defined TACACS+ server is available. Fallback to local users is only possible if a root password has been set for the LANCOM. The fallback to local users must be deactivated for devices without a root password. Otherwise a failure of the network connection (TACACS+ server unavailable) would make the LANCOM accessible without a password.

2.54.2 Authorization

WEBconfig: /Setup/Tacacs+

WEBconfig English: LCOS Menu Tree/Setup/TACACS+

Activates authorization via TACACS+ server. If TACACS+ authorization is activated, all authorization data is transmitted via TACACS+ protocol to the configured TACACS+ server.

Possible values: Activated, deactivated

Default: Deactivated



TACACS+ authorization will only activate if the defined TACACS+ server is available. If TACACS+ authorization is activated, the TACACS+ server will be queried for authorization each time a user enters a command. Data traffic during configuration will increase correspondingly. Also, the user rights must be defined in the TACACS+ server.

2.54.10 Fallback to local users

WEBconfig: /Setup/Tacacs+

WEBconfig English: LCOS Menu Tree/Setup/TACACS+

Should the defined TACACS+ server be unavailable, it is possible to fallback to local user accounts on the LANCOM. This allows for access to the device even if the TACACS+ connection should fail, e.g. when deactivating the usage of TACACS+ or for correcting the configuration.

Possible values: Allowed, prohibited

Default: Allowed



The fallback to local user accounts presents a security risk if no root password is set for the LANCOM. For this reason, TACACS+ authentication with fallback to local user accounts can only be activated if a root password has been set. If no root password is set, access to the device configuration can be blocked for security reasons if no connection is available to the TACACS+ server. In this case, the device may have to be reset to its factory settings in order to regain access to the configuration.

2.54.6 Shared secret

WEBconfig: /Setup/Tacacs+

The password for encrypting the communications between NAS and TACACS+ servers.

Possible values: 31 alphanumeric characters

Default: Blank



The password must be entered identically into the LANCOM and the TACACS+ server. We recommend that you do not operate TACACS+ without encryption.

2.54.12 SNMP-GET requests accounting

WEBconfig: /Setup/Tacacs+**WEBconfig English:** LCOS Menu Tree/Setup/TACACS+

Numerous network management tools use SNMP for requesting information from network devices. LANmonitor also uses SNMP to access the LANCOM devices to display information about current connections, etc., or to execute actions such as disconnecting a connection. SNMP can be used to configure devices. For this reason TACACS+ requires authentication for SNMP access requests. Since LANmonitor regularly queries these values, a large number of unnecessary TACACS+ connections would be established. If authentication, authorization and accounting by TACACS+ are activated, then each request would initiate three sessions with the TACACS+ server.

This parameter allows the regulation of the behavior of LANCOM devices with regard to SNMP access in order to reduce the number of TACACS+ sessions required for accounting. Authentication via the TACACS+ server remains necessary if authentication for TACACS+ is activated generally.



Entering a read-only community under /Setup/SNMP also enables authentication by TACACS+ to be deactivated for LANmonitor. The read-only community defined here is then entered into LANmonitor as a user name.

Possible values:

- **only_for_SETUP_tree:** With this setting, accounting via TACACS+ server is only required for SNMP access via the setup branch of LCOS.
- **All:** With this setting, accounting by TACACS+ server will be carried out for every SNMP access. In case of regular request for status information, for example, the load on the TACACS+ server will increase significantly.
- **None:** With this setting, accounting by TACACS+ server will not be carried out for SNMP accesses.

Default: only_for_SETUP_tree

2.54.11 SNMP-GET requests authorization

WEBconfig: /Setup/Tacacs+**WEBconfig English:** LCOS Menu Tree/Setup/TACACS+

This parameter allows the regulation of the behavior of LANCOM devices with regard to SNMP access in order to reduce the number of TACACS+ sessions required for authorization. Authentication via the TACACS+ server remains necessary if authentication for TACACS+ is activated generally.

Possible values:

- **only_for_SETUP_tree:** With this setting, authorization via TACACS+ server is only required for SNMP access via the setup branch of LCOS.
- **All:** With this setting, authorization by TACACS+ server will be carried out for every SNMP access. In case of regular request for status information, for example, the load on the TACACS+ server will increase significantly.
- **None:** With this setting, authorization by TACACS+ server will not be carried out for SNMP accesses.

Default: only_for_SETUP_tree

2.54.13 Bypass-Tacacs-for-CRON/Scripts/Action-table

You can activate or deactivate the bypassing of TACACS+ authorization and TACACS+ accounting for various actions.

Telnet path: /Setup/Tacacs+

Possible values:

- Activated
- Deactivated

Default: Deactivated



Please observe that this option influences the TACACS+ function for the entire system. Be sure that you restrict the use of CRON, the action tables, and scripts only to an absolutely trustworthy circle of administrators!

2.54.7 Encryption

WEBconfig: /Setup/Tacacs+

WEBconfig English: LCOS Menu Tree/Setup/TACACS+

Activates or deactivates the encryption of communications between NAS and TACACS+ servers.

Possible values:

- Activated
- Deactivated

Default: Activated



We recommend that you do not operate TACACS+ without encryption. If encryption is activated here, the password for encryption entered here must match with the password on the TACACS+ server.

2.54.14 Include value into authorization request

If you deactivate this function, then TACACS + only checks the rights of the user on login. When entering values, the device no longer checks whether the user has permission to change certain values.

Telnet path: /Setup/Tacacs+/Include-value-into-authorization

Possible values:

- **Activated:** When values are submitted, TACACS + checks whether the user has the right to make these changes
- **Deactivated:** TACACS + checks the identity of the user only on login

Default: Activated

2.54.9 Server

Two servers can be defined to work with TACACS+ functions. One server acts as a backup in case the other one fails. When logging in via telnet or WEBconfig, the user can select the server to be used.

This menu contains the settings for TACACS servers.

Telnet path: /Setup/Tacacs+

2.54.9.1 Server address

Address of the TACACS+ server to which requests for authentication, authorization and accounting are to be forwarded.

Telnet path: /Setup/Tacacs+/Server/Server-Address

Possible values:

- Valid DNS resolvable name or valid IP address.

Default: Blank

2.54.9.2 Loopback address

Optionally you can configure a loopback address here.

Telnet path: /Setup/Tacacs+/Server/Loopback-Address

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LBO to LBF for the 16 loopback addresses
- Any valid IP address

Default: Blank

2.54.9.3 Compatibility mode

TACACS+ servers are available as open-source or commercial versions, each of which works with different messages. The compatibility mode enables the processing of messages from free TACACS+ servers.

Telnet path: /Setup/Tacacs+/Server/Compatibility-Mode

Possible values:

- Activated
- Deactivated

Default: Deactivated

2.56 Autoload

This menu is used to configure the automatic uploading of firmware or configurations from external data media.

Telnet path: /Setup/Autoload

2.56.1 Firmware and loader

This option activates the automatic loading of loader and/or firmware files from a connected USB medium.

Telnet path: /Setup/Autoload/Firmware-and-loader

Possible values:

- Inactive: Automatic loading of loader and/or firmware files is deactivated.
- Active: Automatic loading of loader and/or firmware files is activated. When a USB medium is mounted, a suitable loader and/or firmware file is uploaded to the device. The USB medium is mounted when it is plugged into the USB connector on the device, or when it is restarted.

- If-unconfigured Automatic loading of loader and/or firmware files is only activated when the device has its factory settings. A configuration reset can be used to return the device to its factory settings at any time.

Default:

- If-unconfigured



This option is set to "inactive" in the Security Settings Wizard or the Basic Settings Wizard.

2.56.2 Configuration and script

This option activates the automatic loading of configuration and/or script files from a connected USB medium.

Telnet path: /Setup/Autoload/Config-and-script

Possible values:

- Inactive: Automatic loading of configuration and/or script files is deactivated.
- Active: Automatic loading of configuration and/or script files is activated. When a USB medium is mounted, a suitable configuration and/or script file is uploaded to the device. The USB medium is mounted when it is plugged into the USB connector on the device, or when it is restarted.
- If-unconfigured Automatic loading of configuration and/or script files is only activated when the device has its factory settings. A configuration reset can be used to return the device to its factory settings at any time.

Default:

- If-unconfigured



This option is set to "inactive" in the Security Settings Wizard or the Basic Settings Wizard.



A device can be fed with an undesirable configuration by resetting it to its factory settings and inserting a prepared USB data media. To prevent this you have to deactivate the reset switch.

2.59 WLAN management

This menu is used to configure the WLAN management.

2.59.120 Log entries

This parameter defines the maximum number of log entries for the device.

Telnet path: /Setup/WLAN-Management/Log-Entries

Possible values:

- 0 to 9999

Default: 200

2.59.1 Static WLC configuration

Use this table to define the preferred wireless LAN controllers (WLCs) that this managed access point should contact. This setting is not required if the access point and WLC are located in the same IP network.

This setting is only relevant if at least one of the device's WLAN interfaces is switched to the 'Managed' operating mode.

Telnet path: /Setup/WLAN-Management/Static-WLC-Configuration

2.59.1.1 IP address

This is where the name of the CAPWAP service is defined that is used to trigger the WLAN controller via the DNS server.

The name is preset, so you do not need to change anything here. However, this parameter does offer the option of using the CAPWAP service of other manufacturers.

Telnet path: /Setup/WLAN-Management/Static-WLC-Configuration/IP-Address

Possible values:

- Valid IP address or resolvable name of a WLC controller

Default: WLC address

2.59.1.2 Port

The port to be used for communication with the WLAN controller is set here.

Telnet path: /Setup/WLAN-Management/Static-WLC-Configuration/Port

Possible values:

- Valid port descriptor

Default: 1027

2.59.1.3 Loopback address

This is where you can configure an optional sender address to be used instead of the one otherwise automatically selected for the destination address.

If you have configured loopback addresses, you can specify them here as sender address.

Telnet path: /Setup/WLAN-Management/Static-WLC-Configuration/Loopback-Addr.

Possible values:

- Name of the IP networks whose addresses are to be used.
- "INT" for the address of the first intranet.
- "DMZ" for the address of the first DMZ (Note: If there is an interface named "DMZ", its address will be taken).
- LBO ... LBF for the 16 loopback addresses.
- Furthermore, any IP address can be entered in the form x.x.x.x.

Default: Blank



The sender address specified here is used **unmasked** for every remote station.

2.60 Autoload

This menu is used to set up the automatic uploading of firmware, configurations or scripts from external data media or from a URL.

Telnet path: /Setup/Autoload

2.60.1 Network

This menu is used to configure the automatic uploading of firmware, configurations or scripts over the network.

The settings made in this area are used when the commands LoadFirmware, LoadConfig or LoadScript are invoked from the command line. These commands upload firmware, configurations or scripts to the device using the TFTP or HTTP(S) client.

Telnet path: /Setup/Autoload/Network



Loading firmware, configurations or scripts using the TFTP or HTTP(S) client can only succeed if the URL required to load the relevant file is fully configured and the URL is accessible when the command is executed. Alternatively, the URL can be entered as a parameter when the command is executed.



The values for Condition, URL and Minimum-Version set under /Setup/Autoload/Network constitute default values. These values are only used in cases where no other appropriate parameters are entered when the commands LoadFirmware, LoadConfig or Load Script are invoked on the command line.

2.60.1.1 Firmware

This menu is used to configure the automatic uploading of firmware over the network.

Telnet path: /Setup/Autoload/Network/Firmware

2.60.1.1.1 Condition

This is where you select the condition under which the firmware specified under /Setup/Autoload/Network/Firmware/URL will be uploaded when the command LoadFirmware is executed.

Telnet path: /Setup/Autoload/Network/Firmware

Possible values:

- Unconditionally: The firmware will always be uploaded to and executed from the memory location of the inactive firmware. This setting deactivates version checking and the firmware specified will be uploaded in every case.
- If different: The firmware is uploaded to and executed from the memory location for the inactive firmware if it is of a different version to the firmware active in the device and the inactive firmware. If the specified firmware is of the same version as one of the two existing firmware versions, then the firmware will not be uploaded. The LoadFirmware command compares the firmware version (e.g. "8.10"), the release code (e.g. "RU1") and the file date.
- If newer: The firmware is uploaded and executed only if it is newer than the firmware currently active in the device. The firmware is only uploaded to the memory location for the inactive firmware if it is newer than the active and inactive firmware versions on the device. If the specified firmware is older than one of the two existing firmware versions, then it will not be uploaded.

Default: Unconditionally



If the command LoadFirmware is executed twice in succession with the setting "unconditionally", both memory locations will contain the same firmware version.

2.60.1.1.2 Minimum version

Specify the minimum version of the firmware to be loaded over the network.

Telnet path: /Setup/Autoload/Network/Minimum-Version

Possible values:

- Max. 14 characters

Default: Blank



Firmware versions with a lower version number will be ignored.

2.60.1.1.3 URL

Specify the URL of the firmware that is to be uploaded over the network using the LoadFirmware command.

Telnet path: /Setup/Autoload/Firmware/URL

Possible values:

- Max. 127 characters beginning with "tftp://", "http://" or "https://"

Default: Blank



The TFTP or HTTP(S) client loads the file entered here only if the LoadFirmware command is entered without a URL as a parameter. A specific file at a known location can be loaded by entering its URL as a parameter.

2.60.1.2 Configuration

This menu is used to configure the automatic uploading of a configuration over the network.

Telnet path: /Setup/Autoload/Network/Configuration

2.60.1.2.1 Condition

This is where you select the condition under which the configuration specified under /Setup/Autoload/Network/Configuration/URL will be uploaded when the device is started.

Telnet path: /Setup/Autoload/Network/Configuration

Possible values:

- Unconditionally: The configuration will always be uploaded.
- If different: The configuration will only be uploaded if it has a different version number than the configuration that is currently active in the device.

Default: Unconditionally

2.60.1.2.3 URL

Specify the URL of the configuration that is to be uploaded over the network using the LoadConfig command.

Telnet path: /Setup/Autoload/Configuration/URL

Possible values:

- Max. 127 characters beginning with "tftp://", "http://" or "https://"

Default: Blank



The TFTP or HTTP(S) client loads the file entered here only if the LoadConfig command is entered without additional parameters. Defining appropriate parameters when the command is invoked allows a specific file to be loaded.

2.60.1.3 Script

This menu is used to configure the automatic uploading of a script over the network.

Telnet path: /Setup/Autoload/Network/Script

2.60.1.3.1 Condition

This is where you select the condition under which the script specified under /Setup/Autoload/Network/Configuration/URL will be uploaded when the command LoadScript is executed.

Telnet path: /Setup/Autoload/Network/Script

Possible values:

- Unconditionally: The script will always be executed. This setting deactivates the checksum comparison and the specified script will always be uploaded unconditionally. In this case, the LoadScript command does not change the checksum for the most recently executed scripts as stored in the device.
- If different: The script will only be executed if it differs from the last executed script. The difference to the last executed script is determined using a checksum. For this the complete script is always uploaded. The LoadScript command then compares the checksum of the uploaded script with the checksum of the last executed script stored in the device. When the script is executed, the LoadScript command updates the checksum stored in the device.

Default: Unconditionally

2.60.1.3.3 URL

Specify the URL of the script that is to be uploaded over the network using the LoadFirmware command.

Telnet path: /Setup/Autoload/Script/URL

Possible values:

- Max. 127 characters beginning with "tftp://", "http://" or "https://"

Default: Blank



The TFTP or HTTP(S) client loads the file entered here only if the LoadScript command is entered without additional parameters. Defining appropriate parameters when the command is invoked allows a specific file to be loaded.

2.60.1.4 TFTP client

This menu contains the configuration for the TFTP client.

Telnet path: /Setup/Autoload/Network/TFTP-Client

2.60.1.4.1 Bytes per hashmark

This setting determines the number of bytes successfully loaded by the TFTP client after which a hash sign (#) is output on the command line when running LoadFirmware, LoadConfig or LoadScript. The TFTP client uses these hash marks to produce a progress bar when uploading firmware, configurations or scripts.

Telnet path: /Setup/Autoload/Network/TFTP-Client

Possible values:

- 4 characters

Default: 8192



This value is used only when loading with TFTP, not HTTP or HTTPS. With HTTP or HTTPS a hash mark is displayed at least every 100ms to display progress.

2.60.56 USB

This menu is used to configure the automatic uploading of firmware or configurations from external data media.

Telnet path: /Setup/Autoload/USB

2.60.56.1 Firmware and loader

This option activates the automatic loading of loader and/or firmware files from a connected USB medium. Save the required loader and/or firmware files in the "Firmware" directory located in the root directory of the connected USB media.

Telnet path: /Setup/Autoload/USB

Possible values:

- Inactive: Automatic loading of loader and/or firmware files is deactivated.
- Active: Automatic loading of loader and/or firmware files is activated. When a USB medium is mounted, a suitable loader and/or firmware file is uploaded to the device. The USB medium is mounted when it is plugged into the USB connector on the device, or when it is restarted.
- If-unconfigured: Automatic loading of loader and/or firmware files is only activated when the device has its factory settings. A configuration reset can be used to return the device to its factory settings at any time.

Default:

- If-unconfigured



This option is set to "inactive" in the Security Settings Wizard or the Basic Settings Wizard.

2.60.56.2 Configuration and script

This option activates the automatic loading of configuration and/or script files from a connected USB medium. Save the required configuration and/or script files in the "Config" directory located in the root directory of the connected USB media.

Telnet path: /Setup/Autoload/USB

Possible values:

- Inactive: Automatic loading of configuration and/or script files is deactivated.
- Active: Automatic loading of configuration and/or script files is activated. When a USB medium is mounted, a suitable configuration and/or script file is uploaded to the device. The USB medium is mounted when it is plugged into the USB connector on the device, or when it is restarted.
- If-unconfigured Automatic loading of configuration and/or script files is only activated when the device has its factory settings. A configuration reset can be used to return the device to its factory settings at any time.

Default:

- If-unconfigured



This option is set to "inactive" in the Security Settings Wizard or the Basic Settings Wizard.



A device can be fed with an undesirable configuration by resetting it to its factory settings and inserting a prepared USB data media. To prevent this you have to deactivate the reset switch.

3 Firmware

This menu contains the actions and settings options for managing the device firmware.

Telnet path: /Firmware

3.7 Feature word

Displays the feature bits that provide information on the options activated in the device.

Telnet path: /Firmware/Feature-Word

3.3 Firmsafe mode

Only one of the two firmware versions stored in the device can be active at any time. When new firmware is uploaded, the currently inactive firmware version will be overwritten. The firmsafe mode lets you decide which firmware is to be activated after the upload.

Possible values:

- Immediate: This option allows you to upload the new firmware and activate it immediately. The following situations can arise:
 - The new firmware is uploaded successfully and it then becomes active as desired. Everything is OK.
 - After uploading the firmware the device no longer responds. If an error occurred during the upload, the device will automatically activate the previous firmware and will restart.
- Login: To respond to the problems of a faulty upload, there is a second option to upload and immediately activate the firmware.
 - In contrast to the first variant, the device then waits for firmsafe timeout while waiting for a successful login via telnet, a terminal program or WEBconfig. Only after this login is the firmware activated.
 - If the device stops responding or it is not possible to login, then the old firmware is activated automatically and the device starts again.
- Manually: The third option allows you set a time period in which you can test the new firmware. The device starts with the new firmware and waits for the set time period for the uploaded firmware to be activated manually, in which case it will be activated permanently. Under LANconfig you activate the new firmware with Device > Firmware management > Release tested firmware, under telnet under 'Firmware/Firmsafe-Table' with the command 'set # active', where # is the position of the firmware in the firmsafe table. Under WEBconfig you will find the firmsafe table under Firmware in the Expert configuration.

Default:

- Immediate

It is only possible to upload a second firmware if the device has sufficient memory available for two complete firmware versions. Up-to-date firmware versions (with additional software options, if applicable) may take up more than half of the available memory in older hardware models. In this case these device uses the asymmetric Firmsafe.

Telnet path: /Firmware/Firmsafe-Mode

3.4 Firmsafe timeout

The time in seconds for testing new firmware.

Possible values:

- 0 to 99999 seconds.

Default:

- 300 seconds

Telnet path: /Firmware/Timeout-Firmsafe

3.1 Version table

This table contains information about the firmware version and serial number of the device.

Telnet path: /Firmware/Version-Table

3.1.1 Interface

The interface referred to by the entry.

Telnet path: /Firmware/Version-Table/Ifc

3.1.2 Module

Full description of the device type.

Telnet path: /Firmware/Version-Table/Module

3.1.3 Version

The firmware version currently active in the device, along with the release date.

Telnet path: /Firmware/Version-Table/Version

3.1.4 Serial number

The device serial number.

Telnet path: /Firmware/Version-Table/Serial-Number

3.2 Table Firmsafe

For each of the two firmware versions stored in the device, this table contains information on the memory space number (1 or 2), the status (active or inactive), the firmware version number, the date, the size, and the index (sequential number).

Telnet path: /Firmware/Table- Firmsafe

3.2.1 Position

Position in memory space of the current entry.

Telnet path: /Firmware/Table- Firmsafe/Position

3.2.2 Status

Status of the current entry.

Possible values:

- Inactive: This firmware is in a wait state and can be activated.
- Active: This firmware is currently in use in the device.
- Loader: This entry is not a firmware version but a loader with offering supporting functions.

Telnet path: /Firmware/Table- Firmsafe/Status

3.2.3 Version

Version descriptor of the firmware for the current entry.

Telnet path: /Firmware/Table- Firmsafe/Version

3.2.4 Date

Release date of the firmware for the current entry.

Telnet path: /Firmware/Table- Firmsafe/Date

3.2.5 Size

Size of the firmware for the current entry.

Telnet path: /Firmware/Table- Firmsafe/Size

3.2.6 Index

Index for the current entry.

Telnet path: /Firmware/Table- Firmsafe/Index

4 Other

This menu contains additional functions from the LCOS menu tree.

Telnet path: Other

4.5 Cold boot

This action is used to reboot the device.

Telnet path: /Other/Cold-Boot

4.2 System boot

This action is used to manually reboot the device.

Telnet path: /Other/Boot-System

4.1 Manual dialing

This menu contains the actions for manual connection establishment.

Telnet path: /Other/Manual-Dialing

4.1.2 Disconnect

This action causes a connection to a remote site to be disconnected.

For the action parameter you can enter the name of the corresponding remote site.

Telnet path: /Other/Manual-Dialing/Disconnect

4.1.1 Connect

This action prompts a connection to be established to a remote site.

For the action parameter you can enter the name of the corresponding remote site.

Telnet path: /Other/Manual-Dialing/Connect

4.1.4 Test call

This action test the connection establishment to a remote site.

For the action parameter you can enter the name of the corresponding remote site.

Telnet path: /Other/Manual-Dialing/Testcall

4.6 Voice Call Manager

This menu contains the actions for the Voice Call Manager.

Telnet path: /Other/Voice-Call-Manager

4.6.1 Lines

This menu contains the actions for the Voice Call Manager's lines.

Telnet path: /Other/Voice-Call-Manager/Lines

4.6.1.2 Register

This action allows you to select a line used by the Voice Call Manager that is to be registered.

For the action parameter you can enter the name of the corresponding line.

Telnet path: /Other/Voice-Call-Manager/Lines/Register

4.6.1.1 Unregister

This action allows you to select a line used by the Voice Call Manager that is to be unregistered.

For the action parameter you can enter the name of the corresponding line.

Telnet path: /Other/Voice-Call-Manager/Lines/Unregister

4.6.2 Groups

This menu contains the actions for the Voice Call Manager's groups.

Telnet path: /Other/Voice-Call-Manager/Groups

4.6.2.1 Show

This action allows you to display a group used by the Voice Call Manager.

For the action parameter you can enter the name of the corresponding group.

Telnet path: /Other/Voice-Call-Manager/Groups/Show