HIRSCHMANN
A Belden Company

Reference Manual
Command Line Interface
BAT Family

BAT CLI
Release 8.5x 06/11

Technical Support
HAC-Support@hirschmann.de

The performance features described here are binding only if they have been expressly guaranteed in the contract. This publication has been created by Hirschmann Automation and Control GmbH according to the best of our knowledge. Hirschmann reserves the right to change the contents of this manual without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the details in this publication.

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

Printed in Germany (09.05.2011)

Hirschmann Automation and Control GmbH
Stuttgarter Straße 45-51
72654 Neckartenzlingen
Tel. +49 1805 141538

Contents

1 Introduction

The following chapters contain the description of menus, tables and parameters in HiLCOS.

The leading numbers for the individual entries correspond to SNMP-IDs of menus, tables and parameters, which can be used to access them via Telnet or other command line tools. Hence the leading numbers don’t reflect a continous numbering. Because some parameters have been removed from HiLCOS over time, there might appear some gaps in the numbering.

2 Setup

This menu allows you to adjust the settings in the device.

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 alpha numeric characters

Default: Blank

2.2 WAN

This menu contains the configuration of the Wide Area Network (WAN).
Telnet path: Setup

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/WLAN
Note: Observe the following advice when editing the remote-sites lists:
If two remote-site lists contain identical names for remote sites (e.g. DSL broadband remote sites and Dialup peers), the device 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 access concentrator (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 digital subscriber line (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:

- Selection from the list of the 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 alpha numeric characters

Default: blank

2.2.2.3 B1-DT

The connection is terminated if it remains unused for the time in seconds set here.
Telnet path: Setup/WAN/Dialup-Peers
Possible values:

- 0 to 9999

Default: 0

2.2.2.4 B2-DT

Hold time in seconds 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 Point-to-Point Protocol High-Level Data Link Protocol (PPPHDLC) entry to establish a Point-to-Point Protocol (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 device 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 'Fast' mode and, at the called party, the return call must be set to 'Looser'.

Default: No
Note: The setting 'Name' offers the highest security if there is an entry in the numbers list and in the PPP list.
Note: 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 Remote site

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

Telnet path: Setup/WAN/Round-Robin
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, for example: 1234-4567-8910
Telnet path: Setup/WAN/Round-Robin

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/Round-Robin
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

The layer is selected in the peer list under this name.
Telnet path: Setup/WAN/Layer
Possible values:

- max. 9 alpha numeric characters

Default: blank

2.2.4.2 Encaps.

Additional encapsulations can be set for data packets. 'Transparent' No additional encapsulations. 'Ethernet' Encapsulation in the form of ethernet frames. 'LLC-MUX' Multiplexing via ATM with LLC/SNAP encapsulation according to RFC 2684. Several protocols can be transmitted over the same VC (Virtual Channel). 'VC-MUX' Multiplexing with ATM by establishing additional VCs according to RFC 2684.
Telnet path: Setup/WAN/Layer
Possible values:

- TRANS: No additional encapsulation
- ETHER: 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 Lay-3

The following options are available for the network layer:
'Transparent' No additional header is added.
'PPP' The connection is established according to the PPP protocol (in synchronous mode, i.e. bit oriented).
The configuration data is 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 optionally be executed by a dedicated script. The script is
specified in the script list.
'DHCP' Allocation of network parameters by DHCP.
Telnet path: Setup/WAN/Layer
Possible values:

- Transparent: No additional header is inserted.
- PPP: The connection is established according to the PPP protocol (in the synchronous mode, i.e. bit-oriented). The configuration data are taken from the PPP table.
- AsyncPPP: Like PPP, only the asynchronous mode is used. This means that PPP functions character-oriented.
- ... with script: All options can be run with their own script if desired. The script is specified in the script list.
- DHCP: Assignment of the network parameters via DHCP.

Default: PPP

2.2.4.4 Lay-2

This field configures the upper sublayer of the data link layer. The following options are available:
Telnet path: Setup/WAN/Layer
Possible values:

- Transparent: No additional header is inserted.
- PPPoE: The PPP negotiation runs via Ethernet. The PPP packets are encapsulated in Ethernet frames for this purpose. This process is frequently used for DSL connections.

Default: Blank

2.2.4.5 L2-Opt.

Here you can activate the compression of the data to be transmitted and the bundling of channels. The selected option only becomes active when it is supported by both the ports used and the selected Layer-2 and Layer-3 protocols. For further information see section ’ISDN Channel bundling with MLPPP’.
Telnet path: Setup/WAN/Layer
Possible values:

- None
- Compr.: Compression
- Bundle: Channel bundling
- bnd+compr.: Compression + bundling

Default: Compr.

2.2.4.6 Lay-1

This field configures the lower sublayer of the data link layer. The following options are available:
Telnet path: Setup/WAN/Layer
Possible values:

- SERIAL: Usage of the serial interface for connections as per V.24_DEF
- ETH: Transparent Ethernet as per IEEE 802.3.

Default: ETH

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 Remote site

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 device logs on with its name. The device 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.

2.2.5.2 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 Key

Password transferred by your router to the remote site (if demanded). An asterisk (*) in the list indicates that an entry is present.
Telnet path: Setup/WAN/PPP
Possible values:

- max. 32 alpha numeric characters

Default: blank

2.2.5.4 Time

Time between two checks of the connection with LCP (see the following section). This is specified in multiples of 10 seconds (i.e. 2 for 20 seconds, for instance). The value is simultaneously the time between two verifications of the connection to CHAP. Enter this time in minutes. The time must be set to '0' for remote sites using a Windows operating system.
Telnet path: Setup/WAN/PPP
Possible values:

- max. 10 characters

Default: 0

2.2.5.5 Try

Number of retries for the check attempt. You can eliminate the effect of short-term line interference by selecting multiple retries. The connection will only be dropped if all attempts are unsuccessful. The time interval between two retries is 1/10 of the time interval between two checks. Simultaneously this is the maximum number of "Configure requests", which are send by the router before it assumes a line error and clears the connection.
Telnet path: Setup/WAN/PPP
Possible values:

- max. 10 characters

Default: 5

2.2.5.6 Username

The name with which your router logs onto the remote site. The device name of your router is used if nothing is specified here.
Telnet path: Setup/WAN/PPP
Possible values:

- max. 64 alpha numeric characters

Default: No entry

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. 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 numeric 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, you can refer to this RFC in conjunction with the PPP statistics of the router for 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 numeric 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, you can refer to this RFC in conjunction with the PPP statistics of the router for 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 numeric characters

Default: 2

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 (all four values selected)
Note: The device only uses the protocols enabled here—other negotiations with the remote site are not possible.

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 Telephone number

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. 02121122334, 0221445566.
For remote sites in other countries, you must add the corresponding country code with two leading zeroes, e.g. , 0012121122334, 0049221445566 .

2.2.6.2 Remote site

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.
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 Remote site

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

2.2.9 Protect

Telnet path: Setup/WAN/Protect
Description
Possible values:

- none
- number
- screened

Default: none

2.2.10 Callback-Attempts

Telnet path: Setup/WAN/Callback-Attempts
If the device is called by a remote station that has been set up for automatic callback, then this value sets the number of callback attempts.
Possible values:

- 0 to 9

Default: 3

2.2.11 Router-Interface

Here you can enter further settings (e.g. the call number) for each WAN interface used by the router.
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 numeric characters

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

- Yes
- No

Default: Yes
Note: This function must be supported by your network operator.

2.2.11.8 YC (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
Note: The channel bundling incurs costs for two connections. No further connections can be made over LANCAPI. 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
Note: 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

2.2.13.1 Connect

Establishes a connection to the remote site which is entered as a parameter.
Telnet path: Setup/WAN/Manual-Dialing
Possible values:

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

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:

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

Default: Blank

2.2.18 Backup-Delay-Seconds

Wait time before establishing a backup connection in case a remote site stops communicating.
Telnet path: Setup/WAN
Possible values:

- max. 4 numeric characters

Default: 30 (seconds)

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:

- Selection from the list of the defined peers.

Default: blank

2.2.19.3 SH-time

The number of seconds after which the connection should be closed if no data has been transferred within the elapsed time.
The value 9999 results in an immediate connection establishment with unlimited duration.
Telnet path: Setup/WAN/DSL broadband peers
Possible values:

- 0 to 9999 seconds

Default: 300 seconds

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 alpha numeric characters

Default: blank

2.2.19.9 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 numeric characters

Default: Blank

2.2.19.10 Service name

Telnet path: Setup/WAN/DSL-Broadband-Peers/Service name
The service parameters are used to specify your Internet provider.
Contact your provider for these parameters.
Possible values:

- max. 32 characters

Default: blank

2.2.19.13 user-def.-MAC

Enter the MAC address of your choice if 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 numeric characters

Default: 0

2.2.20 IP-List

If certain remote sites do not automatically transmit the IP parameters required for a connection, these values can be entered 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 stops communicating.
Telnet path: Setup/WAN/IP-List
Possible values:

- Selection from the list of the 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 stops communicating.
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 device 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 Masq. IP addr.

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: 0.0.0.0
Note: 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

IP address of the PPTP gateway, often the address of the DSL modem.
Telnet path: Setup/WAN/PPTP-Peers
Possible values:

- Selection from the list of the defined peers.

Default: blank

2.2.21.3 Port

IP port the PPTP protocol runs on. For conformity with the protocol standard enter the port '1.723'
Telnet path: Setup/WAN/PPTP-Peers
Possible values:

- max. 10 numeric 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 Rtg-tag

Routing tag for this entry.
Telnet path: Setup/WAN/PPTP-Peers
Possible values:

- max. 10 numeric characters

Default: 0

2.2.21.6 IP address

Telnet path: Setup/WAN/Manual dialing/PPTP peers/IP address
Description

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

2.2.22.2 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

2.2.22.3 Auth. port

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

Telnet path: Setup/WAN/RADIUS
Possible values:

- Max. 10 numeric characters

Default: 1812

2.2.22.4 Key

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

Telnet path: Setup/WAN/RADIUS
Default: Blank

2.2.22.5 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
Note: If you switch the PPP mode to 'Exclusive', the internal user authentication data is ignored, otherwise these have priority.

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

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 alpha numeric characters

Default: blank

2.2.22.8 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.
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 called "DMZ", its address will be taken in this case).
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.

  Note: If you have an interface named "DMZ", then the name of that interface will be taken.
- LB0 to LBF for the 16 loopback addresses
- Any valid IP address

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

2.2.22.9 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

2.2.22.10 Auth. 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
- (multiple entries can be selected)

Default: MS-CHAPv2, MS-CHAP, CHAP, PAP (all four values selected)
Note: If all methods are selected, the next available method of authentication is used if the previous one was unsuccessful.
If none of the methods are selected, authentication is not requested from the remote site.

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

2.2.23.1 Peer

Name of the remote station which is to be checked with this entry.
Telnet path: Setup/WAN/Polling-Table
Possible values:

- Selection from the list of the 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

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

2.2.23.8 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 interface, the address of which is to be used.
- "INT" for the address of the first intranet.
- "DMZ" for the address of the first DMZ

  Note: If you have an interface named "DMZ", then the name of that interface will be taken.
- LB0 to LBF for the 16 loopback addresses.
- Any IP address can be entered in the form x.x.x.x.

Default: blank
Note: 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.

2.2.23.9 Type

This option defines how the polling for the corresponding remote site is being executed.
Telnet path: Setup/WAN/Polling-Table
Possible values:

- Auto: Polling is active only if no data is received from the remote site.
- Forced: Polling is active in any case, regardless if data is received from the remote site or not.

Default: Forced

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:

- Selection from the list of the 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.
Possible values:

- max. 10 numeric 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).
Possible values:

- max. 64 alpha numeric characters

Default: blank

2.2.25.3 Peer

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

- Selection from the list of the defined peers.

Default: blank

2.2.25.4 Lock-Time

Prevents this action from being repeated within the period defined here in seconds.
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.
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).
- Error: 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.
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. Forexample, you can use the following action to use 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. Forexample, 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 Subsidiary 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.
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 Active

Activates or deactivates this entry.
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.
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 Remote site

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

Telnet path: Setup/WAN/Additional PPTP gateways
Up to 32 additional gateways can be configured to help assure the availability of any PPTP remote station. Consequently, each PPTP remote station can use a total of up to 33 gateways.
The additional PPTP gateways are defined in a separate list.

2.2.30.1 Peer

Telnet path: Setup/WAN/Additional PPTP gateways/Peer
Here you select the PPTP remote site that this entry applies to.
Possible values: Select from the list of defined PPTP remote stations.
Default: Blank

2.2.30.2 Begin-With

Telnet path: Setup/WAN/Additional PPTP gateways/Begin with
Here you select the order in which the entries are to be tried.
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

2.2.30.3 Gateway-1

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 1
Enter the IP address that can be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.4 Rtg-Tag-1

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 1
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 2
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.6 Rtg-Tag-2

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 2
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 3
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.8 Rtg-Tag-3

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 3
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 4
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.10 Rtg-Tag-4

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 4
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 5
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.12 Rtg-Tag-5

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 5
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 6
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.14 Rtg-Tag-6

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 6
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 7
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.16 Rtg-Tag-7

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 7
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 8
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.18 Rtg-Tag-8

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 8
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 9
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.20 Rtg-Tag-9

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 9
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 10
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.22 Rtg-Tag-10

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 10
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 11
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.24 Rtg-Tag-11

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 11
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 12
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.26 Rtg-Tag-12

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 12
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 13
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.28 Rtg-Tag-13

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 13
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 14
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.30 Rtg-Tag-14

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 14
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 15
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.32 Rtg-Tag-15

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 15
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 16
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.34 Rtg-Tag-16

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 16
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 17
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.36 Rtg-Tag-17

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 17
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 18
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.38 Rtg-Tag-18

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 18
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 19
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.40 Rtg-Tag-19

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 19
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 20
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.42 Rtg-Tag-20

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 20
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 21
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.44 Rtg-Tag-21

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 21
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 22
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.46 Rtg-Tag-22

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 22
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 23
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.48 Rtg-Tag-23

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 23
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 24
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.50 Rtg-Tag-24

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 24
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 25
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.52 Rtg-Tag-25

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 25
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 26
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.54 Rtg-Tag-26

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 26
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 27
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.56 Rtg-Tag-27

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 27
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 28
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.58 Rtg-Tag-28

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 28
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 29
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.60 Rtg-Tag-29

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 29
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 30
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.62 Rtg-Tag-30

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 30
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 31
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.64 Rtg-Tag-31

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 31
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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

Telnet path: Setup/WAN/Additional PPTP gateways/Gateway 32
Enter the IP address of the additional gateway to be used for this PPTP remote station.
Possible values:IP address or 63 alphanumerical characters.
Default: Blank

2.2.30.66 Rtg-Tag-32

Telnet path: Setup/WAN/Additional PPTP gateways/Rtg tag 32
Enter the routing tag for setting the route to the relevant remote gateway.
Possible values: Maximum 5 characters.
Default: 0

Note: 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.

2.2.31 PPTP-Source-Check

This option defines how incoming PPTP connections are being checked.
Path Telnet: /Setup/WAN
Possible values:

- Address: Only the address is being checked.
- Tag+Address: In addition to the address the routing tag of the corresponding interface is being checked.

Default: Address

Note: The IP address '0.0.0.0' or an empty IP address in the PPTP table will cause the device to accept all incoming PPTP connections with any IP address, if PPTP-Source-Check is set to 'address'. If the routing tag is set in the PPTP table, the device will accept only incoming PPTP connections matching this tag, if PPTP-Source-Check is set to 'tag+address'.

2.3 Charges

This menu contains the settings for charge management.
Telnet path: Setup

2.3.2 Days-per-Period

Enter a time in days to serve as the basis for the monitoring of call charges and time limits.
Telnet path: Setup/Charges
Possible values:

- max. 10 characters

Default: 1

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

Interface referred to be 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

2.3.8 DSL-Broadband-Minutes-Budget

Enter the maximum number of online minutes that may be used within a specified period. The router will not establish any further connections once this limit has been reached.
Telnet path: Setup/Charges
Possible values:

- max. 10 characters

Default: 600

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

2.3.10 Router-DSL-Broadband-Minutes-Active

Displays the number of minutes used by DSL broadband connections in the current time period.
Telnet path: Setup/Charges

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

2.3.12 Activate-Additional-Budget

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

2.3.13 Dialup-Minutes-Budget

Enter the maximum number of online minutes that may be used within a specified period. The router will not establish any further connections once this limit has been reached.
Telnet path: Setup/Charges
Possible values:

- max. 10 characters

Default: 210

2.3.14 Spare-Dialup-Minutes

Displays the number of minutes remaining for dial-in connections in the current period.
Telnet path: Setup/Charges

2.3.15 Router-ISDN-Serial-Minutes-Active

Displays the number of minutes used by dial-in connections in the current time period.
Telnet path: Setup/Charges

2.3.16 Reset-Budgets

Enter here any additional arguments for the command you are about to execute.
Telnet path: Setup/Charges

2.4 LAN

Telnet path: Setup/LAN
This menu holds the settings for the LAN interfaces.

2.4.2 MAC address

Telnet path: Setup/LAN/MAC address
Description

2.4.3 Spare heap

Telnet path: Setup/LAN/Spare heap
Description
Possible values:

- Numeric characters from 0 to 999

Default: 10

2.4.8 Trace MAC

Telnet path: Setup/LAN/Trace MAC
Description
Possible values:

- Numeric characters from 0 to 999999999999

Default: 0

2.4.9 Trace level

Telnet path: Setup/LAN/Trace level
Description
Possible values:

- Numeric characters from 0 to 255

Default: 255

2.4.10 IEEE802.1x

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

2.4.10.1 Supplicant Ifc setup

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

2.4.10.1.1 Ifc

Telnet path: Setup/LAN/IEEE802.1x/Supplicant Ifc setup/Ifc
Description
Possible values:

- LAN-1

Default: LAN-1

2.4.10.1.2 Method

Telnet path: Setup/LAN/IEEE802.1x/Supplicant Ifc setup/Method
Description
Possible values:

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

Default: None

2.4.10.1.3 Credentials

Telnet path: Setup/LAN/IEEE802.1x/Supplicant Ifc setup/Credentials
Description
Possible values:
Max. 64 alpha numeric 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

2.7.6 Access-List

The access list contains those stations that are to be given 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

Enter an IP address range here that is to be assigned to users that dial in to the unit. The unit automatically uses a free address from this range for each user. As soon as a user separates the connection to the unit once more, the address assigned to this user is free once more and available to other users.
Telnet path: Setup/TCP-IP/Access-List
Possible values:

- Valid IP address.

Default: 0.0.0.0

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 Rtg tag

Routing tag for selecting a specified route.
Telnet path: Setup/TCP-IP/Access list
Possible values: Max. 5 characters

2.7.7 DNS-Default

Enter the address of a name Server to which DNS queries should be forwarded.
This field may be left blank if you have an Internet provider or other remote Station that automatically assigns a name Server when logging in.
Telnet path: Setup/TCP-IP
Possible values:

- Valid IP address.

Default: 0.0.0.0

2.7.8 DNS-Backup

Enter the name Server that should be used as an alternate to the first DNS.
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: 0.0.0.0

2.7.10 NBNS-Backup

Enter the NetBIOS name Server that should be used as an alternate to the first NBNS.
Telnet path: Setup/TCP-IP
Possible values:

- Valid IP address.

Default: 0.0.0.0

2.7.11 ARP-Aging-Minutes

A time in minutes may be entered in this field afterwhich the ARP table is automatically refreshed, i.e. the addresses that have not been used since the last refresh are removed.
Telnet path: Setup/TCP-IP
Possible values:

- 1 to 60 minutes

Default: 15 minutes

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:

- Selection from the list of the 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 where the station is connected to.
Telnet path: Setup/TCP-IP/ARP table/Connect
Possible values:

- Selection 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-Addr.

16 optional loopback addresses can be configured here. The device receives any of those addresses as own address and performs as if it received the packet on the LAN. This is particularly essential on masked connections. Packet answers to a loopback address will not be masked.
Telnet path: Setup/TCP-IP/Loopback-List
Possible values:

- Name of the IP interface, the address of which is to be used.
- "INT" for the address of the first intranet.
- "DMZ" for the address of the first DMZ

  Note: If you have an interface named "DMZ", then the name of that interface will be taken.
- LB0 to LBF for the 16 loopback addresses.
- Any IP address can be entered in the form x.x.x.x.

Default: 0.0.0.0

2.7.17.2 Name

NO HELP TOPIC
Telnet path: Setup/TCP-IP/Loopback-List
Possible values:

- max. 16 alpha numeric characters

Default: blank

2.7.17.3 Rtg-tag

This is the routing tag used to determine the routes to all remote gateways that have no routing tag configured (i.e. routing tag is 0).
Telnet path: Setup/TCP-IP/Loopback-List
Possible values:

- 0 to 65535

Default: 0

2.7.20 Non-Loc.-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

2.7.21 Alive-Test

This menu contains the settings for the alive test.
Telnet path: Setup/TCP-IP

2.7.21.1 Target-Address

IP address being pinged.
Telnet path: Setup/TCP-IP/Alive-Test
Possible values:

- Valid IP address.

2.7.21.2 Test-Interval

Interval at which pings 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

2.7.21.4 Retry-Interval

Interval at which the retries are sent.
Telnet path: Setup/TCP-IP/Alive-Test

2.7.21.5 Fail-Limit

Undocumented function
Telnet path: Setup/TCP-IP/Alive-Test
Possible values:

- Numeric characters from 0 to 4289999999

Default: 10

2.7.21.6 Boot-Type

Click here to open a table with boot images. Each entry states the Server on which the boot image is stored and the name of the file on the Server.
Telnet path: Setup/TCP-IP/Alive-Test

2.7.22 ICMP-On-ARP-Timeout

When the device receives a packet that it should transmit to the LAN it uses ARP requests to ascertain the recipient. If this goes unanswered, the device returns a "ICMP host unreachable" message to the sender of the packet.
Telnet path: Setup/TCP-IP

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 an unambiguous name here so that the network can be referenced by other modules (e.g. DHCP Server, RIP, NetBIOS, etc.).
Telnet path: Setup/TCP-IP/Network-list
Possible values:

- max. 16 alpha numeric characters

Default: blank

2.7.30.2 IP-Address

If you use a private address range in your local network, enter a free address from this range here. These addresses are not visible to remote networks when using IP masquerading, but are replaced by the Internet IP address valid for the specific 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 you have entered an address from a private address range under Intranet IP Address, 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 physical interface can be used to combine multiple separate VLANs (which were separated "in front" of it by a switch). To achieve this, the router must be assigned with its own address or network in each of these VLANs. The interface and the applicable VLAN can be defined for each network for this. A packet with this VLAN-ID arriving at an interface will be assigned to the appropriate network. Consequently, the network is only accessible to packets which originate from the same VLAN. Packets originate from the device itself are marked with this VLAN ID on sending. A '0' stands for an untagged net (no VLAN).
Note: It is easy to lock yourself out of the router, if you do not have access to the assigned VLAN. Observe that this setting also applies to all of the data traffic managed by this network. This includes all packets which are routed via this network.
Telnet path: Setup/TCP-IP/Network-list
Possible values:

- max 4094

Default: 0

2.7.30.5 Interface

Here you select the interface which is to be allocated to the network. If "Any" is selected, then this network is valid at all interfaces which are not otherwise.
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 Src-check

This switch affects the address check for the firewall. Loose does not expect an explicit return route. Any source address is accepted when the device is addressed itself. The router can be reached directly as in the past. Strict, in contrast, expects an explicit return route to prevent an IDS alarm.
Telnet path: Setup/TCP-IP/Network-list
Possible values:

- loose
- strict

Default: Loose

2.7.30.7 Type

Here you select the type of network (intranet or DMZ) oryou can deactivate it.
Telnet path: Setup/TCP-IP/Network-list
Possible values:

- Disabled
- Intranet
- DMZ

Default: Intranet

2.7.30.8 Rtg-tag

Enter a value for the interface tag here; this value should specify the network unambiguously. All packets received by the network will be internally marked with this tag. The interface tag allows the Separation of routes which are valid for this network even without an explicit firewall rule. Furthermore, this tag influences the routes which are propagated via RIP and also the hosts and groups which are visible to the NetBIOS proxy.
Telnet path: Setup/TCP-IP/Network-list
Possible values:

- 0 to 65535

Default: 0

2.7.30.9 Comment

This field is for free commenting purpose.
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:

- yes
- no

Default: inactive

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

Enter the target address for this route. This may be an individual Station that you would like to integrate or an entire network which you would like to link to your own network.
Telnet path: Setup/IP-Router/IP-Routing-Table
Possible values:

- Valid IP address.

Default: 0.0.0.0

2.8.2.2 IP-Netmask

Enter the netmask associated with the specified IP address. If you would like to address a Single Station only, enter the netmask 255.255.255.255.
Telnet path: Setup/IP-Router/IP-Routing-Table
Possible values:

- Valid IP address.

Default: 0.0.0.0

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

Specify the number of hops to this router. Specifying this value is usually not required as it is automatically controlled by the router.
Telnet path: Setup/IP-Router/IP-Routing-Table
Possible values:

- 0 to16

Default: 0

2.8.2.5 Masquerade

IP masquerading can be used to hide a logical IP network behind a Single address - namely, that of the router For example, if you have Internet access, you can use this functionality to connect your entire network to the Internet. For most Internet Service Providers, it is common practice to assign an IP address to your router dynamically whenever it connects. In the rare case that your Internet Service provider has allocated fixed IP addresses for you, you can assign those IP addresses to each connection in the IP parameter list. You should select masking Intranet and DMZ to activate IP masquerading for all LAN interfaces. You should select masking Intranet only if you assigned fixed IP addresses to the stations in the demilitarized zone (Short DMZ). In this case all LAN interfaces except the DMZ (this means Intranet) will be masked.
Telnet path: Setup/IP-Router/IP-Routing-Table
Possible values:

- IP masquerading switched off
- Intranet and DMZ masquerading (standard)
- Intranet masquerading only

Default: IP masquerading

2.8.2.6 Active

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:

- The route is activated and will always be propagated by RIP (sticky).
- The route can be activated and is propagated via RIP when the destination network can be reached (conditional).
- The route is off.

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

2.8.2.7 Comment

This field is for free commenting purpose.
Telnet path: Setup/IP-Router/IP-Routing-Table
Possible values:

- max. 64 characters

2.8.2.8 Rtg 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 from a network with the corresponding interface tag.
Telnet path: Setup/IP router/IP routing table
Possible values:

- Maximum 65535

Default: 0
Note: It follows that the use of routing tags only makes sense in combination with corresponding, decorative rules in the firewall or tagged networks.

2.8.5 Proxy-ARP

This is where you can activate or deactivate proxy ARP mechanisms. Proxy ARP allows you to integrate remote clients into your local network as if they were attached directly to your LAN.
Telnet path: Setup/IP-Router
Possible values:

- yes
- no

Default: inactive

2.8.6 Send-ICMP-Redirect

This is where you can choose if ICMP redirects should be sent.
Telnet path: Setup/IP-Router
Possible values:

- yes
- no

Default: active

2.8.7 Routing method

This menu contains the configuration of the routing methods used by your IP router.
Telnet path: Setup/IP router

2.8.7.1 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

2.8.7.2 ICMP routing method

Specify if the router should transmit secure ICMP packets.
Telnet path: Setup/IP router
Possible Values:

- Normal
- Secured

Default: Normal

2.8.7.3 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:

- Yes
- No

Default: Yes

2.8.7.4 L2-L3 tagging

Specify what should happen with DiffServ layer 2 tags.
Telnet path: Setup/IP router
Possible Values:

- Ignore
- Copy to layer 3
- 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/Routing-Method
Possible values:

- No
- Yes

Default: No

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
Possible values:

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

Default: No

Note: The internal services VPN and PPTP need special handling, as the routing all of the packets without exception would lead to a clear loss of performance. With this option activated, only the initial packets sent by these services during connection establishment are directed via the router. Subsequent packets are sent to the "next hop" as determined during the connection establishment.

2.8.8 RIP

This menu contains the configuration of RIP for your IP router.
Telnet path: Setup/IP-Router

2.8.8.2 R1-Mask

This setting is only required if you have selected RIP-1 as RIP support. This influences the how network masks are formed for routes learned using RIP. Please refer to your handbook for further information.
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

Select the remote site for which to support RIP on WAN.
Telnet path: Setup/IP-Router/RIP/WAN-Sites
Possible values:

- Selection from the list of the 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_*".

2.8.8.4.2 RIP-Type

Select the RIP Version to be used for propagating local routes.
Telnet path: Setup/IP-Router/RIP/WAN-Sites
Possible values:

- Off
- RIP-1
- RIP-1 compatible
- RIP-3

Default: off

2.8.8.4.3 RIP-Accept

You can accept or deny RIP from WAN. If you accept RIP from WAN, you must specify the RIP type.
Note: Allowing RIP on WAN poses a potential security risk.
Telnet path: Setup/IP-Router/RIP/WAN-Sites
Possible values:

- On
- Off

Default: off

2.8.8.4.4 Masquerade

Select if and how to mask on the route. The following values are possible.
Auto: The masquerading type is acquired from the routing table. If no routing entry exists for this remote site, it will not be masked.
On: All connections will be masked.
Intranet: Connections from Intranet will be masked, connections from DMZ are routed transparently.
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 Dft-Rtg-Tag

This is the default routing tag used for this WAN connection. All unmarked routes (routing tag is 0) will be marked with this tag if forwarded to the WAN. All routes learned from WAN are internally handled as untagged routes and will be forwarded to the LAN without being tagged (routing tag to 0). However, on the WAN, the routes are forwarded with the tag with which they were learned.
Telnet path: Setup/IP-Router/RIP/WAN-Sites
Possible values:

- max. 65535

Default: 0

2.8.8.4.6 Rtg 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 alpha numeric characters

Default: Blank

2.8.8.4.7 Poisoned reverse

Poisoned reverse prevents routing loops from forming. 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
Note: 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

The router basically supports RIP according to RFC 2091. The setting "Proposing RFC 2091" is only relevant for active connection establishment. For passive connections the RIP Version which is proposed by the remote site is always used - independent of the State of this switch. For active connections and activated proposing of RIP according to RFC 2091 there is a fallback to 'normal' RIP according to RFC 2453: the fallback is initiated if the remote site does not answer after 10 retries of the first packet (10 retries last approximately 30 seconds). The IP address of the RIP partner on the remote side of the WAN connection has to be entered as gateway. It is possible to enter 0.0.0.0 here if a PPP negotiation is established on the WAN connection and thereby the IP address of the remote site is transferred.

Note: In a central-side gateway the RFC 2091 proposing can always be set to off and the gateway can always be 0.0.0.0, as the central-side gateway always adapts to the subsidiary-side gateway.

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

- Valid IP address.

Default: 0.0.0.0
Special values: If 0.0.0.0 is entered, the gateway address is determined from PPP negotiation.
Note: 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.
Note: The device automatically reverts to standard RIP if the indicated gateway does not support RFC 2091.
Note: 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.

2.8.8.4.10 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

Telnet path: Setup/IP router/RIP/ WAN sites/RIP send
Description
Possible values:
No
Yes
Default: No

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 the name of the network which these settings apply to.
Telnet path: Setup/IP-Router/RIP/LAN-Sites
Possible values:

- Intranet
- DMZ

Default: blank

2.8.8.5.2 RIP-Type

Select whether the router should support IP-RIP. Routing information can be exchanged automatically between individual stations using IP-RIP.
Telnet path: Setup/IP-Router/RIP/LAN-Sites
Possible values:

- Off
- RIP-1
- RIP-1 compatible
- RIP-3

Default: off

2.8.8.5.3 RIP-Accept

Here you decide whether or not routes will be learned by this network.
Telnet path: Setup/IP-Router/RIP/LAN-Sites
Possible values:

- yes
- no

Default: no

2.8.8.5.4 Propagate

Here you decide if the associated network is to be propagated to other networks.
Telnet path: Setup/IP-Router/RIP/LAN-Sites
Possible values:

- yes
- no

Default: no

2.8.8.5.5 Dft-Rtg-Tag

Enter a value for the Standard routing tag which applies to the selected interface. Routes which are marked with this interface tag will be propagated on this interface with the Standard routing tag. Routes learned at the interface which are marked with the Standard routing tag configured here will be included into the RIP table with the interface tag. Furthermore, unmarked routes (i.e. routes with the tag 0) are not propagated over 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 Rtg-Tag-List

This is a comma-separated list of routing tags which are accepted at this interface. If this list is empty all routes will be accepted, irrespective of their routing tags. If at least one tag is in this list, then only those routes with tags in this list are accepted. Similarly, only routes with tags entered here will be forwarded. The routing tag list corresponds with the WAN RIP list, with the exception that any necessary mapping regarding the default routing tag is incorporated. This means that if, for example, the interface tag is 1 and the default routing tag is 0, then tag 0 must be present in the routing tag list, because it will be changed to tag 1 internally upon reception. When being sent, the internal tag 1 is changed to the external tag 0. This is necessary to enable a Virtual router to work with other routers in the LAN which do not support tagged routes.
Telnet path: Setup/IP-Router/RIP/LAN-Sites
Possible values:

- max. 33 alpha numeric characters

Default: blank

2.8.8.5.7 Poisoned reverse

Poisoned reverse prevents routing loops from forming. 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:

- No
- Yes

Default: No

2.8.8.5.10 Rx filter

Telnet path: Setup/IP router/RIP/LAN sites/RX filter
Description
Possible values:

- Max. 16 alpha numeric characters

Default: Blank

2.8.8.5.11 TX filter

Telnet path: Setup/IP router/RIP/LAN sites/TX filter
Description
Possible values:

- Max. 16 alpha numeric characters

Default: Blank

2.8.8.5.12 RIP send

Telnet path: Setup/IP router/RIP/ WAN sites/RIP send
Description
Possible values:

- No
- Yes

Default: No

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

2.8.8.6.1 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

2.8.8.6.2 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 device will only accept a route from the same router that propagated the original route until the holddown interval expires. Within this period, the 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 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

2.8.8.6.4 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

2.8.8.6.5 Upd. 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 wrong 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

2.8.8.6.6 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

2.8.8.7 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:

- max. 18 alpha numeric characters

Note: 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.

Note: The plus-sign for accepted networks is optional.
Note: 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

Telnet path: /Setup/IP-Router/RIP/Best-Routes
In large network infrastructures more than one route can be learned to another network. The Best-Routes table holds only the best RIP learned route to a certain remote network regarding metric and timeouts. The table is filled automatically via RIP and holds the following values of the learned networks:

- IP-Address
- VLAN-ID
- Name
- Port (logical port that has received the route, e.g. LAN-1, LAN-2, not the physical port ETH-1 or ETH-2)
- IP-Netmask
- Time to reach the remote network
- Distance to the remote network in hops
- Gateway
- Rtg-Tag
- Peer

2.8.8.8.1 IP-Address

Telnet path: Setup/IP-Router/RIP/Parameter/Best-Routes/IP-Address
This entry contains the explanation for the parameter IP-Address

2.8.8.8.2 IP-Netmask

Telnet path: Setup/IP-Router/RIP/Parameter/Best-Routes/IP-Netmask
This entry contains the explanation for the parameter IP-Netmask

2.8.8.8.3 Time

Telnet path: Setup/IP-Router/RIP/Parameter/Best-Routes/Time
This entry contains the explanation for the parameter Time

2.8.8.8.4 Distance

Telnet path: Setup/IP-Router/RIP/Parameter/Best-Routes/Distance
This entry contains the explanation for the parameter Distance

2.8.8.8.5 Gateway

Telnet path: Setup/IP-Router/RIP/Parameter/Best-Routes/Gateway
This entry contains the explanation for the parameter Gateway

2.8.8.8.6 Rtg-tag

Telnet path: Setup/IP-Router/RIP/Parameter/Best-Routes/Rtg-tag
This entry contains the explanation for the parameter Rtg-tag

2.8.8.8.8 Peer

Telnet path: Setup/IP-Router/RIP/Parameter/Best-Routes/Peer
This entry contains the explanation for the parameter Peer

2.8.8.8.10 VLAN-ID

Telnet path: Setup/IP-Router/RIP/Parameter/Best-Routes/VLAN-ID
This entry contains the explanation for the parameter VLAN-ID

2.8.8.8.11 Network-name

Telnet path: Setup/IP-Router/RIP/Parameter/Best-Routes/Network-name
This entry contains the explanation for the parameter Network-name

2.8.8.8.12 Port

Telnet path: Setup/IP-Router/RIP/Parameter/Best-Routes/Port
This entry contains the explanation for the parameter Port
Possible values:

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

Default: LAN-1

2.8.8.9 All-Routes

Telnet path: /Setup/IP-Router/RIP/All-Routes
In large network infrastructures more than one route can be learned to another network. The All-Routes table holds all RIP learned routes regardless of the metric and timeouts. The table is filled automatically via RIP and holds the following values of the learned networks:

- IP-Address
- VLAN-ID
- Name
- Port (logical port that has received the route, e.g. LAN-1, LAN-2, not the physical port ETH-1 or ETH-2)
- IP-Netmask
- Time to reach the remote network
- Distance to the remote network in hops
- Gateway
- Rtg-Tag
- Peer

2.8.8.9.1 IP address

Telnet path: Setup/IP router/RIP/All routes/IP address
Description

2.8.8.9.2 IP netmask

Telnet path: Setup/IP router/RIP/All routes/IP netmask
Description

2.8.8.9.3 Time

Telnet path: Setup/IP router/RIP/All routes/Time
Description

2.8.8.9.4 Distance

Telnet path: Setup/IP router/RIP/All routes/Distance
Description

2.8.8.9.5 Gateway

Telnet path: Setup/IP router/RIP/All routes/Gateway
Description

2.8.8.9.6 Rtg tag

Telnet path: Setup/IP router/RIP/All routes/Rtg. tag
Description

2.8.8.9.8 Peer

Telnet path: Setup/IP router/RIP/All routes/Peer
Description

2.8.8.9.10 VLAN-ID

Telnet path: Setup/IP router/RIP/All routes/VLAN-ID
Description

2.8.8.9.11 Network name

Telnet path: Setup/IP router/RIP/All routes/Network name
Description

2.8.8.9.12 Port

Telnet path: Setup/IP router/RIP/All routes/Port
No description is available for this parameter yet.

2.8.9 1-N-NAT

This menu contains the configuration of 1-N-NAT for your IP router.
Telnet path: Setup/IP-Router

2.8.9.1 TCP-Aging-Seconds

In this field, enter the period of inactivity of a TCP connection (in seconds) after which the appropriate entry in the masquerading table should be removed.
Telnet path: Setup/IP-Router/1-N-NAT
Possible values:

- 0 to 65535

Default: 300 (seconds)

2.8.9.2 UDP-Aging-Seconds

In this field, enter the period of inactivity of a UDP connection afterwhich the appropriate entry in the masquerading table should be removed.
Telnet path: Setup/IP-Router/1-N-NAT
Possible values:

- 0 to 65535

Default: 20 (seconds)

2.8.9.3 ICMP-Aging-Seconds

In this field, enter the period of inactivity of a ICMP connection (in seconds) after which the appropriate entry in the masquerading table should be removed.
Telnet path: Setup/IP-Router/1-N-NAT
Possible values:

- 0 to 65535

Default: 10 (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 into this table.
Telnet path: Setup/IP-Router/1-N-NAT

2.8.9.4.1 D-port-from

Specify the port of the required Service here.
Telnet path: Setup/IP-Router/1-N-NAT/Service-Table
Possible values:

- max. 65535

Default: 0

2.8.9.4.2 Intranet-Address

In this field, 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: 0.0.0.0

2.8.9.4.3 D-port-to

Specify the port of the required Service here.
Telnet path: Setup/IP-Router/1-N-NAT/Service-Table
Possible values:

- max. 65535

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:

- max. 65535

Default: 0

2.8.9.4.5 Active

You can temporarily deactivate this entry without having to delete it.
Telnet path: Setup/IP-Router/1-N-NAT/Service-Table
Possible values:

- Yes
- No

Default: Yes

2.8.9.4.6 Comment

This field is for free commenting purpose.
Telnet path: Setup/IP-Router/1-N-NAT/Service-Table
Possible values:

- max. 64 characters

Default: /

2.8.9.4.7 Peer

Select the remote site to which this entry applies. If the name is left empty the entry applies to all remote Sites.
Telnet path: Setup/IP-Router/1-N-NAT/Service-Table
Possible values:

- Selection from the list of the 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 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: 0.0.0.0

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.

2.8.9.6 Fragments

This setting controls the firewall's behavior regarding fragmented IP packets.
Telnet path: Setup/IP-Router/1-N-NAT
Possible values:

- Filters: Fragments are always rejected (filtered).
- Routes: 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

2.8.9.7 Fragment-Aging-Seconds

If an IP packet cannot be fully demasked 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

2.8.9.8 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 65535

Default: 2000

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.

2.8.9.9.2 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

2.8.9.9.10 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 starts when a DPD packet is received from one end. If no DPD packet is received from the other end within 30 seconds, then this entry is removed.
Telnet path: Setup/IP-Router/1-N-NAT/IPSec-Table

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

2.8.10 Firewall

This menu contains the configuration of the firewall.
Telnet path: Setup/IP-Router

2.8.10.1 Objects table

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 alpha numeric characters

Default: blank

2.8.10.1.2 Description

The 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 – 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
Note: 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 device can resolve the names into IP addresses. To this end, the 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 table

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 interrelationships 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

Note: 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 alpha numeric characters

Default: blank

2.8.10.2.2 Prot.

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 it is 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 it is 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 it is 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 it is 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 Prio

Priority of the rule.
Telnet path: Setup/IP-Router/Firewall/Rules
Possible values:

- 0 to 255

Default: blank

2.8.10.2.10 Firewall-Rule

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 alpha numeric characters

Default: blank

2.8.10.2.14 Rtg-tag

Routing tag for the rule.
Telnet path: Setup/IP-Router/Firewall/Rules
Possible values:

- 0 to 65535

Default: 0

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 Idx.

Index for this entry in the list.
Telnet path: Setup/IP-Router/Firewall/Filter-List

2.8.10.3.2 Prot.

TCP protocol for data packets processed by this entry.
Telnet path: Setup/IP-Router/Firewall/Filter-List

2.8.10.3.3 Src-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 Src-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.

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

Finish address of range of source IP addresses whose data packets are processed by this entry.
Telnet path: Setup/IP-Router/Firewall/Filter-List

2.8.10.3.7 Dst-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 Dst-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

2.8.10.3.10 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 Src-MAC

Source MAC address for data packets processed by this entry.
Telnet path: Setup/IP-Router/Firewall/Filter-List

2.8.10.3.14 Dst-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 Prio

Priority for this entry.
Telnet path: Setup/IP-Router/Firewall/Filter-List

2.8.10.3.17 Rtg-tag

This routing tag is added to data packets processed by this entry.
Telnet path: Setup/IP-Router/Firewall/Filter-List

2.8.10.4 Actions table

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 alphanumeric 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 Src-Address

This rule applies to packets on connections from all stations and connections from the following stations.
Telnet path: Setup/IP-Router/Firewall/Connection-List
Possible values:

- Valid IP address.

2.8.10.5.2 Dst-Address

This rule applies to packets on connections from all stations and connections from the following stations.
Telnet path: Setup/IP-Router/Firewall/Connection-List
Possible values:

- Valid IP address.

2.8.10.5.3 Prot.

Protocol allowed on this connection.
Telnet path: Setup/IP-Router/Firewall/Connection-List

2.8.10.5.4 Src-Port

Source port of the station that established a connection.
Telnet path: Setup/IP-Router/Firewall/Connection-List

2.8.10.5.5 Dst-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

Undocumented function
Telnet path: Setup/IP-Router/Firewall/Connection-List

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-Route

Source route used to establish this connection.
Telnet path: Setup/IP-Router/Firewall/Connection-List

2.8.10.5.10 Dest-Route

Destination route to which a connection was established.
Telnet path: Setup/IP-Router/Firewall/Connection-List

2.8.10.5.11 Rtg-tag

Connection routing tag.
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 Src-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 Dst-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 Prot.

Protocol that is blocked by this entry.
Telnet path: Setup/IP-Router/Firewall/Port-Block-List

2.8.10.7.3 Dst-Port

Select one of the three additional countermeasures:
• With the source host lock, you can temporarily block all packets that are received from a specific address.
• With the target port lock, you can temporarily block all packets that are transmitted to a specific port.
Note: The duration of the source host or target port lock should be specified. Otherwise the respective addresses or ports will be permanently locked. These locks can only be released on the device by using a Telnet console or WEBconfig.
• The most effective countermeasure is to disconnect the device. If your provider reassigns another IP each time the device establishes a connection, it will be no longer accessible to a potential aggressor from the Internet after reconnection.
Note: All of these countermeasures can be abused to run a denial of service attack against your router.
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

2.8.10.8 Max.-Half-Open-Conns.

Half-open connections are connections that are still in negotiation. If the amount of this connections to a specific host exceeds the value given here, a Denial of Service attack will be detected and the DoS actions defined will be executed.
Telnet path: Setup/IP-Router/Firewall
Possible values:

- 100 to 9999

Default: 100

2.8.10.9 DoS-Action

Here, you can specify what should happen to packets that are responsible for triggering an action or exceeding a limit. The packets can be transmitted, dropped without notification to the addressor or rejected with ICMP reject (with notification to the addressor).
Telnet path: Setup/IP-Router/Firewall
Possible values:

- transmit
- drop
- reject

Default: Drop

2.8.10.10 Admin.-Email

If you want to be notified of pre-defined occurrences (DoS, IDS or when limits are exceeded), you must specify a valid e-mail address here.

Note: To receive e-mail notification, you must also configure all necessary settings in the main section under 'Log & Trace', subsection 'SMTP.

Note: To send e-mail notifications, the device will establish connections if necessary. This can generate additional costs.
Telnet path: Setup/IP-Router/Firewall
Possible values:

- max. 255 characters

Default: Blank
Note: For e-mail messaging, you have to enter the necessary settings into the main group "Log & Trace" 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. 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:

- yes
- no

Default: yes
Note: Defined VPN rules continue to be observed even with the firewall switched off.

2.8.10.12 Port-Scan-Threshold

Intrusion-Detection-System (IDS). Your device is capable of recognizing most intrusions and will react with the countermeasures specified here.
Telnet path: Setup/IP-Router/Firewall
Possible values:

- 50 to 9999

Default: 50

2.8.10.13 IDS-Action

Here, you can specify what should happen to packets that are responsible for triggering an action or exceeding a limit. The packets can be transmitted, dropped without notification to the addressor or rejected with ICMP reject (with notification to the addressor).
Telnet path: Setup/IP-Router/Firewall
Possible values:

- transmit
- drop
- reject

Default: Drop

2.8.10.14 Ping-Block

A controversial method of increasing security is concealing the router by not answering ping and trace route inquiries (Ping blocking). It is controversial due to the fact that neglecting to answer also betrays the existence of a device: If there is truly no device present, the previous router will answer the inquiry with 'undeliverable' because the router actually cannot deliver it. But, if the previous router did not answer with a corresponding denial, the inquiry could be delivered and, regardless of the recipient's subsequent behavior, it is still most certainly present. It must also be mentioned that the behavior of the previous router cannot be simulated without staying offline or switching off your device (and thereby remaining unreachable for your own requested Services).
Telnet path: Setup/IP-Router/Firewall
Possible values:

- Off
- Always
- For WAN Route only
- For default route only

Default: off

2.8.10.15 Stealth-Mode

A controversial method of increasing security is to conceal the router by not conforming to Standards by rejecting TCP and UDP inquiries, but ignoring them (Stealth mode). It is controversial due to the fact that neglecting to answer also betrays the existence of a device: If there is truly no device present, the previous router will answer the inquiry with 'undeliverable' because the router actually cannot deliver it. But, if the previous router did not answer with a corresponding denial, the inquiry could be delivered and, regardless of the recipient's subsequent behavior, it is still most certainly present. It must also be mentioned that the behavior of the previous router cannot be simulated without staying offline or switching off your device (and thereby remaining unreachable foryour own requested Services).
Telnet path: Setup/IP-Router/Firewall
Possible values:

- Off
- Always
- For WAN Route only
- For default route only

Default: off

2.8.10.16 Auth-Port

Hiding TCP or UDP ports can slow down performance on masked connections. If for example the so called "Authenticate" or "Ident" inquiries from special mail or news Servers are returned to receive further user data and your device does not reject them, the corresponding connections will deliver a timeout. This can slow down mail or news delivery significantly. To overcome this delay with stealth mode switched on, stealth mode is

temporarily switched off for the corresponding port. The firewall recognizes that the internal stations intend to establish connections to mail (SMTP, POP3, IMAP2) or news (NNTP) Servers and opens the ports for 20 seconds. You can suppress the Short term cancellation of the stealth mode for the authentication port.
Note: This Option can slow mail or news delivery significantly.
Telnet path: Setup/IP-Router/Firewall
Possible values:

- Yes
- No

Default: No

2.8.10.17 Deny-Session-Recover

The firewall opens appropriate Channels for each Session initiated along with its corresponding connections (e.g. FTP with its control plus data connection). If a Channel no longer in use for a certain period (as defined by the ageing Parameters under IP router/ masquerading), then it is assumed that the Session is completed and the according Channels will be closed. The session recovery parameter determines firewall behavior when receiving packets relating to a past session. Either packets belonging to a former closed session are discarded or a similar, equivalent session is re-established. The latter can either be allowed or disallowed in general, or disallowed only for the default route or WAN connections.
Telnet path: Setup/IP-Router/Firewall
Possible values:

- Always allowed
- Always denied
- Denied for WAN
- Denied for default route

Default: Denied for default route

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 Src-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 Dst-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 Prot.

Protocol opened by this entry.
Telnet path: Setup/IP-Router/Firewall/Open-Port-List

2.8.10.19.5 Dst-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 Src-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

2.8.10.20.1 FTP

This menu contains the configuration of FTP for your firewall.
Telnet path: Setup/IP-Router/Firewall/Applications

2.8.10.20.1.1 FTP-Block

If an FTP Session is recognized on any port, the countermeasures specified beneath will apply. 'React on any FTP Session' specifies if and on which routes any type of FTP should be dealt with in particular. Default setting is 'Off'.
Telnet path: Setup/IP-Router/Firewall/Applications/FTP
Possible values:

- No
- Always
- For WAN Route only
- For default route only

Default: No

2.8.10.20.1.2 Active-FTP-Block

If an FTP Session is recognized on any port, the countermeasures specified beneath will apply. 'React on active FTP' specifies if and on which routes active FTP should be dealt with in particular. Default setting is 'Off'.
Telnet path: Setup/IP-Router/Firewall/Applications/FTP
Possible values:

- No
- Always
- For WAN Route only
- For default route only

Default: No

2.8.10.20.1.3 Min-Port

If an FTP Session is recognized on any port, the countermeasures specified beneath will apply. 'Least allowed port number1 is used as a lower boundary for active FTP. Default setting is port '1024'.
Telnet path: Setup/IP-Router/Firewall/Applications/FTP
Possible values:

- 1024 to 9999

Default: 1024

2.8.10.20.1.4 Check-Host-IP

If an FTP Session is recognized on any port, the countermeasures specified beneath will apply. Check host IP address' specifies if and on which routes the address transferred in the FTP command Channel should be checked against the source address of the FTP client. If it does not match, the countermeasures specified beneath will apply. This check will be skipped certainly if a Site-To-Site transfer should take place and is allowed already. Default setting is 'Only for default route'.
Telnet path: Setup/IP-Router/Firewall/Applications/FTP
Possible values:

- No
- Always
- For WAN Route only
- For default route only

Default: For default route only

2.8.10.20.1.5 FXP-Block

If an FTP Session is recognized on any port, the countermeasures specified beneath will apply. 'React on FXP sessions' specifies if and on which routes Site-To-Site transfers (FXP) should be dealt with in particular special. Default settinq is 'Only for default route'.
Telnet path: Setup/IP-Router/Firewall/Applications/FTP
Possible values:

- No
- Always
- For WAN Route only
- For default route only

Default: For default route only

2.8.10.20.2 IRC

This menu contains the configuration of IRC for your firewall.
Telnet path: Setup/IP-Router/Firewall/Applications

2.8.10.20.2.1 IRC-Block

If an IRC session is recognized on any port, the countermeasures specified beneath will apply. 'React on IRC sessions' specifies if and on which routes any type of IRC should be dealtwith in particular. Default setting is 'Off'.
Telnet path: Setup/IP-Router/Firewall/Applications/IRC
Possible values:

- No
- Always
- For WAN Route only
- For default route only

Default: No

2.8.10.20.2.2 DDC-Block

If an IRC session is recognized on any port, the countermeasures specified beneath will apply. 'React on Direct-Data-Connect' specifies if and on which routes Direct-Data-Connect (DDC - private Chats and file transfers) should be dealt with in particular. Default setting is 'Off.
Telnet path: Setup/IP-Router/Firewall/Applications/IRC
Possible values:

- No
- Always
- For WAN Route only
- For default route only

Default: No

2.8.10.20.2.3 Min-Port

If an IRC session is recognized on any port, the countermeasures specified beneath will apply. 'Least allowed port number" is used as a lower boundary for active DDC. Default setting is port '1024'.
Telnet path: Setup/IP-Router/Firewall/Applications/IRC
Possible values:

- 1024 to 9999

Default: 1024

2.8.10.20.2.4 Check-Host-IP

If an IRC session is recognized on any port, the countermeasures specified beneath will apply. 'Check host IP address' specifies if and on which routes the address transferred in the DDC command should be checked against the source address of the IRC client. If it does not match, the countermeasures specified beneath will apply. This check will be skipped certainly if a Site-To-Site transfer should take place and is allowed already. Default setting is 'Only for default route'.
Telnet path: Setup/IP-Router/Firewall/Applications/IRC
Possible values:

- No
- Always
- For WAN Route only
- For default route only

Default: For the default route only

2.8.10.20.10 Appl.-Action

If an IRC session is recognized on any port, the countermeasures specified beneath will apply. Here, you can specify what should happen to packets that are responsible for triggering an action or exceeding a limit. The packets can be transmitted, dropped without notification to the addressor or rejected with ICMP reject (with notification to the addressor).
Telnet path: Setup/IP-Router/Firewall/Applications
Possible values:

- transmit
- drop
- reject

Default: Reject

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: 0.0.0.0

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: 0.0.0.0

2.8.13 Default time list

Time-dependent control allows you to specify different targets 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

Select the days during which this entry should apply.
Telnet path: Setup/IP-Router/Default-Time-List
Possible values:

- Mondays
- Tuesdays
- Wednesdays
- Thursdays
- Fridays
- Saturdays
- Sundays
- Public holidays

Default: No days have been marked

2.8.13.3 Start

Select the period during which this entry should apply.
Telnet path: Setup/IP-Router/Default-Time-List
Possible values:

- 00:00 to 23:59

Default: 0

2.8.13.4 Stop

Select the period during which this entry should apply.
Telnet path: Setup/IP-Router/Default-Time-List
Possible values:

- 00:00 to 23:59

Default: blank

2.8.13.5 Peer

When this entry becomes valid because the specified period has been reached, the remote station entered here will be used as the destination of the default mute. Select the name of a remote station from the list of remote sites here.
Telnet path: Setup/IP-Router/Default-Time-List
Possible values:

- Selection from the list of the defined peers.

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:

- yes
- no

Default: inactive
Note: 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.

2.8.19 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 Idx.

Unique index for the entry
Telnet path: Setup/IP-Router/N-N-NAT
Possible values:

- max. 4 alpha numeric characters

Default: blank

2.8.19.2 Src-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: 0.0.0.0

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: 0.0.0.0

2.8.19.4 Dst-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:

- Selection from the list of the defined peers.

Default: blank

2.8.19.5 Mapped network

IP addresses or address range to be used for translation.
Telnet path: Setup/IP router/N-N-NAT
Possible values:

- Valid IP address

Default: 0.0.0.0
Note: 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. This means that 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.
Note: The address range for translation must be at least as large as the source address range.
Note: 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

The Virtual Router Redundancy Protocol is used to configure several physical routers like one "Virtual" router. Only one of the physical routers will take the role of the "master". The master is the only one that has an Internet connection and transfers data. The other routers will only become active if the master breaks down, i.e., if it freezes up or if the Internet connection is disrupted. The VRRP protocol is then used to negotiate which router will take over the role as master next. The new master will completely assume the previous master's tasks.
Telnet path: Setup/IP-Router/VRRP
Possible values:

- yes
- no

Default: no

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 ofthe Virtual router. Values between 0 and 255 are accepted.
Telnet path: Setup/IP-Router/VRRP/VRRP-List
Possible values:

- ▶ 0 to 255

Default: 1

2.8.21.2.2 virt.-Address

IP address of the Virtual router. All routers that a Single Virtual router is directed to must assign the same IP address.
Telnet path: Setup/IP-Router/VRRP/VRRP-List
Possible values:

- ▶ Valid IP address.

Default: 0.0.0.0

2.8.21.2.3 Prio

Main priority of the Virtual router. Values between 0 and 255 are accepted. The values 0 and 255 have a certain meaning. The value 0 disables the Virtual router. The value 255 will only be accepted if the address of the Virtual router is identical to the address of the interface where the router is mapped to. Otherwise, this router will be listed at the event log of all other routers.
Telnet path: Setup/IP-Router/VRRP/VRRP-List
Possible values:

- ▶ 0 to 255

Default: 0

2.8.21.2.4 B-Prio

Backup priority of the Virtual router. Values between 0 and 255 are accepted. The values 0 and 255 have a certain meaning. The value 0 disables the Virtual router in a backup scenario. Whether or not the main connection can be established again is checked in periodic intervals. The interval can be adjusted with the reconnect delay parameter. The value 255 will only be accepted if the address of the Virtual router is identical to the address of the

interface where the router is mapped to. Otherwise this router will be listed at the event log of all other routers. If the backup connection cannot be established, then the Virtual router will quit completely and try in periodic intervals (reconnect delay) to re-establish either the main or backup connection.
Telnet path: Setup/IP-Router/VRRP/VRRP-List
Possible values:

- 0 to 255

Default: 0

2.8.21.2.5 Peer

The remote site name is an optional entry. If a remote site is entered here, it controls the VRRP. If none is entered, VRRP can be used to support a hardware breakdown. This remote site can be also assigned to other Virtual routers.
Telnet path: Setup/IP-Router/VRRP/VRRP-List
Possible values:

- Selection from the list of the defined peers.

Default: blank

2.8.21.2.6 Comment

Comment describing the Virtual router.
Telnet path: Setup/IP-Router/VRRP/VRRP-List
Possible values:

- max. 64 characters

Default: blank

2.8.21.3 Reconnect-Delay

If the backup connection of the Virtual router could not be established, the Virtual router will no longer be propagated. The reconnect delay parameter holds the time interval in minutes afterwhich the Virtual router will try again to establish the main or backup connection again. During the connection procedure, the router will not be propagated.
Telnet path: Setup/IP-Router/VRRP
Possible values:

- 0 to 999 minutes

Default: 30 min.

2.8.21.4 Advert.-Intervall

The advertisement interval parameter holds the time value in seconds after a Virtual router is to be propagated.
Telnet path: Setup/IP-Router/VRRP
Possible values:

- 0 to 999 seconds

Default: 1 second

2.8.21.5 Internal-Services

The internal Services switch controls the behavior of the router when it is called by the address of a Virtual router. In default position "On", the router will react to the Services DNS and NETBIOS just as if it were addressed by its physical address. This will only function if the router itself is master of the Virtual router. The position "Off" ensures RFC-compliant behavior. That means that the respective packets will be discarded silently.
Telnet path: Setup/IP-Router/VRRP
Possible values:

- on
- off

Default: on

2.8.22 WAN-Tag-Creation

WAN tag generation defines the source for the assignment of interfaces 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 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
Note: 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.

2.8.23 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 to whose packets interfaces tags are to be added on receipt.
Telnet path: Setup/IP-Router/Tag-Table
Possible values:

- Selection from the list of the 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: 0.0.0.0

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: 0.0.0.0
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

2.9.1 Send-Traps

The device can automatically send an error message to one or more SNMP managers in the event of detected errors such as unauthorized access. Enable this option and enter the addresses of those computers into the SNMP manager table.
Telnet path: Setup/SNMP
Possible values:

- Yes
- No

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 on which a SNMP manager is installed here.
Telnet path: Setup/SNMP/IP-Traps
Possible values:

- Valid IP address.

Default: blank

2.9.2.3 Loopback-Addr.

An optional source address can be configured here. This address is used instead of the source address, which is otherwise obtained automatically for the respective destination.
Telnet path: Setup/SNMP/IP-Traps
Possible values:

- Name of the IP interface, the address of which is to be used.
- "INT" for the address of the first intranet.
- "DMZ" for the address of the first DMZ

  Note: If you have an interface named "DMZ", then the name of that interface will be taken.
- LB0 to LBF for the 16 loopback addresses.
- Any IP address can be entered in the form x.x.x.x.

Default: blank
Note: If the list of IP networks or loopback addresses contains an entry named 'DMZ', the associated IP address is 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

2.9.3 Administrator

Name of the device administrator. For display purposes only.
Telnet path: Setup/SNMP
Possible values:

- max. 255 alpha numeric characters

Default: blank

2.9.4 Location

Location information for this device. For display purposes only.
Telnet path: Setup/SNMP
Possible values:

- max. 255 alpha numeric 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.
Note: 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.

2.9.6 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 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|*>

Default: blank

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 Device-name

Name of the remote station from where an SNMP agent accesses the device.
Telnet path: Setup/SNMP/Monitor-Table
Possible values:

- Selection from the list of the defined peers.

2.9.7.6 Loopback-Addr.

An optional source address can be configured here. This address is used instead of the source address, which is otherwise obtained automatically for the respective destination.
Telnet path: Setup/SNMP/Monitor-Table
Possible values:

- Name of the IP interface, the address of which is to be used.
- "INT" for the address of the first intranet.
- "DMZ" for the address of the first DMZ

  Note: If you have an interface named "DMZ", then the name of that interface will be taken.
- LB0 to LBF for the 16 loopback addresses.
- Any IP address can be entered in the form x.x.x.x.

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

2.9.10 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

2.9.11 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

2.9.15 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 alpha numeric characters

Default: Blank

2.9.16 Comment 5

Comment on this device. For display purposes only.
Telnet path: Setup/SNMP
Possible values:

- Max. 255 alpha numeric characters

Default: Blank

2.9.17 Comment 6

Comment on this device. For display purposes only.
Telnet path: Setup/SNMP
Possible values:

- Max. 255 alpha numeric characters

Default: Blank

2.9.18 Comment 7

Comment on this device. For display purposes only.
Telnet path: Setup/SNMP
Possible values:

- Max. 255 alpha numeric characters

Default: Blank

2.9.19 Comment 8

Comment on this device. For display purposes only.
Telnet path: Setup/SNMP
Possible values:

- Max. 255 alpha numeric characters

Default: Blank

2.9.20 Full host MIB

Telnet path: Setup/SNMP/Full host MIB
Description
Possible values:

- No
- Yes

Default: No

2.10 DHCP

This menu contains the DHCP settings.
Telnet path: Setup

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 values governs the maximum length of lease that the client may request.
Telnet path: Setup/DHCP
Possible values:

- max. 10 numeric characters

Default: 6000

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 numeric characters

Default: 500

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.

2.10.8.2 MAC-Address

The client's MAC address.
Telnet path: Setup/DHCP/DHCP-Table

2.10.8.3 Timeout

Period of validity (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

2.10.8.10 LAN Ifc

The LAN interface that this entry refers to.
Telnet path: Setup/DHCP/DHCP table/LAN Ifc

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 into 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 alpha numeric 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 alpha numeric characters

Default: blank
Note: 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, it will be assigned the relevant IP address defined for the MAC address.
Telnet path: Setup/DHCP/Hosts
Possible values:

- max. 16 alpha numeric 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.
Note: 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 alpha numeric 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 alpha numeric 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

2.10.19 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. 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 alpha numeric characters

Default: blank

2.10.20 Network list

DHCP settings for the IP networks are defined in this table.
Telnet path: Setup/DHCP/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.

2.10.20.1 Network-name

The name of the network which the DHCP server settings apply to.
Telnet path: Setup/DHCP/Network-list
Possible values:

- max. 16 alpha numeric characters

Default: blank

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 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 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).
Note: We recommend that only experienced network specialists change the pre-setting for the broadcast address. Inproper configuration here can lead to costly connections being established.

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 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
The IP address of the device in this network is taken as the gateway.

2.10.20.7 DNS-Default

IP address of the DNS name server for the forwarding of DNS requests.
Telnet path: Setup/DHCP/Network-list
Possible values:

- Valid IP address.

Default: 0.0.0.0

2.10.20.8 DNS backup

IP address of the backup DNS name server for the forwarding of DNS requests, in the event that the first name server stops communicating.
Telnet path: Setup/DHCP/Network list
Possible values:

- Valid IP address

Default: 0.0.0.0
The IP address from the global TCP/IP settings is communicated as the backup DNS server.

2.10.20.9 NBNS-Default

IP address of the NetBIOS name server for the forwarding of NetBIOS requests.
Telnet path: Setup/DHCP/Network-list
Possible values:

- Valid IP address.

Default: 0.0.0.0

2.10.20.10 NBNS backup

IP address of the backup NBNS name server for the forwarding of NBNS requests, in the event that the first name server stops communicating.
Telnet path: Setup/DHCP/Network list
Possible values:

- Valid IP address

Default: 0.0.0.0
The IP address from the global TCP/IP settings is communicated as the backup NBNS server.

2.10.20.11 Operating

DHCP server operating mode in this network. Depending on the operating mode, the DHCP server can enable or disable itself. You can see whether the DHCP server is enabled from the DHCP statistics.
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. Inproper 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 device 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 device 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
Note: 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 superordinate DHCP server is entered when the mode 'Relay requests' is selected.
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 device. Subsequent requests can then be answered by the device 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 Adaptation

This option allows the responses from the superordinate DHCP server to be adapted to the local network. When activated, the device adapts the responses from the superordinate DHCP server by replacing the following entries with its own address (or local 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

Note: 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, 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 when the mode 'Relay requests' is selected.
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 when the mode 'Relay requests' is selected.
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 when the mode 'Relay requests' is selected.
Telnet path: Setup/DHCP/Network list/2nd master server
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 obtains its operating system via BOOTP.
Telnet path: Setup/DHCP/Additional options
Possible values:

- Max. 3 characters

Default: Blank

Note: 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 specified with the usual notation for IPv4 addresses, e.g.as "123.123.123.100", integer types are entered as normal decimal numbers, and strings 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

Note: You can find out the possible length of the option value either from the corresponding RFC or from the manufacturer's documentation of their DHCP options.

2.10.21.4 Option type

Telnet path: Setup/DHCP/Additional options
Entry type. 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

Note: 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

2.11.3 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

2.11.4 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.

2.11.5 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

2.11.6 Language

The language for the LANconfig, LANmonitor or WLANmonitor graphical user interface can be set to 'German' or 'English'.

Telnet path: Setup/Config

Possible values:

- german
- english

Default: English

Note: Ensure that the language you use to enter commands matches with that set for the console, otherwise scheduler commands will not be observed.

2.11.7 Login-Errors

As a measure of protection against attacks, the maximum allowed number of unsuccessful attempts to login can be set. If this limit is reached, access will be barred for a certain length of time. If barring is activated on one port all other ports are automatically barred too.

Telnet path: Setup/Config

Possible values:

- max. 10 characters

Default: 10

2.11.8 Lock-Minutes

If the limit (in minutes) of unsuccessful attempts to log in is reached, access will be barred for the time you set up here.
Telnet path: Setup/Config
Possible values:

- max. 10 characters

Default: 45
Special values: 0 switches the lock off.

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

2.11.13 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

2.11.13.1 Config-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 Config-Filename

Default path for the configuration file when the parameter -f is not specified for LoadConfig commands.
Telnet path: Setup/Config/TFTP-Client
Possible values:

- max. 63 alpha numeric 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 alpha numeric 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 alpha numeric 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 Ifc.

Port of the device, which is effected by this entry.
Telnet path: Setup/Config/Access-Table

2.11.15.2 Telnet

Here, you can specify the access rights to the device configuration with the TELN ET protocol. This protocol is necessary to configure your device with the implemented operating system independent and text-based Telnet console.
Telnet path: Setup/Config/Access-Table
Possible values:

- VPN
- Yes
- Read
- No

Default: Yes

2.11.15.3 TFTP

Here, you can specify the access rights to the device configuration with the Trivial File Transfer Protocol (TFTP). This protocol is necessary for use with our software LANconfig.
Telnet path: Setup/Config/Access-Table
Possible values:

- VPN
- Yes
- Read
- No

Default: Yes

2.11.15.4 HTTP

Here you can specify the access rights to the device configuration with the Hypertext Transfer Protocol (HTTP). This protocol is necessary to configure your device with the implemented operating system independent web browser interface.
Telnet path: Setup/Config/Access-Table
Possible values:

- VPN
- Yes
- Read
- No

Default: Yes

2.11.15.5 SNMP

Here, you can specify the access rights to the device configuration with the Simple Network Management Protocol (SNMP). This protocol is necessary for use with our software LANconfig.
Telnet path: Setup/Config/Access-Table
Possible values:

- VPN
- Yes
- Read
- No

Default: Yes

2.11.15.6 HTTPS

Here, you can specify the access rights to the device configuration with the Hypertext Transfer Protocol Secure (HTTPS or SSL over HTTP). This protocol is necessary to securely configure your device with the implemented operating system independent web browser interface.
Telnet path: Setup/Config/Access-Table
Possible values:

- VPN
- Yes
- Read
- No

Default: Yes

2.11.15.7 Telnet-SSL

Here, you can specify the access rights to the device configuration with the TELN ET/SSL protocol. This protocol is necessary to securely configure your device with the implemented operating system independent and text-based Telnet console.
Telnet path: Setup/Config/Access-Table
Possible values:

- VPN
- Yes
- Read
- No

Default: LAN: yes, WAN: no

2.11.15.8 SSH

Here, you can specify the access rights to the device configuration with the SSH protocol (Secure Shell). This protocol is necessary to securely configure your device with the implemented operating system independent and text-based Telnet console.
Telnet path: Setup/Config/Access-Table
Possible values:

- VPN
- Yes
- Read
- No

Default: Yes

2.11.16 Screen-Height

Specifies the maximum height of the screen in pixels.
Telnet path: Setup/Config
Possible values:

- max.10 characters

Default: 24

2.11.17 Prompt

Telnet path: Setup/Config/Prompt

Use the prompt parameter to configure the individual output of the command line interface prompt. Static text and the following variables may be used:
%f: Displays "Test", if the flash parameter is set to "off" (Config test Mode).
%u: User name
%n: Device name
%p: Current path
%t: Current time
%o: Current operating time

Possible values:

- Max. 31 numeric characters.

Default: Blank

2.11.18 LED-Test

Activates the test mode for the LEDs which tests LED function in different colors.

Telnet path: Setup/Config

Possible values:

- off: Deactivates all LEDs
- red: All red LED's illuminate
- green: All green LED's illuminate
- orange: All orange LED's illuminate
- no_test: Normal operating state of the LEDs
- Off, Green, Red, Orange, No_Test

Default: No_test

2.11.20 Cron-Table

CRON jobs are used to carry out recurring tasks on a device automatically at certain times. If the installation has 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 terminate 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

2.11.20.2 Minute

The value defines the time when a command is to be executed. With no value entered, it is not included in the controlling. For each parameter, 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 time when a command is to be executed. With no value entered, it is not included in the controlling. For each parameter, 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 time when a command is to be executed. With no value entered, it is not included in the controlling. For each parameter, 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 day when a command is to be executed. With no value entered, it is not included in the controlling. For each parameter, 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 time when a command is to be executed. With no value entered, it is not included in the controlling. For each parameter, 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 command-line function can be executed.
Telnet path: Setup/Config/Cron-Table
Possible values:

- max. 100 characters

Default: blank

2.11.20.8 Base

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.
- 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

2.11.20.10 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.
Note: Real-time based rules can only be executed if the device has a time from a relevant source, e.g. via NTP.

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 differing access rights. For one device up to 16 different administrators can be set up.
Telnet path: Setup/Config/Admins
Possible values:

- max. 16 alpha numeric characters

Default: blank
Note: 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

Keyword for this entry.
Telnet path: Setup/Config/Admins
Possible values:

- max. 16 alpha numeric characters

Default: blank

2.11.21.3 Function-Rights

Each administrator also has "function rights" that determine the 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
- 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

Default: blank

2.11.21.4 Active

Activates /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 (RAS) 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 LANCAPI clients. Furthermore, the following internal functions can be switch 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

2.11.23 Telnet-Port

This port is used for unencrypted configuration connections via telnet.
Telnet path: Setup/Config
Possible values:

- max.10 numeric 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 numeric characters

Default: 992

2.11.25 SSH-Port

This port is used for configuration connections via SSH.
Telnet path: Setup/Config
Possible values:

- max.10 numeric characters

Default: 22

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 Ifc.

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 or by using a public key.
Telnet path: Setup/Config/SSH-Authentication-Methods
Possible values:

- All: Allows authentication using password and digital certificate.
- Password: Allows authentication with a password.
- Public key: Only allows authentication with a digital certificate.

Default: All

2.11.27 Predef. admins

Telnet path: Setup/Config/Predef. admins
This table contains the pre-defined admin accounts.

2.11.27.1 Name

Telnet path: Setup/Config/Predef. admins/Name
This is the pre-defined admin account for the device, which cannot be edited. The password for this account and the corresponding privileges can be set up under Setup/Config/Admins.

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.
Some devices simply cannot be installed under lock and key. There is consequently a potential 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): Press the button briefly to re-start the device. Pressing the button for 5 seconds or longer restarts the device and resets the configuration to its factory settings. All LEDs on the device light up continuously. Once the switch is released the device will restart with the restored factory settings.

Default: Reset-or-boot

Note: After resetting, the device returns to managed mode, in which case the configuration cannot be directly accessed via the WLAN interface.

Note: After resetting, the device starts completely unconfigured and all settings are lost. If possible be sure to backup the current device configuration before resetting.

Note: The settings 'Ignore' or 'Boot only' makes it impossible to reset the configuration to the factory settings. 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.

2.11.33 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

2.11.35 Monitortrace

This menu contains the settings for monitor tracing.
Telnet path: Setup/Config

2.11.35.1 Tracemask1

This parameter is only available for support.
Telnet path: /Setup/Config/Monitortrace/Tracemask1

2.11.35.2 Tracemask2

This entry is only available for support.
Telnet path: /Setup/Config/Monitortrace/Tracemask2

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 e-mail
Possible values:

- Valid e-mail address

Default: Blank

2.11.40 Crash message

Telnet path: Setup/Config/Crash message

This text string is used as header for messages in the LCOS bootlog after detecting an error.

Possible values:

- 32 alpha numeric characters

Default: LCOS-Watchdog

2.11.41 Admin gender

Telnet path: Setup/Config/Admin gender

Declare the admin's gender here.

Possible values:

- unknown
- male
- female
- Geek

Default: unknown

2.11.42 Assert action

Telnet path: Setup/Config/Assert action

Description

Possible values:

- log_only
- reboot

Default: log_only

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:
Possible values:

- Selection of the buttons 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)
^^ A double caret symbol stands for the caret symbol itself.
Note: 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. A Windows operating system makes, for example, an Â from input caret symbol + A. To call the caret symbol itself, enter a space before the following character. Sequence ^A is then formed from caret symbol + space + A.

2.11.44 Config-Date

This menu entry stores the point of time (in UTC format), when the configuration of the device has been changed or imported to the device for the last time.
This menu entry is not visible in the configuration and accessible via sysinfo or SNMP only.
Path Telnet: /Setup/Config

Note: If the configuration being imported contains a value for this time, the value from the configuration is used instead of the time of the import procedure.

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:
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:
Possible values:

- 0 to 4294967295

Default: 0
Special values: 0 disables the time limit. The LL2M server stays permanently enabled in this state.

2.11.60 CPU-load interval

A number of device types feature a display which shows the load on the CPU. This value can also be viewed in the status menu under 'Status/Hardware info/CPU load percent' Furthermore, LANmonitor displays this status information as a graph in the system information.
Mean values for CPU load is available as averaged over the following time intervals.
Telnet path: Setup/Config
Possible values:

- **T1s** (arithmetic mean)
- **T5s** (arithmetic mean)
- **T60s** (moving average)
- **T300s** (moving average)

Default: T60s.

2.12 WLAN

This menu contains the settings for wireless LAN networks.
Telnet path: Setup

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

2.12.7 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 selected stations only.
Telnet path: Setup/WLAN

2.12.7.1 MAC-Address

Enter the MAC address of a station.
Possible values:

- Valid MAC address.

Default: blank

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 alpha numeric characters

Default: Blank

2.12.7.3 Comment

Comment on this entry
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.
Possible values:

- ASCII character string with a length of 8 to 63 characters

Default: blank
Note: This field has no significance for networks secured by WEP.
Note: 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 65535 kbps

Default: 0
Special values: 0: No limit
Note: 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 65535 kbps

Default: 0
Special values: 0: No limit
Note: 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 entered MAC address.
Possible values:

- 0 to 4096

Default: 0
Special values: 0: No VLAN ID entered

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 selected stations only.
Telnet path: Setup/WLAN
Possible values:

- Data from listed stations is filtered out; data from all other stations is transmitted.
- Transfer data from the listed stations, authenticate all others via RADIUS or filter them out

Default: Data from listed stations is filtered out; data from all other stations is transmitted.

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 roaming process, so that the former access point can delete the client from its station table.
Telnet path: Setup/WLAN
Possible values:

- Yes
- No

Default: Yes

2.12.13 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 roaming process (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

2.12.26 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

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:

- Yes
- No

Default: No

2.12.29 RADIUS-Access-Check

This menu contains the settings for the RADIUS access checking.
Telnet path: Setup/WLAN

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
Note: 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.
Note: WLAN clients must be entered as follows on the RADIUS server: The user name is the MAC address in the format AABBCC-DDEEFF. The password for all users is identical to the key (shared secret) for the RADIUS server.

2.12.29.2 Auth.-Port

Port for communication with the RADIUS server during authentication
Telnet path: Setup/WLAN/RADIUS-Access-Check
Possible values:

- Valid port number

Default: 1812

2.12.29.3 Key

Password used to access the RADIUS server.
Telnet path: Setup/WLAN/RADIUS access check
Possible values:

- Max. 64 numeric 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

2.12.29.5 Backup-Auth.-Port

Port for communication with the backup RADIUS server during authentication.
Telnet path: Setup/WLAN/RADIUS-Access-Check
Possible values:

- Valid port number

Default: 1812

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 alpha numeric characters

Default: blank

2.12.29.7 Response-Lifetime

Undocumented function
Telnet path: Setup/WLAN/RADIUS-Access-Check
Possible values:

- Numeric characters from 0 to 4289999999

Default: 15

2.12.29.8 Password-Source

Undocumented function
Telnet path: Setup/WLAN/RADIUS-Access-Check
Possible values:

- Secret
- MAC-Address

Default: Secret

2.12.29.9 Recheck-Cycle

Undocumented function
Telnet path: Setup/WLAN/RADIUS-Access-Check
Possible values:

- Numeric characters from 0 to 4289999999

Default: 0

2.12.29.10 Provide-Server-Database

Undocumented function
Telnet path: Setup/WLAN/RADIUS-Access-Check
Possible values:

- Yes
- No

Default: Yes

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.

  Note: If you have an interface named "DMZ", then the name of that interface will be taken.
- LB0 to LBF for the 16 loopback addresses
- Any valid IP address

Default: Blank
Note: If there is an interface named "DMZ", then its address is used.

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

Note: If there is an interface named "DMZ", then its address is used.

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

2.12.29.14 Backup protocol

Telnet path: Setup/WLAN/RADIUS access check/Backup protocol
Description
Possible values:

- RADIUS
- RADSEC

Default: RADIUS

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.

2.12.38 ARP handling

A station in the LAN attempting to establish a connection to a WLAN station which is in power-save mode will restart only 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

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
Note: An SMTP account must be set up to make use of the e-mail function.

2.12.44 Allow-Illegal-Association-Without-Authentication

This parameter enables the association to WLAN network without authentication.
Telnet path: Setup/WLAN/Allow-Illegal-Association-Without-Authentication
Possible values:

- No
- Yes

Default: No

2.12.45 RADIUS accounting

The accounting function in the device 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

2.12.45.1 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
Note: The general values for retry and timeout must also be configured in the RADIUS section.
Note: WLAN clients must be entered as follows on the RADIUS server: The user name is the MAC address in the format AABBCC-DDEEFF. The password for all users is identical to the key (shared secret) for the RADIUS server.

2.12.45.2 Accnt.-Port

Port for communication with the RADIUS server during accounting
Telnet path: Setup/WLAN/RADIUS-Accounting
Possible values:

- Valid port number

Default: 1812

2.12.45.3 Secret

Password used to access the RADIUS server
Telnet path: Setup/WLAN/RADIUS-Accounting
Possible values:

- max. 64 alpha numeric 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

2.12.45.5 Backup-Accnt.-Port

Port for communication with the backup RADIUS server during accounting.
Telnet path: Setup/WLAN/RADIUS-Accounting
Possible values:

- Valid port number

Default: 1812

2.12.45.6 Backup-Secret

Password used to access the backup RADIUS server.
Telnet path: Setup/WLAN/RADIUS-Accounting
Possible values:

- max. 64 alpha numeric characters

Default: blank

2.12.45.7 Client-Brg.-Handling

Undocumented function
Telnet path: Setup/WLAN/RADIUS-Accounting
Possible values:

- All-Traffic
- Bridge-Traffic-Only
- Client-Traffic-Only
- Separate-Accounting

Default: All-Traffic

2.12.45.8 Interim-Update-Period

Undocumented function
Telnet path: Setup/WLAN/RADIUS-Accounting
Possible values:

- Numeric characters from 0 to 4289999999

Default: 0

2.12.45.9 Excluded-VLAN

Undocumented function
Telnet path: Setup/WLAN/RADIUS-Accounting
Possible values:

- Numeric characters from 0 to 9999

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.

  Note: If you have an interface named "DMZ", then the name of that interface will be taken.
- LB0 to LBF for the 16 loopback addresses
- Any valid IP address

Default: Blank
Note: If there is an interface named "DMZ", then its address is used.

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:

Note: If there is an interface named "DMZ", then its address is used.

2.12.45.12 Protocol

Telnet path: Setup/WLAN/RADIUS accounting/Protocol
Description
Possible values:

- RADIUS
- RADSEC

Default: RADIUS

2.12.45.13 Backup protocol

Telnet path: Setup/WLAN/RADIUS accounting/Backup protocol
Description
Possible values:

- RADIUS
- RADSEC

Default: RADIUS

2.12.45.14 Restart accounting

Telnet path: Setup/WLAN/RADIUS accounting/Restart accounting
Description

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 potential 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:

- Yes
- No

Default: No
Note: Indoor operation may only be activated if the base station and all other stations are operated within an enclosed space.
Note: Indoor operation may only be activated if the base station and all other stations are operated within an enclosed space.

2.12.47 Idle timeout

Telnet path: Setup/WLAN/Idle timeout
No description is available for this parameter yet.

2.12.48 Use full channel set

Telnet path: Setup/WLAN/Use full channel set
No description is available for this parameter yet.

2.12.50 Signal-Averaging

This menu contains the settings for signal averaging.
Telnet path: Setup/WLAN

2.12.50.1 Method

Undocumented function
Telnet path: Setup/WLAN/Signal-Averaging

2.12.50.2 Standard-Parameters

This menu contains the configuration of the standard parameters for signal averaging.
Telnet path: Setup/WLAN/Signal-Averaging

2.12.50.2.1 Factor

Undocumented function
Telnet path: Setup/WLAN/Signal-Averaging/Standard-Parameters

2.12.50.3 Filtered-Parameters

This menu contains the configuration of the filtered parameters for signal averaging.
Telnet path: Setup/WLAN/Signal-Averaging

2.12.50.3.1 Ct

Undocumented function
Telnet path: Setup/WLAN/Signal-Averaging/Filtered-Parameters

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

2.12.50.3.2.1 Index

Undocumented function
Telnet path: Setup/WLAN/Signal-Averaging/Filtered-Parameters/
Coefficients

2.12.50.3.2.2 Value

Undocumented function
Telnet path: Setup/WLAN/Signal-Averaging/Filtered-Parameters/
Coefficients

2.12.60 IAPP-IP network

Telnet path: Setup/WLAN/IAPP-IP network
Description
Possible values:

- Max. 16 alpha numeric characters

Default: Blank

2.12.100 Card-Reinit-Cycle

In this interval (in seconds) the internal WLAN cards in older access points are reinitialized in order keep point-to-point connections 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.

2.12.101 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.

2.12.103 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.

2.12.105 Therm.-Recal.-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.
Note: Deactivating the thermal recalibration cycle for these cards means that they cannot react to changes in temperature.

2.12.107 Radar-Pattern-Thresholds

This table is used to define threshold values to be used for activating radar detection.
Telnet path: Setup/WLAN

2.12.107.1 Pattern-pps

Undocumented function
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

Undocumented function
Telnet path: Setup/WLAN/Radar-Pattern-Thresholds
Possible values:

- Numeric characters from 0 to 4289999999

Default:

- for EN301893-1.2-700pps: 8
- for EN301893-1.2-1800pps: 6
- for EN301893-1.2-330pps: 15
- for EN301893-1.3-750pps: 7
- for EN301893-1.3-200pps: 7
- for EN301893-1.3-300pps: 7
- for EN301893-1.3-500pps: 7
- for EN301893-1.3-800pps: 7
- for EN301893-1.3-1000pps: 7
- for EN301893-1.3-1200pps: 4
- for EN301893-1.3-1500pps: 7
- for EN301893-1.3-1600pps: 5
- for EN301893-1.3-2000pps: 7
- for EN301893-1.3-2300pps: 7
- for EN301893-1.3-3000pps: 7
- for EN301893-1.3-3500pps: 7
- for EN301893-1.3-4000pps: 7
- for EN302502-3000pps: 4
- for EN302502-4500pps: 4

2.12.108 Radar-Load-Threshold

Undocumented function
Telnet path: Setup/WLAN
Possible values:

- Numeric values from 0 to 100

Default: 40

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

Undocumented function
Telnet path: Setup/WLAN/Noise-Offsets
Possible values:

- 2.4GHz
- 5GHz

Default: 2.4 GHz

2.12.109.2 Channel

Undocumented function
Telnet path: Setup/WLAN/Noise-Offsets
Possible values:

- Numeric characters from 0 to 65535

Default: Blank

2.12.109.3 Interface

Undocumented function
Telnet path: Setup/WLAN/Noise-Offsets
Possible values:

- WLAN-1
- WLAN-2

Default: WLAN-1

2.12.109.4 Value

Undocumented function
Telnet path: Setup/WLAN/Noise-Offsets
Possible values:

- Numeric characters from 0 to 127

Default: 0

2.12.110 Trace-Level

The output of trace messages for the WLAN data trace can be limited to 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: only the message weather a packet is sent/recieved
- 1: additional the physical parameters of the packets/data rate, signal strength etc.
- 2: additional the MAC-Header
- 3: additional the Layer3-Header (e.g. IP/IPX)
- 4: additional the Layer4-Header (TCP, UDP...)
- 5: additional the TCP/UDP-Payload

Default: 255

2.12.111 Noise immunity

Telnet path: Setup/WLAN/Noise immunity
Description

2.12.111.1 Noise immunity level

Telnet path: Setup/WLAN/Noise immunity/Noise immunity level
Description
Possible values:

- numeric characters from 0 to 255

Default: 255

2.12.111.2 OFDM weak signal detection

Telnet path: Setup/WLAN/Noise immunity/OFDM weak signal detection
Description
Possible values:

- numeric characters from 0 to 255

Default: 255

2.12.111.3 CCK weak signal detection threshold

Telnet path: Setup/WLAN/Noise immunity/OFDM weak signal detection threshold
Description
Possible values:

- numeric characters from 0 to 255

Default: 255

2.12.111.4 Fir step level

Telnet path: Setup/WLAN/Noise immunity/Fir step level
Description
Possible values:

- numeric characters from 0 to 255

Default: 255

2.12.111.5 Spurious immunity level

Telnet path: Setup/WLAN/Noise immunity/Spurious immunity level
Description
Possible values:

- numeric characters from 0 to 255

Default: 255

2.12.114 Aggregate repeat limit

Telnet path: Setup/WLAN/Aggregate repeat limit
Description

2.12.115 Omit global crypto sequence check

Telnet path: /Setup/WLAN/Omit global crypto sequence check
Description
Possible values:

- Auto
- No
- Yes

Default: Auto

2.12.116 Trace packets

Telnet path: Setup/WLAN/Trace packets
Description
Possible values:

- Management
- Control
- Data
- EAPOL
- All
- multiple value choice between the first four

Default: All

2.12.117 WPA-Handshake-Delay-ms

This value defines a waiting period in ms before starting the WPA handshake. This time starts after the client's association and after a preceeding 1x authentication to prevent the access point from sending WPA messages, if the client is not yet ready.
Path Telnet: /Setup/WLAN
Possible values:

- maximum 10 numerical characters

Default: 0

2.14 Time

This menu contains the configuration of the device time settings.
Telnet path: Setup

2.14.1 Fetch-Method

Select whether and how the device should synchronize its internal real-time clock.
Telnet path: Setup/Time
Possible values:

- none
- ISDN
- NTP

Default: NTP

2.14.2 Current-Time

Display of current time.
Telnet path: Setup/Time

2.14.7 UTC in seconds

Telnet path: Setup/Time/UTC in seconds
Description

2.14.10 Timezone

Here, you can specify the time zone for your device's location. The time zone specifies the difference between the local time and the Coordinated Universal Time (UTC) in hours. This is important if you use 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

2.14.11 Daylight-saving-time

The switch between daylight-saving time and normal time can be controlled either manually or automatically. For automatic clock changes, the appropriate time region for the location of your device has to be set. Should your device be located outside of the listed time regions, it will be necessary to prompt an automatic daylight-saving changeover by choosing 'User defined' and entering the values for the automatic daylight-saving changeover in the table that follows.

Telnet path: Setup/Time

Possible values:

- Yes
- No
- Europe (EU)
- Russia
- USA
- User defined

Default: Europe (EU)

Note: Furthermore it should be observed that time entries can be ambiguous in the last hour of daylight-saving and the first hour that follows in standard time. If the time is acquired via ISDN or set manually during this time, then it is always assumed that the time entry is in daylight-saving time.

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 start and the end of the 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 the recurring weekday of the month when the change will take place.
Telnet path: Setup/Time/DST-clock-changes

2.14.12.4 Month

Defines the month at which the change will take place.
Telnet path: Setup/Time/DST-clock-changes

2.14.12.5 Hour

Defines the hour at which the change will take place.
Telnet path: Setup/Time/DST-clock-changes

2.14.12.6 Minute

Defines the minute at which the change will take place.
Telnet path: Setup/Time/DST-clock-changes

2.14.12.7 Time-type

Defines the timezone which is the basis for the time settings in this table. (UTC for Coordinated Universal Time or LST for Local Standard Time).
Telnet path: Setup/Time/DST-clock-changes

2.14.13 Get-Time

Running this command causes the device to get the current time from the configured time server.
Telnet path: Setup/Time

2.14.15 Holidays

This table contains the holidays that have been defined.
Telnet path: Setup/Time/Holidays

2.14.15.1 Index

Index of the entry to define the position within 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 stop time (time of day) when the selected profile ceases to be valid.
Telnet path: Setup/Time/Timeframe
Possible values:

- Max. 5 characters
- Format HH:MM

Default: 23:59

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, 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

2.15.1 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 for telephone calls, which are selected depending upon the time, day and code dialed.
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 numeric characters

Default: 0

2.15.4.2 Prefix

Enter the prefix 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. You can, however, enter only 03 - then all calls to any place that begins with the prefix 03 will be redirected.
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
- Holiday

Default: blank

2.15.4.4 Start

The start of the period on which this entry should apply.
Telnet path: Setup/LCR/Time-List
Possible values:

- max. 5 alpha numeric characters

Default: blank

2.15.4.5 Stop

The end of the period on 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 alpha numeric 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

2.16.1 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

2.16.2 UPD

Undocumented function
Telnet path: Setup/NetBIOS

2.16.4 Peers

In this list you enter the remote sites to which NetBIOS is to be transmitted over IP. These remote sites also have to be entered into 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 alpha numeric characters

Default: blank

2.16.4.3 Type

Specifies 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:

- Selection from the list of the 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 Rtg-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:

- Selection from the list of the 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 Rtg-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

2.16.7.2 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-Ver.

Displays the SMB version of the NetBIOS host.
Telnet path: Setup/NetBIOS/Server-List

2.16.7.7 Server-Typ

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:

- Selection from the list of the defined peers.

2.16.7.9 Timeout

Displays the time in minutes until the NetBIOS information is updated.
Telnet path: Setup/NetBIOS/Server-List

2.16.7.10 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 Rtg-tag

Routing tag for the connection to the NetBIOS host.
Telnet path: Setup/NetBIOS/Server-List

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

2.16.9 Update

The unit must exchange routing information with other NetBIOS routers from time to time To avoid unnecessary setup of connections, select when this should occur.

Telnet path: Setup/NetBIOS

Possible values:

- pBack
- Trig
- Time

Default: pBack

2.16.10 WAN-Update-Minutes

Once you have established 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

2.16.11 Leasetime

Telnet path: Setup/NetBIOS/Leasetime

The leasetime, after which registered NetBIOS names are deleted.

A host enrolls to the device with it's NetBIOS name. After this leasetime, the host needs to enroll to the device again with it's NetBIOS name.

Possible values:

- max. 4 numeric characters

Default: 500

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 the name of the network which these settings apply to.
Telnet path: Setup/NetBIOS/Networks
Possible values:

- max. 16 alpha numeric 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

2.16.13 Browser list

Telnet path: Setup/NetBIOS/Browser list
Description

2.16.13.1 Browser

Telnet path: Setup/NetBIOS/Browser list/Browser
Description

2.16.13.2 Domains

Telnet path: Setup/NetBIOS/Browser list/Group/Domains
Description

2.16.13.4 IP address

Telnet path: Setup/NetBIOS/Browser list/IP address
Description

2.16.13.5 OS ver.

Telnet path: Setup/NetBIOS/Browser list/OS ver.
Description

2.16.13.7 Server type

Telnet path: Setup/NetBIOS/Browser list/Server type
Description

2.16.13.8 Peer

Telnet path: Setup/NetBIOS/Browser list/Peer
Description

2.16.13.9 Timeout

Telnet path: Setup/NetBIOS/Browser list/Timeout
Description

2.16.13.10 Flags

Telnet path: Setup/NetBIOS/Browser list/Flags
Description

2.16.13.11 Network name

Telnet path: Setup/NetBIOS/Browser list/Network name
Description

2.16.13.12 Rtg tag

Telnet path: Setup/NetBIOS/Browser list/Rtg-Tag
Description

2.16.14 Support browsing

Telnet path: Setup/NetBIOS/Support browsing
Possible values:

- Yes
- No

Default: Yes

2.17 DNS

This menu contains the domain-name system (DNS) configuration.
Telnet path: Setup

2.17.1 Operating

Telnet path: Setup/DNS/Operating
Activates or deactivates 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

2.17.3 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

2.17.4 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 Host name

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 alpha numeric 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: 0.0.0.0

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 Idx.

Index for the filter entries.
Telnet path: Setup/DNS/Filter-List
Possible values:

- max. 4 alpha numeric characters

Default: blank

2.17.6.2 Domain

Enter the name of a station or domain which should be blocked from access. The characters '*' and '?' can be used as wildcards.
Telnet path: Setup/DNS/Filter-List
Possible values:

- max. 64 alpha numeric 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: 0.0.0.0

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: 0.0.0.0
Note: If you have entered the address of a single station only, then enter 255.255.255.255 as the subnet mask.

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 what time in minutes 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

2.17.8 Dyn.-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 Host-name

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 alpha numeric characters

Default: blank

2.17.9.2 Destination

Specify the remote station for DNS forwarding.
It is possible to enter two IP addresses specifying primary and secondary DNS server for the forwarded domain. On repeated DNS requests, the DNS forwarder selects the secondary server as destination.
Telnet path: Setup/DNS/DNS-Destinations
Possible values:

- max. 31 alpha numeric characters

Default: blank
Note: A mix of IP addresses and remote station is not possible, which means it has to be specified either a remote station or two IP addresses. If two IP addresses are specified, they have to be separated by at least one blank character.

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 alpha numeric characters

Default: Blank

2.17.10.2 Host-name

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 alpha numeric 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 Host-name

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

2.17.12 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

2.17.13 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 alpha numeric 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

Default: Yes

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

Default: No

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

Default: Time

2.18.4 Current-User

Displays an accounting list for all current users.
Telnet path: Setup/Accounting

2.18.4.1 Username

Shows the name of the user.
Telnet path: Setup/Accounting/Current-User

2.18.4.3 Peer

Shows the name of the remote station.
Telnet path: Setup/Accounting/Current-User

2.18.4.4 Conn.-Type

Shows the type of connection (e.g. DSL-connection).
Telnet path: Setup/Accounting/Current-User

2.18.4.5 Rx-KBytes

Shows the received bytes.
Telnet path: Setup/Accounting/Current-User

2.18.4.6 Tx-KBytes

Shows the forwarding bytes.
Telnet path: Setup/Accounting/Current-User

2.18.4.8 Total-Time

Shows the time of connection.
Telnet path: Setup/Accounting/Current-User

2.18.4.9 Connections

Shows 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

Shows the name of the user.
Telnet path: Setup/Accounting/Accounting-List

2.18.5.3 Peer

Shows the name of the remote station.
Telnet path: Setup/Accounting/Accounting-List

2.18.5.4 Conn.-Type

Shows the type of connection (e.g. DSL-connection).
Telnet path: Setup/Accounting/Accounting-List

2.18.5.5 Rx-KBytes

Shows the received bytes.
Telnet path: Setup/Accounting/Accounting-List

2.18.5.6 Tx-KBytes

Shows the forwarding bytes.
Telnet path: Setup/Accounting/Accounting-List

2.18.5.8 Total-Time

Shows the time of connection.
Telnet path: Setup/Accounting/Accounting-List

2.18.5.9 Connections

Shows the number of connection.
Telnet path: Setup/Accounting/Accounting-List

2.18.6 Delete-Accounting-List

Here you can delete parameters.
Telnet path: Setup/Accounting

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 Active

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:

- 1 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

Shows the name of the user.
Telnet path: Setup/Accounting/Last-Snapshot

2.18.9.3 Peer

Shows the name of the remote station.
Telnet path: Setup/Accounting/Last-Snapshot

2.18.9.4 Conn.-Type

Shows the type of connection (e.g. DSL-connection).
Telnet path: Setup/Accounting/Last-Snapshot

2.18.9.5 Rx-KBytes

Shows the received bytes.
Telnet path: Setup/Accounting/Last-Snapshot

2.18.9.6 Tx-KBytes

Shows the forwarding bytes.
Telnet path: Setup/Accounting/Last-Snapshot

2.18.9.8 Total-Time

Shows the time of connection.
Telnet path: Setup/Accounting/Last-Snapshot

2.18.9.9 Connections

Shows the number of connection.
Telnet path: Setup/Accounting/Last-Snapshot

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

2.19 VPN

This menu contains the configuration of the Virtual Private Network (VPN).
Telnet path: /Setup

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

Note: 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

Note: 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

Note: 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

Note: 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

Note: 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

Note: 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

2.19.8 Operating

Switches the VPN module on or off.
Telnet path: /Setup/VPN
Possible values:

- Activated
- Deactivated

Default: Deactivated

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

2.19.9.2 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

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

Note: 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

2.19.9.10 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 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

Note: 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

Note: 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 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

Note: 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

Note: 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 device 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

2.19.10 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

2.19.11 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

2.19.12 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

2.19.12.2 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

2.19.12.3 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

2.19.12.4 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

2.19.12.5 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

2.19.12.6 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

2.19.12.7 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

2.19.12.8 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

2.19.12.9 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

2.19.12.10 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

2.19.12.11 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

2.19.12.12 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

2.19.12.13 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

2.19.12.14 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

2.19.12.15 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

2.19.12.16 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

2.19.12.17 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

2.19.12.18 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

2.19.12.20 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

2.19.12.21 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

2.19.12.22 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

2.19.12.23 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

2.19.12.24 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

2.19.12.25 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

2.19.12.26 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

2.19.12.27 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

2.19.12.28 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

2.19.12.29 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

2.19.12.30 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

2.19.12.31 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

2.19.12.32 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

2.19.12.33 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

2.19.12.34 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

2.19.13 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

2.19.14 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

2.19.15 Legacy dyn. VPN (LCOS5.0x) support

Allows fallback from DynVPNv2 to DynVPNv1.
Telnet path: /Setup/VPN
Possible values:

- Yes
- No

Default: No

2.19.16 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

Note: 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.

Caution: If the device 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.

2.19.17 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

2.19.19 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

2.19.20 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

2.19.21 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

2.19.22 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 entered, 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

Note: 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.

2.19.23 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

2.19.24 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

Note: With a value of 0, the device may take fully advantage of the maximum number permitted by the license. Values above the license limits are ignored.

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

Note: Flexible identity comparison is used when checking the (received) remote identity and also for selecting the certificate based on the local identity.

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

2.19.27 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 (VPN device or VPN client).
Telnet path: /Setup/VPN
Possible values:

- Yes, No

Default: No

Note: The 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.

2.20 LAN-Bridge

This menu contains the settings for the LAN bridge.
Telnet path: Setup

2.20.1 Protocol version

Telnet path: Setup/LAN bridge/Protocol version
No description is available for this parameter yet.

2.20.2 Bridge priority

Telnet path: Setup/LAN bridge/Bridge priority
No description is available for this parameter yet.

2.20.4 Encapsulation-Table

This table defines which protocols are by default used with Ethernet II framing on an Ethernet medium, and which are by default used with SNAP framing on an Ethernet medium.
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 value, i.e. the valid range is from 0001 to ffff. Even if the table is empty, some protocols are implicitly assumed to be listed in this table as type SNAP (namely, IPX and AppleTalk). This may be overridden by explicitly setting their protocol (8137 resp. 80f3) to Ethernet II.
Telnet path: Setup/LAN-Bridge/Encapsulation-Table

2.20.4.2 Encapsulation

Here you can define, weather data packets get an Ethernet-Header or not while being transmitted.
Telnet path: Setup/LAN-Bridge/Encapsulation-Table
Possible values:

- ETH_II
- SNAP

Default: ETH_II

2.20.5 Max age

Telnet path: Setup/LAN bridge/Max age
No description is available for this parameter yet.

2.20.6 Hello time:

Telnet path: Setup/LAN bridge/Hello time
No description is available for this parameter yet.

2.20.7 Forward delay

Telnet path: Setup/LAN bridge/Forward delay
No description is available for this parameter yet.

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.

Note: 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.

Telnet path: Setup/LAN bridge
Possible values:

- Bridge or router (isolated mode)

Default: Bridge

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 is the name of the rule.
Note: This is also the index column of the table, i.e. the table index is a string.
Telnet path: Setup/LAN-Bridge/Protocol-Table
Possible values:

- max. 15 alpha numeric characters

Default: blank

2.20.10.2 Protocol

This is a 4-digit hexadecimal value that allows to match a packet by its Ethernet 2 protocol identifier (e.g. 0800 for IPv4, 8137 for IPX etc.). In case the packet uses 802.x instead of Ethernet 2 framing, its ’protocol type’ is regarded to be the concatenation of DSAP and SSAP, e.g. E0E0 for IPX with 802.x framing. A packet’s protocol type is not regarded if this value is all-zeroes (0000).
Telnet path: Setup/LAN-Bridge/Protocol-Table
Possible values:

- 4-digit hexadecimal number

Default: blank

2.20.10.3 Sub-Protocol

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,...) will match the given value, or if it’s an ARP packet and the ARP type matches the given value.
Telnet path: Setup/LAN-Bridge/Protocol-Table
Possible values:

- max. 5 numeric characters from 0 to 65535

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:

- max. 5 numeric character from 0 to 65535

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:

- max. 5 numeric characters from 0 to 65535

Default: 0

2.20.10.6 Ifc-List

This field specifies the list of LAN interfaces this rule shall be applied to. The syntax of interface lists is given in appendix.
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. The redirection feature is only available for packets that carry 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:

- Drop
- Pass
- Redirect

Default: Drop

2.20.10.8 Redirect-IP-Address

In case the rule is a redirect rule, this field defines the address packets shall be redirected to.
Telnet path: Setup/LAN-Bridge/Protocol-Table
Possible values:

- Valid IP address.

Default: 0.0.0.0.

2.20.10.9 Dest-MAC-Addr.

This setting allows to specify a MAC address that must be present in a packet’s destination MAC address field for the rule to match. The destination MAC address is not regarded if the given MAC address is all-zeroes.
Telnet path: Setup/LAN-Bridge/Protocol-Table
Possible values:

- 12-digit hexadecimal number

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’s 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’s 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 rule depends on the source of the MAC address, as this receives 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

2.20.11 Port-Data

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-Data
Possible values:

- Select from the list of the device's logical interfaces, e.g. LAN-1, WLAN-1 or P2Ü-1-1

2.20.11.3 Active

Setting this switch to ’No’ will block all traffic to and from the respective interface, and will force its operational state to ’disabled’.
Telnet path: Setup/LAN-Bridge/Port-Data
Possible values:

- Yes
- No

Default: Yes

2.20.11.5 Bridge-Group

The LAN interfaces may be individually assigned to one of up to eight bridge groups, which will limit the forwarding of packets to interfaces belonging to the same bridge group. This option is comparable to the port-based VLAN option of some Ethernet switches. Setting an interface’s bridge group to none will remove it from all bridge groups and therefore effectively disable any layer-2 packet forwarding from/to this interface.
Telnet path: Setup/LAN-Bridge/Port-Data
Possible values:

- BRG-1 to BRG-8
- none

Default: BRG - 1
Note: 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

If DHCP tracking is enabled on this LAN interface, this value defines the maximum number of MAC addresses tracked on this interface. Paired with the proper filtering rules in the protocol filter table, this value allows to limit the number of valid allowed DHCP clients in the network segment connected to this LAN interface. A value of 0 (default) disables the limit.
Telnet path: Setup/LAN-Bridge/Port-Data
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 data
Possible values:

- Automatic
- Off
- Off

Default: Automatic

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:

- max. 10 numeric characters

Default: Max. lease period 6,000 minutes, standard lease: 500 minutes

2.20.13 Priority mapping

Telnet path: Setup/LAN bridge/Priority mapping
Description

2.20.13.1 Name

Telnet path: Setup/LAN bridge/Priority mapping/Name
Description
Possible values:

- Max. 16 alpha numeric characters

Default: Blank

2.20.13.2 DSCP value

Telnet path: Setup/LAN bridge/Priority mapping/DSCP value
Description
Possible values:

- Numeric characters from 0 to 255

Default: 0

2.20.13.3 Priority

Telnet path: Setup/LAN bridge/Priority mapping/Priority
Description
Possible values:

- Best-Effort
- Background
- Two
- Excellent-Effort
- Controlled-Latency
- Video
- Voice
- Network-Control

Default: Best-Effort

2.20.20 Spanning-Tree

This submenu holds all entries regarding the spanning tree feature provided by the LAN bridge. It is in accordance with IEEE 802.1D-1998 (classic spanning tree) resp. 802.1D-2004 (rapid spanning tree). See these standards for a detailed description of the configuration entries in this submenu-tree.
Telnet path: Setup/LAN-Bridge

2.20.20.1 Operating

This switch allows to turn the spanning tree feature on and off. If turned off, the device’s LAN bridge will remain invisible for possible other bridges and switches that implement spanning tree. Namely, it will forward bridge PDUs used by spanning tree like any other data packets.
Telnet path: Setup/LAN-Bridge/Spanning-Tree
Possible values:

- Yes
- No

Default: No

2.20.20.2 Bridge-Priority

This value defines the priority of the LAN bridge in the root bridge detection process. The bridge with highest priority (i.e. lowest priority value) will become root bridge. Modification of this setting from the default value (32768) is only necessary if there is a preference for a certain bridge. Even with same bridge priority on all devices, root bridge election will work since the bridges' MAC addresses are taken as a tie-breaker in case of equal priority. Though this menu option will allow configuration of arbitrary 16-bit values, newer revisions of the rapid and multiple spanning tree protocol mandate that the bridge priority shall only be incremented or decremented in steps of 4096, i.e. the lower 12 bits of this value are used for different purposes and might be ignored in future LCOS releases.
Telnet path: /Setup/LAN-Bridge/Spanning-Tree
Possible values:

- max. 5 numeric characters from 0 to 65535

Default: 32768

2.20.20.5 Max-Age

This value defines the maximum age of a message (specified in seconds before it is considered outdated and discarded. Increasing of this value should only be necessary in networks with a possibly high number of hops, and it should be done with care.)
Telnet path: Setup/LAN-Bridge/Spanning-Tree
Possible values:

- max. 65535 seconds

Default: 20 Sec

2.20.20.6 Hello-Time

This time defines how often the bridge shall emit spanning tree messages to its designated (i.e. downstream) ports.
Note: Non-root bridges take over the value from the root bridge, so 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 Sec

2.20.20.7 Forward-Delay

This value defines how fast ports are brought into the forwarding state.
Note: This value has no effect in many cases if the rapid spanning tree protocol is used, since rapid spanning tree includes procedures to determine that a port can be brought in to the forwarding state without waiting so long. Do not change this value without detailed knowledge of spanning tree, since it may increase the potential of temporary loops in the network.
Telnet path: Setup/LAN-Bridge/Spanning-Tree
Possible values:

- max. 32768 seconds

Default: 6 Sec

2.20.20.11 Port-Data

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, given as an 8-bit unsigned value. In case there is more than one port available as path to a certain LAN, and both ports offer the same path cost, this value will be used as a tie-breaker to deduce the port to be used. In case two ports have the same priority, the port with the lower number (i.e. earlier in the table) will be used.

Note: For rapid spanning tree, only the upper four bits of this value will be used, i.e. the value must be incremented and decremented in steps of 16. Lower values mean a higher priority.

Telnet path: /Setup/LAN-Bridge/Spanning-Tree/Port-Data
Possible values:

- max. 255

Default: 128

2.20.20.11.6 Edge-Port

If rapid spanning tree is used, this switch may be used by the administrator to give the algorithm the hint that a port is an edge port, i.e. it is the only port connected to a certain LAN segment. Even if set to yes, rapid spanning tree may override this setting if it detects another bridge in the segment in question.
Telnet path: Setup/LAN-Bridge/Spanning-Tree/Port-Data
Possible values:

- yes
- no

Default: yes or no

2.20.20.11.7 Path-Cost-Override

If set to a value unequal to zero, the path cost of this port will not be computed automatically any more, but instead be set to the given value. This allows the administrator to manually influence the priority of redundant paths in the network.
Telnet path: Setup/LAN-Bridge/Spanning-Tree/Port-Data
Possible values:

- max. 10 numeric characters from 0 to 4294967297

Default: 0

2.20.20.12 Protocol-Version

This switch selects the spanning tree protocol version to be used. Setting this switch to ’Classic’ will engage the algorithm defined IEEE 802.1D-1998 chapter 8, while setting it to ’Rapid’ will engage the rapid spanning three scheme defined by IEEE 802.1D-2004 chapter 17.

Note: Rapid spanning tree is upward-compatible to classic spanning tree, in the sense that rapid spanning tree will automatically fall back to classic spanning tree PDUs and schemes if other bridges are detected that only support classic spanning tree.

Telnet path: /Setup/LAN-Bridge/Spanning-Tree
Possible values:

- classic
- rapid

Default: classic

2.20.20.13 Transmit-Hold-Count

This value limits the number of spanning tree PDUs sent per second if rapid spanning tree is used. It has no effect for the classic spanning tree protocol.
Telnet path: Setup/LAN-Bridge/Spanning-Tree
Possible values:

- max. 999

Default: 6

2.20.20.14 Path-Cost-Computation

Rapid spanning tree introduces new values to compute the path cost of a LAN connection based upon its bandwidth. The values now exploit the full 32-bit range of this parameter, and can now correctly map the capacities of much faster links (the default path cost values of classic spanning tree already assigned a value of 4 to a 1Gbps link, making it difficult to differentiate links of higher bandwidth). The computation of path costs from link speed however has to be consistent across a network, and cannot be automatically detected. By default, the scheme given by classic spanning

tree is used which limits the path cost range to 16-bit values. Setting this value to 'Rapid' will use the new values given by 802.1D-2004. Do this only if all bridges in the network support 32-bit path cost values, and use a consistent setting throughout the whole network. The spanning tree will still configure a loop-free network, but it might not represent the optimal topology.
Telnet path: Setup/LAN-Bridge/Spanning-Tree
Possible values:

- classic
- rapid

Default: classic

2.20.30 IGMP snooping

Telnet path: Setup/LAN bridge/IGMP snooping

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
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).

2.20.30.2 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

2.20.30.3 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
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

2.20.30.4 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
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 the 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 the 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

2.20.30.5 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 "Robustness*Query-Interval+(Query-Response-Interval/2)".
A port loses its router-port status after a time equal to "Robustness*Query-Interval+(Query-Response-Interval/2)".
Telnet path: Setup/LAN bridge/IGMP snooping
Possible values: 10-figure number greater than 0.
Default: 125

Note: The query interval must be greater than the query response interval.

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
Possible values: 10-figure number greater than 0.
Default: 10

Note: The query response interval must be less than the query interval.

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
Possible values: 10-figure number greater than 0.
Default: 2

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 alphanumerical 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

2.20.30.9 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
Possible values:

- 4 to 180 seconds.

Default: 20

2.21 HTTP

This menu contains the HTTP settings.
Telnet path: Setup

2.21.1 Document root

Telnet path: Setup/HTTP/Document root
Description
Possible values:

- Max. 99 alpha numeric characters

Default: Blank

2.21.2 Page-Headers

Undocumented function
Telnet path: Setup/HTTP

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

Telnet path: Setup/HTTP/Page-Headers
Possible values:

- Images
- Texts

Default: Images

2.21.6 Error page style

Normal error display, or bluescreen.
Telnet path: Setup/HTTP
Possible values:

- Standard
- Nifty

Default: Standard

2.21.7 Port

Port for the HTTP server connection.
Telnet path: Setup/HTTP
Possible values:

- max. 5 characters

Default: 80

2.21.8 SSL-Port

Port for the HTTPS server connection.
Telnet path: Setup/HTTP
Possible values:

- max. 5 characters

Default: 443

2.21.9 Max-Tunnel-Connections

The maximum number of simultaneously active HTTP tunnels.
Telnet path: Setup/HTTP
Possible values:

- max. 255 tunnels.

Default: 3

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

2.21.11 Session-Timeout

Period of validity (lease) for the WEBconfig session without user activity, in seconds. When this period expires the password must be re-entered.
Telnet path: Setup/HTTP
Possible values:

- max. 10 characters

Default: 600

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

2.21.14 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
Memory
Ethernet ports
Throughput(Ethernet)
UMTS/modem interface
Router
Firewall
DHCP
DNS
VPN
ADSL

ISDN
DSLoL
Time
IP addresses

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 numeric characters

Default: 0

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:

- active
- inactive
- Only_for_WAN

Default: active

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 Ifc.

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: The default setting for all access paths is "automatic".

2.21.17 Use-User-Provided-Certificate

This option enables the HTTP(S) server of the device to use a SSL certificate provided by the HTTPS client instead of the SSL certificate stored in the device.

Path Telnet: /Setup/HTTP

Possible values:

- Yes
- No

Default: No

2.21.20 Rollout-Wizard

This menu contains the settings for the Rollout Wizard.

Telnet path: Setup/HTTP

2.21.20.1 Operating

Switches the Rollout Wizard on or off. After being switched on the Wizard appears as an option on the WEBconfig 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. 64 alpha numeric characters

Default: Rollout

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

Default: 0

2.21.20.3.2 Ident

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 alpha numeric 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 alpha numeric 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 have no influence on this value. Checkmarks are set by default if the default is not empty.

Default: Label

2.21.20.3.5 Min-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

Default: 0

2.21.20.3.6 Max-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

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 alpha numeric 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. When the Rollout Wizard is executed, the actions are processed in ascending sequence.
Telnet path: Setup/HTTP/Rollout-Wizard/Actions
Possible values:

- 2 to 232

Default: 0

2.21.20.4.2 0 switches off the monitoring of the relative expiry time.

Action to be executed by the Rollout Wizard after the user data has 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 device. The following example sets the name of the device to 'MyDevice':
exec: set /setup/name MyDevice
mailto: Enables an e-mail to be sent upon entry of the address, subject and body text, for example:
mailto:admin@mydevice.de?subject=Rollout?body=Device setup completed
http and http: 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}(Branch)
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.
Note: If the expression for the action contains spaces then the expression must be enclosed by quotation marks.
Note: 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

2.21.20.5 Renumber variables

As already mentioned, variables and actions are displayed and processed in the sequence of their index. A new entry must sometimes be inserted between two variables/actions with adjacent indices. 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

2.21.20.6 Renumber actions

As already mentioned, variables and actions are displayed and processed in the sequence of their index. A new entry must sometimes be inserted between two variables/actions with adjacent indices. 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-for

The first screen shows the status of the connection.
Telnet path: Setup/HTTP/Rollout-Wizard

2.21.30 File server

This menu holds the settings for the file server using an external USB medium.
Telnet path: Setup/HTTP/File server

2.21.30.1 Public subdirectory

This directory is used on an USB medium as root directory. All other files on the USB medium will be ignored.
Telnet path: Setup/HTTP/File server/Public subdirectory
Possible values:

- 64 characters

Default: public_html

2.21.30.2 Operating

This parameter is used to activate or deactivate the file server for the USB medium.
Telnet path: Setup/HTTP/File server/Operating
Possible values:

- Yes
- No

Default: Yes

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

2.22.2 Server

This table defines the SYSLOG clients.
Telnet path: Setup/SYSLOG

2.22.2.1 Idx.

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: 0.0.0.0

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:

- max. 2 numeric characters
- Alarm: 01
- Error: 02
- Warning: 04
- Information: 08
- Debug: 10

Default: 00
Special values: 00: No level is defined.

2.22.2.6 Loopback-Addr.

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 interface, the address of which is to be used.
- "INT" for the address of the first intranet.
- "DMZ" for the address of the first DMZ

  Note: If you have an interface named "DMZ", then the name of that interface will be taken.
- LB0 to LBF for the 16 loopback addresses.
- Any IP address can be entered in the form x.x.x.x.

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
Here you can set the configuration for following values:

- System
- Login
- Systemtime
- Console-login
- Connections
- Accounting
- Administration
- Router

2.22.3.2 Facility

Mapping sources to specific facilities.
Telnet path: Setup/SYSLOG/Facility-Mapper
Here you can set the configuration for the following values:

- KERNEL
- AUTH
- CRON
- AUTHPRIV
- LOCAL0
- LOCAL1
- LOCAL2
- LOCAL3

2.22.4 Port

Port used for sending SYSLOG messages.
Telnet path: Setup/SYSLOG
Possible values:

- Max. 10 characters

Default: 514

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

2.23 Interfaces

This menu contains the settings for the interfaces.
Telnet path: Setup

2.23.4 DSL

Telnet path: Setup/Interfaces

2.23.4.1 Ifc

Telnet path: Setup/Interfaces/S0/Ifc
Description

2.23.4.2 Operating

Telnet path: Setup/Interfaces/S0/Operating
Description

2.23.4.6 Mode

Telnet path: Setup/Interfaces/S0/Mode
Description

2.23.4.16 Upstream rate

Telnet path: Setup/Interfaces/S0/Upstream rate
Description

2.23.4.17 Ext. overhead

Telnet path: Setup/Interfaces/S0/Ext. overhead
Description

2.23.4.18 Downstream rate

Telnet path: Setup/Interfaces/S0/Downstream rate
Description

2.23.4.23 LAN Ifc

Telnet path: Setup/Interfaces/S0/LAN Ifc
Description

2.23.7 Modem mobile

Telnet path: Setup/Interfaces

2.23.7.1 Ifc

Telnet path: Setup/Interfaces/Modem mobile/Ifc
Description
Possible values:

- DCL-1
- EXT

Default: EXT

2.23.7.2 Operating

Telnet path: Setup/Interfaces/Modem mobile/Operating
Description
Possible values:

- No
- Modem

Default: No

2.23.7.21 Data rate

Telnet path: Setup/Interfaces/Modem mobile/Data rate
Description
Possible 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 alphanumerical characters

Default: Blank

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 Ifc

Select from the logical WLAN interfaces.
Telnet path: Setup/Interfaces/WLAN/Network
Possible values:

- Select from the available logical WLAN interfaces.

2.23.20.1.2 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 alpha numeric 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:

- Yes
- No

Default: Yes

2.23.20.1.9 MAC-Filter

In the MAC filter list (WLAN Security --> Stations --> Stations) the MAC addresses of the Clients are entered, which may connect to the access point. With the switch 'MAC filter enabled' the MAC filter list for single logical networks can be switched off.
Telnet path: Setup/Interfaces/WLAN/Network
Possible values:

- Yes
- No

Default: Yes
Note: The MAC filter list is always required in logical networks, in which clients log in with an individual passphrase over LEPS. The Passphrase used with LEPS must also be enterd in the MAC filter list. For the log in with an individual Passphrase the MAC filter list is always considered, even if the option is deactivated at this place.

2.23.20.1.10 Max-Stations

Here you can specify the number of clients, that can connect to the access point. Further clients are 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
Note: Client-bridge mode can only be used between two devices which both support this feature.

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

Note: 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 WLAN network.
Telnet path: Setup/Interfaces/WLAN/Network/Aironet extensions
Possible values:

- Yes
- No

Default: Yes

2.23.20.1.16 Min-Client-Strength

This values defines the minimum signal strength of WLAN clients which the access point will accept, even if a matching SSID or a wildcard SSID is provided. The access point will silently discard all probe requests below this threshold.
You can use this option to prevent large numbers of potential WLAN clients, e.g. mobile handsets, to decrease the WLAN performance with probe requests looking for available WLAN networks.
The strength threshold is specified in percent, which can be translated into an SNR: a threshold of 100 percent means a minimum SNR of 64 dBm, 50 percent means 32 dBm and so on.
Path Telnet: /Setup/Interfaces/WLAN/Network
Possible values:

- 0% to 100%

Default: 0
Special values: '0' deactivates the minimum signal strenght, the access point will answer all requests.

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 Ifc

Details for the data transfer over the logical interface are set on the 'Transmission' tab.
Telnet path: Setup/Interfaces/WLAN/Transmission
Possible values:

- Select from the available logical WLAN interfaces.

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

2.23.20.2.3 Min-Tx-Rate

The access point normally negotiates the data transmission speeds with the connected WLAN clients continuously and dynamically. In doing this, the access point adjusts the transmission speeds to the reception conditions. As an alternative, you can set fixed values for the minimum and maximum transmission speeds if you wish to prevent the dynamic speed adjustment.
Telnet path: Setup/Interfaces/WLAN/Transmission
Possible values:

- Automatic
- Select from the available speeds

Default: automatically

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 are able to connect "faster".
Telnet path: Setup/Interfaces/WLAN/Transmission
Possible values:

- Select from the available speeds

Default: 2 Mbit/s

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 potential 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

The access point normally negotiates the data transmission speeds with the connected WLAN clients continuously and dynamically. In doing this, the access point adjusts the transmission speeds to the reception conditions. As an alternative, you can set fixed values for the minimum and maximum transmission speeds 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

2.23.20.2.10 Min-Frag-Len

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 repeats the attempt to transmit.
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 less time.
Telnet path: Setup/Interfaces/WLAN/Transmission
Possible values:

- 0 to 15

Default: 10

2.23.20.2.13 Short guard interval

Put simply, the guard interval reduces the signal distortion caused by intersymbol interference (ISI) when using signal multiplexing (OFDM).
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 help prevent the short-guard interval from being used.
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 new and third dimension to the frequency-time matrix available to radio communications until now: 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

Telnet path: Setup/Interfaces/WLAN/Transmission/Send aggregates
Description
Possible values:

- No
- Yes

Default: No

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 new and third dimension to the frequency-time matrix available to radio communications until now: 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

Telnet path: Setup/Interfaces/WLAN/Transmission/EAPOL rate
Description
Possible values:

- Like-Data
- 1M
- 2M
- 5.5M
- 11M
- 6M
- 9M
- 12M
- 18M
- 24M
- 36M
- 48M
- 54M
- HT-1-6.5M
- HT-1-13M
- HT-1-19.5M
- HT-1-26M
- HT-1-39M
- HT-1-52M
- HT-1-58.5M
- HT-1-65M
- HT-2-13M

- HT-2-26M
- HT-2-39M
- HT-2-52M
- HT-2-78M
- HT-2-104M
- HT-2-117M
- HT-2-130M

Default: Like-Data

2.23.20.2.20 Max. aggr. packet number

Telnet path: Setup/Interfaces/WLAN/Transmission/Max. aggr. packet number
Description
Possible values:

- Low
- Medium
- High
- Minicell
- Microcell
- Off

Default: Low

2.23.20.2.21 ProbeRsp retries

Telnet path: Setup/Interfaces/WLAN/Transmission/ProbeRsp retries
Description
Possible values:

- Numeric characters from 0 to 255

Default: 3

2.23.20.2.22 Receive-Aggregates

This option enables or disables the possibility to receive aggregate packets in 802.11n WLAN networks.
Disable this function only if certain WLAN clients are not able to connect to the WLAN and you assume that the reason is based on 802.11n aggregate packets.
Path Telnet: /Setup/Interfaces/WLAN/Transmission
Possible values:

- yes
- no

Default: yes

2.23.20.3 Encryption

Here you can adjust specific encryption settings for each logical wireless LAN network (MultiSSID) supported by your device.
Telnet path: Setup/Interfaces/WLAN

2.23.20.3.1 Ifc

Open the list with the button for WPA or Private WEP settings.
Telnet path: Setup/Interfaces/WLAN/Encryption
Possible values:

- Select from the available logical WLAN interfaces.

2.23.20.3.2 Encryption

Select the type of encryption for the individual logical WLAN interfaces.
Telnet path: Setup/Interfaces/WLAN/Encryption
Possible values:

- Yes
- No

Default: Yes

2.23.20.3.3 Default-Key

The WEP key 1, that applies only to its respective logical WLAN interface, can be entered in different ways depending on the key length.
Telnet path: Setup/Interfaces/WLAN/Encryption
Possible values:

- Key 1
- Key 2
- Key 3
- Key 4

Default: Key 1
Note: 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

Set the encryption method to be used here.
Telnet path: Setup/Interfaces/WLAN/Encryption
Possible values:

- 802.11i (WPA)-PSK
- WEP 152
- WEP 128, WEP 64
- WEP 152-802.1x
- WEP 128-802.1x
- WEP 64-802.1x

Default: WEP-128 (104 Bit)
Note: Consider that not all wireless cards support all encryption methods.

2.23.20.3.5 Authentication

If the encryption method was set as WEP encryption, two different methods for the authentication of the WLAN client are available: 'Open system' and 'Shared key' method, the first data packet is transmitted unencrypted and must be sent back by the client correctly encrypted. This method presents potential attackers with at least one data packet that is unencrypted.
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
Note: 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
Note: Be aware that the security of this encryption method depends on the confidential treatment of this passphrase. Passphrases should not be made public to larger circles of users.

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

2.23.20.3.10 Client EAP method

Devices 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.
Note: The selected client EAP method must match the settings of the access point that this device 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
Note: In addition to setting the client EAP method, also be sure to observe the corresponding setting for the WLAN client operation mode.
The client EAP method setting has no function on logical WLAN networks other than WLAN 1.

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 seconds

Default: 0
Special values: 0 = Rekeying deactivated

2.23.20.3.12 WPA1-Session-Keytypes

If '802.11i (WPA)-PSK' has been entered as the encryption method, the procedure for generating a session or group key can be selected here:
AES – the AES method will be used.
TKIP – the TKIP method will be used.
AES/TKIP – the AES method will be used. If the client hardware does not support the AES method, TKIP will be used.
Telnet path: Setup/Interfaces/WLAN/Encryption
Possible values:

- TKIP
- AES
- TKIP/AES

Default: TKIP/AES

2.23.20.3.13 WPA2-Session-Keytypes

If '802.11i (WPA)-PSK' has been entered as the encryption method, the procedure for generating a session or group key can be selected here:
AES – the AES method will be used.
TKIP – the TKIP method will be used.
AES/TKIP – the AES method will be used. If the client hardware does not support the AES method, TKIP will be used.
Telnet path: Setup/Interfaces/WLAN/Encryption
Possible values:

- TKIP
- AES
- TKIP/AES

Default: TKIP/AES

2.23.20.4 Group-Encryption-Keys

Wired Equivalent Privacy (WEP) is an effective method for the encryption of data for wireless transmission. The WEP method uses keys of 40 (WEP64), 104 (WEP128) or 128 bits (WEP152) in length. Each WLAN interface has four WEP keys: a special key for each logical WLAN interface and three common group WEP keys for each physical WLAN interface.
Telnet path: Setup/Interfaces/WLAN
Note: If 802.1x/EAP is in use and the 'dynamic key generation and transmission' is activated, the group keys from 802.1x/EAP will be used and are consequently no longer available for WEP encryption.

2.23.20.4.1 Ifc

Open the list with the button for WEP Group Keys. These WEP keys apply to the physical WLAN interface and thus globally to all of the associated logical WLAN interfaces.
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 key 2. WEP keys can be entered as ASCII characters or in hexadecimal form. The hexadecimal form begins with the characters '0x'.
Telnet path: Setup/Interfaces/WLAN/Group-Encryption-Keys
Possible values:

- 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 key 3. WEP keys can be entered as ASCII characters or in hexadecimal form. The hexadecimal form begins with the characters '0x'.
Telnet path: Setup/Interfaces/WLAN/Group-Encryption-Keys
Possible values:

- 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 key 4. WEP keys can be entered as ASCII characters or in hexadecimal form. The hexadecimal form begins with the characters '0x'.
Telnet path: Setup/Interfaces/WLAN/Group-Encryption-Keys
Possible values:

- 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 Keytype-2

Select the length and the format (ASCII or HEX) of the key 2 depending on the best option available in the wireless network cards that register with your WLAN. If the encryption in an access point is set to WEP 152, some clients may not be able to log into the WLAN as their hardware does not support the key length.
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 Keytype-3

Select the length and the format (ASCII or HEX) of the key 3 depending on the best option available in the wireless network cards that register with your WLAN. If the encryption in an access point is set to WEP 152, some clients may not be able to log into the WLAN as their hardware does not support the key length.
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 Keytype-4

Select the length and the format (ASCII or HEX) of the key 4 depending on the best option available in the wireless network cards that register with your WLAN. If the encryption in an access point is set to WEP 152, some clients may not be able to log into the WLAN as their hardware does not support the key length.
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 parameters for the communication between and the behavior of base stations.
Telnet path: Setup/Interfaces/WLAN

2.23.20.5.1 Ifc

Opens the settings for the physical WLAN interface.
Telnet path: Setup/Interfaces/WLAN/Interpoint-Peers
Possible values:

- Select from the available physical WLAN interfaces.

2.23.20.5.2 Enable

Select if and how access points that are within radio range of one another are to be connected.
Telnet path: Setup/Interfaces/WLAN/Interpoint-Peers
Possible values:

- Off: This access point can only communicate with mobile stations.
- On: This access point can also communicate with other access points to connect several local wireless networks.
- Exclusive: This access point can only communicate wilh other access points; mobile stations cannot connect to this access point (pure WLAN bridge).

Default: On

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

2.23.20.5.10 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 5 GHz 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 2.4 GHz 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 takes over the leadership when selecting a free WLAN channel.
- Slave: All other access points will search for a channel until they have found a transmitting Master.

Default: Master
Note: The channel selection scheme needs to be 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 alpha numeric characters

Default: blank

2.23.20.6 Client-Modes

If the device is operating as a client, the tab 'Client mode' can be used for further settings that affect the behavior as a client.
Telnet path: Setup/Interfaces/WLAN

2.23.20.6.1 Ifc

Opens the settings for the physical WLAN interface.
Telnet path: Setup/Interfaces/WLAN/Client-Modes
Possible values:

- Select from the available physical WLAN interfaces.

2.23.20.6.3 Connection keepalive

This option helps ensuring 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' controls whether the station can register only with infrastructure networks, or also with adhoc networks.
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:

- All
- 2.4 GHz
- 5 GHz

Default: All

2.23.20.6.6 Preferred-BSS

If the client station is only supposed to log in on a certain access point, you can enter the MAC address of the WLAN card from the access point.
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

Note: Address adaptation only works when just one computer is connected to the client station.

2.23.20.6.8 Cl.-Brg.-Support

With address-adaption the MAC address of only one connected device is visible to the access point. With a Client-Bridge Support all MAC addresses of the stations in the LAN behind the client stations are transmitted transparently to the access point.

Telnet path: Setup/Interfaces/WLAN/Client-Modes

Possible values:

- on
- off

Default: off

Note: The Client-Bridge mode can only be used between two devices which support this feature. Applying the Client-Bridge mode must also be activated in the settings for the logical network of the access point.

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 65535 kbps

Default: 0
Special values: 0: No limit
Note: 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".

2.23.20.6.10 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 65535 kbps

Default: 0
Special values: 0: No limit
Note: 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 AP selection preference

Here you select how this interface is to be used.
Telnet path: Setup/Interfaces/WLAN/Client-Modes
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

2.23.20.7 Operational

In the operational settings you can set basic parameters for operating your WLAN interface.
Telnet path: Setup/Interfaces/WLAN

2.23.20.7.1 Ifc

Opens the settings for the physical WLAN interface.
Telnet path: Setup/Interfaces/WLAN/Operational
Here you can set the configuration for the following 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:

- Yes
- No

Default: Yes

2.23.20.7.3 Operation-Mode

The 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: Wireless routers: Base station; 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 the better the reception quality in the respective antenna position is.
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 device in access point mode.

- Client signal strength: In this operation mode, this LED displays the signal strength of the access point with which the device 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 device 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 device 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 break. 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

Note: 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.

Note: 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 Ifc

Opens the settings for the physical WLAN interface.
Telnet path: Setup/Interfaces/WLAN/Radio settings
Possible values:

- Select from the available physical WLAN interfaces.

2.23.20.8.2 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
Note: 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 range and, data transfer rates.

2.23.20.8.3 5GHz-Mode

Using two neighboring, vacant channels for wireless transmissions can increase the transfer speeds up to 108 Mbps. Set this option for the 2.4 GHz band by selecting the drop down list '2.4 GHz mode', for the 5 GHz band in the appropriate list '5 GHz mode' below.
Telnet path: Setup/Interfaces/WLAN/Radio-Settings
Possible values:

- 54 Mbit/s-Mode
- 108 Mbit/s-Turbo-Mode

Default: 802.11a (54 Mbit/s-Mode) or 802.11a/n mixed (108 Mbit/s-Turbo-Mode) with 11n devices

2.23.20.8.4 Maximum-Distance

Large distances between transmitter and receiver give rise to increasing delays for the data packets. If a certain limit is exceeded, the responses to transmitted packets no longer arrive within an acceptable time limit. The entry for maximum distance increases the wait time for the responses. This distance is converted into a delay which is acceptable for wireless communications.
Telnet path: Setup/Interfaces/WLAN/Radio-Settings
Possible values:

- 0 to 65535 km

Default: 0

2.23.20.8.6 Radio-Band

When selecting the frequency band on the 'Radio' tab under the physical interface settings, you decide whether the WLAN card operates in the 2.4 GHz or in the 5 GHz band.
Telnet path: Setup/Interfaces/WLAN/Radio-Settings
Possible values:

- 2.4 GHz
- 5 GHz

Default: 2.4 GHz
Note: In some countries, the use of the DFS method for automatic channel selection is a legal requirement. Selecting the subband also defines the radio channels that can be used for the automatic channel selection.

2.23.20.8.7 Subbands

In the 5 GHz band, a subband can also be selected 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:

- Depends on the frequency band selected.

Default: 11

Note: 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

Two different wireless standards are based on the 2.4 GHz band: the IEEE 802.11b standard with a transfer rate of up to 11 Mbps and the IEEE 802.11g standard with up to 54 Mbps. When 2.4 GHz is selected as the frequency band, the data transfer speed can be set as well.
The 802.11g/b compatibility optimizes speed and compatibility with slower clients. 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)
Observe: Clients supporting only the slower standards may not be able to register with the WLAN if the speeds set here are higher.

2.23.20.8.10 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 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.
An 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

Note: 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 device 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 device searches the active band for currently unused frequencies to find available access points. This value is the time interval between search cycles.
Devices 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 unauthorized access points should be recognized, e.g. 1 hour. Conversely, devices 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
Note: Forced DFS scans require that the device is set with the correct system time.

2.23.20.8.16 Allow 40MHz

The 802.11n standard specifies a channel bonding from 20MHz to 40MHz. The default setting automatically optimizes the value for bandwidth. If the momentary operting 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.
Telnet path: Setup/Interfaces/WLAN/Radio settings/Allow 40 MHz

2.23.20.8.17 Antenna mask

Telnet path: Setup/Interfaces/WLAN/Radio settings/Antenna mask
Description
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
- Day

Default: Seconds

2.23.20.8.19 Channel pairing

Telnet path: Setup/Interfaces/WLAN/Radio settings/Channel pairing
Description
Possible values:

- 11n-compliant
- legacy-turbo-friendly

Default: 11n-compliant

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

Note: 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.

Note: 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.

2.23.20.9 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 Ifc

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

Activates or deactivates the bursting for packets. This increases the data throughput.
Telnet path: /Setup/Interfaces/WLAN/Performance
Possible values:

- On
- Off

Default: off

2.23.20.9.5 QoS

If a packet for transmission contains a VLAN tag and it priority is not equal to zero, then this priority will be used to prioritize the packet in the WLAN. Otherwise, the top three bits of the TOS/DiffServ field of the IP header are mapped according to IEEE 802.11 e (table 20.23) to the four priority levels of the WLAN.
Telnet path: Setup/Interfaces/WLAN/Performance
Possible values:

- On
- Off

Default: off
Note: 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

Settings in the beaconing table influence the transmission of beacons by the access point in AP mode. In part this can influence the roaming behavior of clients, and in part this serves to optimize the MultiSSID mode for older WLAN clients.
Telnet path: Setup/Interfaces/WLAN

2.23.20.10.1 Ifc

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 Kμs between beacon transmission (1 Kμs corresponds to 1024 microseconds and is a measurement unit of the 802.11 standard. 1 Kμs 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 a non functioning 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 Kμs, then the beacons will be sent to the three WLANs every 100 Kμs. 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 Kμs to WLAN-1, followed by WLAN-2 and WLAN-3. For the second beacon transmission (100 Kμs) WLAN-2 is the first recipient, followed by WLAN-3 and then WLAN-1. For the third beacon transmission (200 Kμs) 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 Kμs, WLAN-1 only is sent; after 33.3 Kμs WLAN-2, after 66.6

Kµs 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 Kµs) is WLAN-1, WLAN-2 and WLAN-3; the second transmission is in the same order, and so on.

Default: Cyclic
Note: 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 Ifc

Opens the Expert settings for the physical WLAN interface.
Telnet path: Setup/Interfaces/WLAN/Roaming
Possible values:

- Select from the available physical WLAN interfaces.

2.23.20.11.2 Beacon miss threshold

The beacon miss 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 smaller 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
Note: 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
Note: 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

2.23.20.11.10 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

2.23.20.12 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 Ifc

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

Select, if you recognize by MAC address or Station name.
Telnet path: /Setup/Interfaces/WLAN/Interpoint-Settings
Possible values:

- MAC address
- station name

Default: MAC-address

2.23.20.12.3 MAC-Address

Enter the MAC address of the wireless LAN adapter for the access point that is connected via Point-to-Point link. MAC address is a hexadecimal numbers with 12 digits (e.g. 00A057010203) The corresponding MAC address can be found on the back of the wireless LAN adapter or under 'Node-ID' in the menu 'Status->WLAN statistics' of the device to be connected via Point-to-Point.
Telnet path: Setup/Interfaces/WLAN/Interpoint-Settings
Possible values:

- Valid MAC address.

Default: blank
Note: 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

Enter here the name of an access point to be connected via Point-to-Point. This name can be the configured device name or a name separately configured in the Point-to-Point menu for each physical WLAN interface.
Telnet path: Setup/Interfaces/WLAN/Interpoint-Settings
Possible values:

- Selection from the list of the defined peers.

Default: blank

2.23.20.12.5 Operating

Activate or deactivate the point-to-point partners.
Telnet path: /Setup/Interfaces/WLAN/Interpoint-Settings
Possible values:

- yes
- no

Default: no

2.23.20.12.6 Tx-Limit

This option enables or disables the possibility to receive aggregate packets in 802.11n WLAN networks.
Disable this function only if certain WLAN clients are not able to connect to the WLAN and you assume that the reason is based on 802.11n aggregate packets.
Path Telnet: /Setup/Interfaces/WLAN/Interpoint-Settings
Possible values:

- Maximum 10 numerical characters

Default: 0

2.23.20.12.7 Rx-Limit

Enter the bandwidth limit (kbps) in the receive direction.The value 0 means there is no limit.
Path Telnet: /Setup/Interfaces/WLAN/Interpoint-Settings
Possible values:

- Maximum 10 numerical characters

Default: 0
This setting is only available for devices with a WLAN module.

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/WLAN/LAN interfaces

2.23.21.1 Ifc

Opens the settings for the LAN interfaces.
Telnet path: Setup/Interfaces/WLAN/LAN interfaces/Ifc
Possible values:

- Select from the available LAN interfaces.

2.23.21.2 Connector

Telnet path: Setup/Interfaces/WLAN/LAN interfaces/Connector
Description
Possible values:

- Auto
- 10B-T
- FD10B-TX
- 100B-TX
- FD100B-TX
- Power-Down

Default: Auto

2.23.21.3 MDI mode

Telnet path: Setup/Interfaces/WLAN/LAN interfaces/MDI mode
Description
Possible values:

- Auto
- MDI
- MDIX

Default: Auto

2.23.21.7 Active

Activate or deactivate the selected LAN interface.
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

Note: 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 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

Telnet path: Setup/Interfaces
Commands and options for an external modem optionally connected to the serial interface.

2.23.40.1 Ring count

Telnet path: Setup/Interfaces/Modem/Ring count
Description
Possible values:

- Numeric characters from 0 to 99

Default: 1

2.23.40.2 Echo-off command

Telnet path: Setup/Interfaces/Modem/Echo-off command
Description
Possible values:
Max. 9 alpha numeric characters
Default: E0

2.23.40.3 Reset

Telnet path: Setup/Interfaces/Modem/Reset
Description
Possible values:
Max. 9 alpha numeric characters
Default: &F

2.23.40.4 Init. command

Telnet path: Setup/Interfaces/Modem/Init. command
Description
Possible values:

- Max. 63 alpha numaric characters

Default: L0X1M1S0=0

2.23.40.5 Dial command

Telnet path: Setup/Interfaces/Modem/Dial command
Description
Possible values:

- Max. 31 alpha numeric characters

Default: DT

2.23.40.6 Request ID

Telnet path: Setup/Interfaces/Modem/Request ID
Description
Possible values:

- Max. 9 alpha numeric characters

Default: I6

2.23.40.7 Answer command

Telnet path: Setup/Interfaces/Modem/Answer command
Description
Possible values:

- Max. 9 alpha numeric characters

Default: A

2.23.40.8 Disconnect command

Telnet path: Setup/Interfaces/Modem/Disconnect command
Description
Possible values:

- Max. 9 alpha numeric characters

Default: H

2.23.40.9 Escape sequence

Telnet path: Setup/Interfaces/Modem/Escape sequence
Description
Possible values:
Max. 9 alpha numeric characters
Default: +++

2.23.40.10 Escape prompt delay (ms)

Telnet path: Setup/Interfaces/Modem/Escape prompt delay (ms)
Description
Possible values:

- Numeric characters from 0 to 9999

Default: 1000

2.23.40.11 Init. dial

Telnet path: Setup/Interfaces/Modem/Init. dial
Description
Possible values:

- Max. 63 alpha numeric characters

Default: Blank

2.23.40.11 Init. answer

Telnet path: Setup/Interfaces/Modem/Init. answer
Description
Possible values:

- Max. 63 alpha numeric characters

Default: Blank

2.23.40.13 Cycletime AT poll (s)

Telnet path: Setup/Interfaces/Modem/Cycletime AT poll (s)
Description
Possible values:

- Numeric characters from 0 to 9

Default: 1

2.23.40.14 AT poll count

Telnet path: Setup/Interfaces/Modem/AT poll count
Description
Possible values:

- Numeric characters from 0 to 9

Default: 5

2.23.41 Mobile telephony

The settings for mobile telephony are located here.
Telnet path: /Setup/Interfaces/Mobile

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

Note: 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

Note: 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.

2.23.41.2 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

2.23.41.3 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 PUK entry procedure.
Telnet path:/Setup/Interfaces/Mobile/Input-PUK

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.

2.23.41.7 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

2.23.41.9 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.

2.23.41.10 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.

2.23.41.11 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

Note: This setting only takes effect if the fallback from 3G to 2G connections has been configured.

2.25 RADIUS

This menu contains the settings for the RADIUS server.
Telnet path: Setup

2.25.4 Auth. 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 Auth. 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

Telnet path: Setup/RADIUS/Backup query strategy
Description
Possible values:

- Block
- Cyclic

Default: Block

2.25.10 Server

This menu contains the settings for the RADIUS server.
Telnet path: Setup/RADIUS

2.25.10.1 Authentication port

Specify here the port used by the authenticators to communicate with the RADIUS server in the device.
Telnet path: Setup/RADIUS/Server
Possible values:

- Max. 4 numbers

Default: 1812
Special values: 0: Switches the RADIUS server off.

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 access point.
Telnet path: Setup/RADIUS/Server/Clients
Possible values:

- max. 32 alpha numeric 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 Protocols

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: 0.0.0.0

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 alpha numeric 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-Addr.

An optional source address can be configured here. This address is used instead of the source address, which is otherwise obtained automatically for the respective destination.
Telnet path: /Setup/RADIUS/Server/Forward-Servers
Possible values:

- Name of the IP interface, the address of which is to 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 IP address can be entered in the form x.x.x.x.

Default: blank

Note: If there is an interface named "DMZ", then its address is used.

Note: If the list of IP networks or loopback addresses contains an entry named 'DMZ', the associated IP address is used.

2.25.10.3.7 Protocol

Protocol for communication between the internal RADIUS server and the forwarding server.
Path Telnet: Setup/RADIUS/Server/Forward servers
Possible values:

- RADSEC
- RADIUS

Default: RADIUS

2.25.10.3.8 Accnt.-IP-Address

Enter here the IP address of the RADIUS server for accounting, if this is different from the main realm defined in this record.
Path Telnet: /Setup/RADIUS/Server/Forward servers
Possible values:

- Valid IP address

Default: 0.0.0.0

Note: If this value is not set, the 'IP address' defined in this record is use even for accounting.

2.25.10.3.9 Accnt.-Port

Enter here the port of the RADIUS server for accounting, if this is different from the main realm defined in this record.
Path Telnet: /Setup/RADIUS/Server/Forward servers
Possible values:

- Valid IP port, maximum 5 characters

Default: 0

Note: If this value is not set, the 'Port' defined in this record is use even for accounting.

2.25.10.3.10 Accnt.-Secret

Enter here the password used for accessing the RADIUS server for accounting, if this is different from the main realm defined in the corresponding record.
Path Telnet: /Setup/RADIUS/Server/Forward servers
Possible values:

- Maximum 32 alphanumerical characters

Default: empty

Note: If this value is empty, the 'Secret' defined in this record is use even for accounting.

2.25.10.3.11 Accnt.-Loopback-Addr.

An optional source address can be configured here, if this is different from the main realm defined in this record. This address is used instead of the source address, which is otherwise obtained automatically for the respective destination.
Path Telnet: Setup/RADIUS/Server/Forward-Servers
Possible values:

- Name of the IP interface, the address of which is to 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 IP address can be entered in the form x.x.x.x.

Default: blank

Note: If there is an interface named "DMZ", then its address is used.

Note: If the list of IP networks or loopback addresses contains an entry named 'DMZ', the associated IP address is used.

Note: If this value is not set, the 'Loopback-Addr.' defined in this record is use even for accounting.

2.25.10.3.12 Accnt.-Protocol

Protocol for communication between the internal RADIUS server and the forwarding server, if this is different from the main realm defined in this record..
Path Telnet: Setup/RADIUS/Server/Forward servers
Possible values:

- RADSEC
- RADIUS

Default: RADIUS

Note: If this value is not set, the 'Protocol' defined in this record is use even for accounting.

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

2.25.10.7 Users

Telnet path: Setup/RADIUS/Server/Users
In the following table, enter the data for the users that are to be authenticated by this server.
Multiple logins
Allows a single user account to login multiple times simultaneously.
Possible values: Yes, No
Default: Yes

Note: 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.

Note: The two options can be combined. In this case the user account expires when one of the two limiting values has been reached.

Note: 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

Note: 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 alpha numeric characters

Default: Blank

2.25.10.7.2 Password

User password.
Telnet path: Setup/RADIUS/Server/Users
Possible values:

- Max. 32 alpha numeric characters

Default: Blank

2.25.10.7.3 Limit auth. 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

Bandwidth restriction for RADIUS clients.
Telnet path: Setup/RADIUS/Server/Users/Tx limit
Possible values:

- 0 to 9999 kbps

Default: 0

2.25.10.7.8 Rx limit

Bandwidth restriction for RADIUS clients.
Telnet path: Setup/RADIUS/Server/Users/Rx limit
Possible values:

- 0 to 9999 kbps

Default: 0

2.25.10.7.9 Multiple login

Telnet path: Setup/RADIUS/Server/Users/Multiple login
Description
Possible values:

- Yes
- No

Default: Yes

2.25.10.7.10 Abs. expiry

Telnet path: Setup/RADIUS/Server/Users/Abs. expiry
Description
Possible values:

- Max. 20 numeric and special characters, e. g. 10/06/2010 06:15:29

Default: Blank

2.25.10.7.11 Time budget

Telnet path: Setup/RADIUS/Server/Users/Time budget
Description
Possible values:

- Max. 10 numeric characters

Default: 0

2.25.10.7.12 Volume budget

Telnet path: Setup/RADIUS/Server/Users/Volume budget
Description
Possible values:
Numeric characters from 0 to 4289999999
Default: 0

2.25.10.7.13 Expiry type

Telnet path: Setup/RADIUS/Server/Users/Expiry type
Description
Possible values:

- absolute
- relative
- no entry
- absolute, relative (both)

Default: no entry

2.25.10.7.14 Rel. expiry

Telnet path: Setup/RADIUS/Server/Users/Rel. expiry
Description
Possible values:

- Numeric characters from 0 to 4289999999

Default: 0

2.25.10.7.15 Comment

You can enter a comment here.
Telnet path: Setup/RADIUS/Server/Users/Comment

2.25.10.7.16 Service type

Telnet path: Setup/RADIUS/Server/Users/Service type
Description
Possible values:

- Any
- Framed
- Login
- Auth.-Only

Default: Any

2.25.10.10 EAP

This menu contains the EAP settings.
Telnet path: Setup/RADIUS/Server

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

2.25.10.10.2 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

2.25.10.10.3 Reauth-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.
Note: 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.
Note: The function is not supported by all authenticators.

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). If 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

2.25.10.10.6 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). If 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

2.25.10.10.7 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

Maximum Transmission Unit used as default for EAP connections.
Telnet path: Setup/RADIUS/Server/EAP/Default MTU
Possible values:

- 100 to 1496 bytes

Default: 1036 bytes

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: 1813
Special values: 0: Switches the use of this function off.

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.

2.25.10.13 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. 4 numbers

Default: 2083
Special values: 0: Deactivates RADSEC in the RADIUS server.

2.25.10.14 Auto-cleanup user table

Telnet path: Setup/RADIUS/Server/Auto-cleanup user table
Possible values:

- Yes
- No

Default: No

2.25.10.15 Allow-Status-Requests

Use this option to enable or disable the processing of RADIUS status requests. Using this requests the WLAN clients can check if a RASIUS server is available before sending requests for authentication or authorization. If this option is enabled, the RADIUS server in the device will respond to these requests.
Path Telnet: /Setup/RADIUS/Server
Possible values:

- yes
- no

Default: yes

2.26 NTP

This menu contains the NTP settings.
Telnet path: Setup

2.26.2 Server-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

2.26.3 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

2.26.4 BC interval

Here you set the time interval in seconds 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 numeric characters

Default: 64

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).

Note: 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
Possible values:

- Max. 10 characters

Default: 86400

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

Here, you can specify timeservers (NTP) which can be reached via your device's interfaces. Separate the individual server names or IP addresses with semicolons.
Note: If required, the device will establish a connection to the time server. This can generate 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 addresses are to 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.
• 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.
- 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.

2.26.12 RQ-Tries

Here you can enter how many times a synchronization with the time server should be executed. A zero has the effect that a synchronization is tried so many times until a valid result has been received.
Telnet path: Setup/NTP
Possible values:

- max. 10 numeric characters

Default: 4

2.27 Mail

This menu contains the e-mail settings.
Telnet path: Setup

2.27.1 SMTP-Server

Enter the name or IP address for the SMTP server. This entry is required if the device is to notify you of certain events via e-mail.
Telnet path: Setup/Mail
Possible values:

- max. 31 characters

Default: blank
The e-mail notification may establish additional connections and therefore may generate additional charges.

2.27.2 SMTP-Port

Enter the SMTP port number of the aforementioned server for unencrypted mail The default value is 25.
Telnet path: Setup/Mail
Possible values:

- max. 10 characters

Default: 25

2.27.3 POP3-Server

Enter the number of the POP3 port on the aforementioned server for unencrypted mail.
Telnet path: Setup/Mail
Possible values:

- max. 31 characters

Default: blank

2.27.4 POP3-Port

The only difference between the POP3 server name for many POP3 servers requiring a "SMTP after POP" login and the SMTP server name is its prefix. In these cases, enter the name of the SMTP server and replace the 'SMTP' with 'POP' or 'POP3´.
Telnet path: Setup/Mail
Possible values:

- max. 10 characters

Default: 110

2.27.5 User-Name

Enter the user-name that the above mentioned SMTP server should use when sending e-mail notifications.
Telnet path: Setup/Mail
Possible values:

- max. 63 alpha numeric characters

Default: blank

2.27.6 Password

Enter the password that the above mentioned SMTP server should use when sending e-mail notifications.
Telnet path: Setup/Mail
Possible values:

- max. 31 alpha numeric characters

Default: blank

2.27.7 E-Mail-Sender

Enter a valid e-mail address to be used by the device as addressor when sending e-mails. This address is used by the SMTP servers involved to provide information on 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 it is in any way invalid.
Telnet path: Setup/Mail
Possible values:

- max. 63 characters

Default: blank

2.27.8 Send-Again-(min.)

In case of connection problems with the SMTP server, mails will be buffered and repeated tries will be made to submit. This will have an affect on mails which cannot be delivered due to incorrect settings such as SMTP parameters or unknown recipients.
You can set up the time after which an attempt will be made to re-submit buffered messages - In addition, any new mail received will also trigger an attempt to re-submit.
Telnet path: Setup/Mail
Possible values:

- max. 10 numeric characters

Default: 30

2.27.9 Hold-Time-(hrs.)

In case of connection problems with the SMTP server, mails will be buffered and repeated tries will be made to submit. This will have an affect on mails which cannot be delivered due to incorrect settings such as SMTP parameters or unknown recipients.
You can set up the timeout in hours, once this time has elapsed, all attempts to submit a certain message will be discontinued.
Telnet path: Setup/Mail
Possible values:

- max. 10 numeric characters

Default: 72

2.27.10 Buffers

In case of connection problems with the SMTP server, mails will be buffered and repeated tries will be made to submit. This will have an affect on mails which cannot be delivered due to incorrect settings such as SMTP parameters or unknown recipients.
You can set up the maximum number of mails buffered - 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

2.27.11 Loopback-Addr.

An optional source address can be configured here. This address is used instead of the source address, which is otherwise obtained automatically for the respective destination address. Whether loopback addresses are configured, they can be used as source address here.
Telnet path: Setup/Mail
Possible values:

- Name of the IP interface, the address of which is to 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 IP address can be entered in the form x.x.x.x.

Default: blank
Note: If there is an interface named "DMZ", then its address is used.

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

Specify a unique name for every RADIUS server in this table. The name 'DEFAULT' is reserved for all WLAN networks that use authentication via IEEE 802.1x and have no own RADIUS server specified. Each WLAN network that uses authentication via IEEE 802.1x can use its own RADIUS server by entering the specified name in place of 'Key 1/passphrase'.
Telnet path: Setup/ IEEE802.1x /RADIUS-Server
Possible values:

- max. 16 alpha numeric characters

Default: blank

2.30.3.2 IP-Address

IP address of the RADIUS server.
Telnet path: Setup/ IEEE802.1x /RADIUS-Server
Possible values:

- Valid IP address.

Default: 0.0.0.0

2.30.3.3 Port

Port of the RADIUS server.
Telnet path: Setup/ IEEE802.1x /RADIUS-Server
Possible values:

- max. 10 characters

Default: 0

2.30.3.4 Secret

Access key (shared secret) of 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.
Telnet path: Setup/ IEEE802.1x /RADIUS-Server
Possible values:

- max. 24 characters

Default: blank

2.30.3.6 Loopback-Addr.

An optional source address can be configured here. This address is used instead of the source address, which is otherwise obtained automatically for the respective destination address. Whether loopback addresses are configured, they can be used as source address here.
Telnet path: Setup/ IEEE802.1x /RADIUS-Server
Possible values:

- An address can be entered in various formats:
- Name of the IP interface, the address of which is to 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 IP address can be entered in the form x.x.x.x.

Default: blank
Note: If there is an interface named "DMZ", then its address is used.

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 registration settings separately for each local network.
Telnet path: Setup/ IEEE802.1x

2.30.4.2 Port

Port of the device, which is effected by this entry.
Telnet path: Setup/ IEEE802.1x /Ports
Possible values:

- All of the interfaces available in the device.

Default: blank

2.30.4.4 Re-Auth-Max

This is a timer from the Authentication State Machine in IEEE 802.1x.
Telnet path: Setup/ IEEE802.1x /Ports
Possible values:

- 0 to 255 seconds

Default: 3
Note: Changing this parameter requires in-depth knowledge of the IEEE 802.1x standard. Change this parameter only if it is demanded categorically by the system configuration.

2.30.4.5 Max-Req

This is a timer from the Authentication State Machine in IEEE 802.1x.
Telnet path: Setup/ IEEE802.1x /Ports
Possible values:

- 0 to 255 seconds

Default: 3
Note: Changing this parameter requires in-depth knowledge of the IEEE 802.1x standard. Change this parameter only if it is demanded categorically by the system configuration.

2.30.4.6 Tx-Period

This is a timer from the Authentication State Machine in IEEE 802.1x.
Telnet path: Setup/ IEEE802.1x /Ports
Possible values:

- 0 to 65553 seconds

Default: 30
Note: Changing this parameter requires in-depth knowledge of the IEEE 802.1x standard. Change this parameter only if it is demanded categorically by the system configuration.

2.30.4.7 Supp-Timeout

This is a timer from the Authentication State Machine in IEEE 802.1x.
Telnet path: Setup/ IEEE802.1x /Ports
Possible values:

- 0 to 65553 seconds

Default: 30
Note: Changing this parameter requires in-depth knowledge of the IEEE 802.1x standard. Change this parameter only if it is demanded categorically by the system configuration.

2.30.4.8 Server-Timeout

This is a timer from the Authentication State Machine in IEEE 802.1x.
Telnet path: Setup/ IEEE802.1x /Ports
Possible values:

- 0 to 65553 seconds

Default: 30
Note: Changing this parameter requires in-depth knowledge of the IEEE 802.1x standard. Change this parameter only if it is demanded categorically by the system configuration.

2.30.4.9 Quiet-Period

This is a timer from the Authentication State Machine in IEEE 802.1x.
Telnet path: Setup/ IEEE802.1x /Ports
Possible values:

- 0 to 65553 seconds

Default: 60
Note: Changing this parameter requires in-depth knowledge of the IEEE 802.1x standard. Change this parameter only if it is demanded categorically by the system configuration.

2.30.4.10 Re-Authentication

This option activates re-authentication at regular intervals. If re-authentication is started, the user remains authorized during negotiation.
Telnet path: Setup/ IEEE802.1x /Ports
Possible values:

- Yes
- No

Default: No

2.30.4.11 Re-Auth-Interval

If re-authentication is started, the user remains authorized during negotiation. A typical value for the re-authentication interval is 3,600 seconds.
Telnet path: Setup/ IEEE802.1x /Ports
Possible values:

- 0 to 65553 seconds

Default: 3600

2.30.4.12 Key-Transmission

You can activate regular creation and transmission of dynamic WE P keys here.
Telnet path: Setup/ IEEE802.1x /Ports
Possible values:

- Yes
- No

Default: No

2.30.4.13 Key-Tx-Interval

A typical default value for the key change interval is 900 seconds.
Telnet path: Setup/ IEEE802.1x /Ports
Possible values:

- max. 10 characters

Default: 900

2.31 PPPoE

This menu contains the PPPoE settings.
Telnet path: Setup

2.31.1 Operating

This button switches the PPPoE server on or off.
Telnet path: Setup/PPPoE-Server
Possible values:

- Yes
- No

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

You can specify a specific peer name for each remote site.
Telnet path: Setup/PPPoE-Server/Name-List
Possible values:

- Selection from the list of the defined peers.

Default: blank

2.31.2.2 SH-Time

The user's shorthold time in seconds is set after the logon.
Telnet path: Setup/PPPoE-Server/Name-List
Possible values:

- max. 4 characters

Default: 0

2.31.2.3 MAC-Address

If you specify a MAC address, the negotiation is terminated if the client logs an from a different MAC address.
Telnet path: Setup/PPPoE-Server/Name-List
Possible values:

- max. 12 characters

Default: 000000000000

2.31.3 Service

The name of the service offered is entered under 'Service'. his 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.

2.31.5 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

2.32.1 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: Max.4 characters

2.32.1.4 Ports

This list contains the device's 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
Note: The first SSID of the first WLAN module is called WLAN-1, the other SSIDs are named WLAN-1-2 to WLAN-1-8. If the device is equipped with two WLAN modules, the SSIDs are correspondingly named WLAN-2, WLAN-2-2 to WLAN-2-8.

2.32.1.5 LLDP-Tx-TLV-PPID

This parameter defines, which member ports are used to propagate the ID of VLAN defined in this entry.
Telnet path: Setup/VLAN/Networks/LLDP-Tx-TLV-PPID
Possible values:

- 251 alphanumeric characters (e.g. LAN-1, WLAN-1)

Default: blank

2.32.1.6 LLDP-Tx-TLV-Name

This parameter defines, which member ports are used to propagate the name of VLAN defined in this entry.
Telnet path: Setup/VLAN/Networks/LLDP-Tx-TLV-Name
Possible values:

- 251 alphanumeric characters (e.g. LAN-1, WLAN-1)

Default: blank

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; 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 to 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.

- **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.
- **Unconditional:** 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:** Incoming packets may or may not have a VLAN tag, outgoing packets never receive a VLAN tag.

Telnet path: Setup/VLAN/Port table
Default: Ingress mixed

2.32.2.7 Tx-LLDP-TLV-Port-VLAN

Activates or deactivates the port as LLDP-TLV-Port in this VLAN.
Telnet path: Setup/VLAN/Port-Table/Tx-LLDP-TLV-Port-VLAN
Possible values:

- Yes
- No

Default: Yes

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
Incorrect 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
Default: 8100

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

Note: 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

Note: 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

Note: 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:

- No
- Yes

Default: No

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 Protokoll

Protocol used for measuring.
Telnet path: Setup/ECHO-Server/Access-Table
Possible values:

- None
- TCP
- UDP
- TCP+UDP

Default: None

2.35.2.4 Aktive

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

2.35.3 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

2.36 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 measurements.
Telnet path: Setup/Performance-Monitoring

2.36.3.1 Protocol

Protocol to be used.
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.

2.36.3.3 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

2.36.3.17 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

2.36.3.255 Index

Shared index for the measurement.
Telnet path: Setup/Performance-Monitoring/RttMonEchoAdmin

2.36.4 RttMonStatistics

This table displays performance monitoring statistics.
Telnet path: Setup/Performance-Monitoring

2.36.4.2 Completions

Number of measurements performed.
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

2.36.4.8 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

2.36.4.10 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

2.36.4.22 Jitter-Min-Neg-SD

Minimum negative jitter value from sender to responder in uSec.
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

2.36.4.28 Jitter-Min-Neg-DS

Minimum negative jitter value from responder to sender in uSec.
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

2.36.4.62 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

2.36.4.255 Index

Shared index for the measurement.
Telnet path: Setup/Performance-Monitoring/RttMonStatistics

2.37 WLAN management

This menu is used to configure WLAN management for WLAN controllers.

2.37.1 AP configuration

This menu contains the settings for the access point configuration.
Telnet path: /Setup/WLAN-Management
Default: Blank

2.37.1.1 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 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 rexample, 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.

2.37.1.1.4 Operating

Switches the logical WLAN on or off separately.
Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles
Possible values:

- On
- Off

Default: On

2.37.1.1.6 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)

Note: 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

2.37.1.1.8 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.

Note: All other WLAN network parameters correspond to those for the standard configuration of access points.

Caution: 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.

Danger: 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

Note: 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

Note: Client-bridge mode can only be used between two devices which support this feature.

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

2.37.1.1.21 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

2.37.1.1.22 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

Note: 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

Note: 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 µs (default) to 0.4 µs (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

2.37.1.1.27 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

2.37.1.1.28 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

Note: 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

Note: 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

Caution: 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.

Caution: 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

2.37.1.2 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

2.37.1.2.2 Parent name

A 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 rexample, 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)

Note: 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

Note: 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.

2.37.1.2.10 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 access point 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 access point searches the active band for currently unused frequencies to find available access points. This value is the time interval between search cycles.
Devices 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, devices 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

Note: 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.

2.37.1.2.16 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

2.37.1.2.17 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

2.37.1.2.20 Report-seen-clients

Use this option to enhance WLAN performance where large numbers of WLAN clients (e.g. mobile handsets) will communicate in the WLAN.
If this option is enabled, the information from the probe requests are accessible in the WLAN controller in /status/wlan-management/seen-clients.
If this option is disabled, managed access points will not send any information from WLAN probe requests to the WLAN controller.
Telnet path: /Setup/WLAN management/AP-Configuration/Radioprofiles
Possible values:

- Yes
- No

Default: Yes

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

Note: From this list, assess 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 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: FFFFFFFFFFFF: 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

2.37.1.4.4 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.

2.37.1.4.8 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.

2.37.1.4.9 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

Note: In the 2.4-GHz band, two separate wireless networks must be at least three channels apart to avoid interference.

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

Note: In the 2.4-GHz band, two separate wireless networks must be at least three channels apart to avoid interference.

2.37.1 Operating

Activates or deactivates this entry.
Telnet path: /Setup/WLAN-Management/AP-Configuration/Access-Points
Possible values:

- Yes
- No

Default: Yes

2.37.1.4.12 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

Note: 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

Note: Cannot be configured with LANconfig

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

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.

2.37.1.4.17 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

Note: 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

Note: Cannot be configured with LANconfig

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

Note: 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'.

2.37.1.4.20 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

Note: 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

Note: 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 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

Note: 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'.

2.37.1.5 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

2.37.1.7 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)

2.37.1.9 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 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 rexample, 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

2.37.1.10 Predef. intranets

This table lists the predefined AP intranets.
Telnet path: /Setup/WLAN-Management/AP-Configuration/Predef.-Intranets

Note: 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

Note: 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.

2.37.1.12 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.

Note: 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

Note: 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.

2.37.5 CAPWAP port

Port number for the CAPWAP service
Telnet path: /Setup/WLAN-Management
Possible values:

- 0 to 65535

Default: 1027

Note: Cannot be configured with LANconfig

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

Note: 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

2.37.8 Provide default configuration

This enables the WLAN controller to assign a default configuration to every new (i.e. those without a valid certificate) even 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

Note: 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.

2.37.9 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

2.37.10 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

2.37.10.2 Syslog

Activates notification by SYSLOG.
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

Note: An SMTP account must be set up to make use of e-mail messaging.

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

2.37.10.5 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

2.37.17 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

Note: 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

Note: 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

Note: 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

Note: Cannot be configured with LANconfig

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

2.37.20 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

Note: 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

Note: 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

Note: 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

Note: 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

2.37.27 Central firmware management

This menu contains the configuration of central firmware management.
Telnet path: /Setup/WLAN-Management

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

2.37.27.12 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

2.37.27.13 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

Note: Do command

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

2.37.27.15 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

2.37.27.18 Reboot updated APs

Reboot updated APs.
Telnet path: /Setup/WLAN-Management/Central-Firmware-Management
Possible values:

- Syntax: Do Reboot-updated-APs

Note: Do command

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

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

2.37.27.26 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

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

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

2.37.31 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

2.37.32 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

Note: This value is for your information only. You cannot change it.

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

Note: This value is for your information only. You cannot change it.

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

2.37.34.2 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

2.37.34.3 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

Note: 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

Note: 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
- LB0 to LBF for the 16 loopback addresses
- Any valid IP address

Default: 0.0.0.0

Note: 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.

2.37.34.4 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

Note: 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.

2.38 LLDP

This submenu holds all configuration options related to the Link Layer Discovery Protocol (LLDP) defined by IEEE STD 802.1AB-2005. The options closely follow the configuration options defined by the LLDP MIB, so consult the IEEE standard if the explanations given here seem insufficient.
Telnet path: Setup/LLDP

2.38.1 Message-Tx-Interval

This value controls the interval in which LLDP Protocol Data Units (PDUs) are transmitted.
Telnet path: Setup/LLDP/Message-Tx-Interval
Possible values:

- 0 to 65535 seconds

Default: 30

2.38.2 Message-Tx-Hold-Multiplier

This value controls the TTL (time to live) conveyed in transmitted LLDP Protocol Data Units (PDUs). The TTL is the product of the message transmit interval and the transmit hold multiplier.
Telnet path: Setup/LLDP/Message-Tx-Hold-Multiplier
Possible values:

- 0 to 99

Default: 4

2.38.3 Reinit-Delay

This value defines the time the transmission of LLDP Protocol Data Units (PDUs) remains blocked, even if it is enabled again.
Telnet path: Setup/LLDP/Reinit-Delay
Possible values:

- 0 to 99 seconds.

Default: 2

2.38.4 Tx-Delay

This value limits the rate at which LLDP Protocol Data Units (PDUs) are transmitted, even if the associated data changes faster. The value defines the minimum time period (given in seconds) between transmissions.
Telnet path: Setup/LLDP/Tx-Delay
Possible values:

- 0 to 9999 seconds.

Default: 2

2.38.5 Notification-Interval

This value limits the rate at which notifications about remote table changes are transmitted. The value defines the minimum time period between notifications.
Telnet path: Setup/LLDP/Notification-Interval
Possible values:

- 0 to 9999 seconds

Default: 5

2.38.6 Ports

This table contains all port-related LLDP configuration options. Note that the table index is a string, namely the interface/port name.
Telnet path: Setup/LLDP/Ports

2.38.6.1 Name

The name of the port resp. interface.
Telnet path: Setup/LLDP/Ports/Name
Possible values:

- Depending on available interfaces, e.g. LAN-1, WLAN-1.

2.38.6.2 Admin-Status

Defines whether PDU transmission and/or reception on this port shall be enabled or not. Transmission and reception can individually be enabled or disabled.
Telnet path: Setup/LLDP/Ports/Admin-Status
Possible values:

- Disabled
- Tx-Only
- Rx-Only
- Rx/Tx

Default: Disabled

2.38.6.3 Notifications

Defines whether changes in remote MSAPs associated with this port shall result in a notification to possible network management systems.
Telnet path: Setup/LLDP/Ports/Notifications
Possible values:

- No
- Yes

Default: No

2.38.6.4 TLVs

This setting defines the set of optional standard TLVs that shall be transmitted in PDUs.
Telnet path: Setup/LLDP/Ports/TLVs
Possible values:

- Port-Description
- Sys-Name
- Sys-Descriptor
- Sys-Caps
- None

Default: Port-Description

2.38.6.6 TLVs-802.3

This setting defines the set of optional standard TLVs-802.3 that shall be transmitted in PDUs.
Telnet path: Setup/LLDP/Ports/TLVs-802.3
Possible values:

- PHY-Config-Status
- Power-via-MDI
- Link-Aggregation
- Max-Frame-Size
- None

Default: PHY-Config-Status

2.38.6.7 Max-Neighbours

This parameter defines the maximum count of LLDP neighbours.
Telnet path: Setup/LLDP/Ports/Max-Neighbours
Possible values:

- 0 to 65535

Default: 0

2.38.6.8 Update-Source

This parameter defines the possible sources for LLDP updates.
Telnet path: Setup/LLDP/Ports/Update-Source
Possible values:

- Auto
- LLDP-Only
- Other-Only
- Both

Default: Auto

2.38.6.9 TLVs-LCS

This setting defines the set of optional standard TLVs-LCS that shall be transmitted in PDUs.
Telnet path: Setup/LLDP/Ports/TLVs-LCS
Possible values:

- SSID
- Radio-Channel
- PHY-Type
- None

Default: SSID

2.38.6.10 TLVs-PNO

This setting defines the set of optional standard TLVs that shall be transmitted in PROFIBUS International (PNO) extension for PROFINET discovery information.
Telnet path: Setup/LLDP/Ports/TLVs-PNO
Possible values:

- SPD
- Port-Status
- Alias
- MRP

Default:SPD, Port-Status and Alias enabled

2.38.7 Management-Addresses

This table allows to define which management addresses shall be transmitted in PDUs. Management addresses are referenced by their names defined in the TCP/IP network list. A network resp.management address not listed in this table will never be transmitted in PDUs. If a network is listed in this table, the port list may be used to further limit the advertisement of the respective device address.
Telnet path: /Setup/LLDP/Management-Addresses

Note: Independent of the port list setting, advertisement of management addresses is implicitly limited by the address binding definitions made in the TCP/IP module. If a certain IP network is not bound to an interface, it will not be advertised regardless of the port list setting.

2.38.7.1 Network-Name

The name of the TCP/IP network, as defined in the TCP/IP network list.
Telnet path: Setup/LLDP/Management-Addresses/Network-Name
Possible values:

- max. 16 alphanumerical characters

Default: blank

2.38.7.2 Port-List

The list of interfaces resp. ports on which the corresponding management address may be advertised.
Telnet path: Setup/LLDP/Management-Addresses/Port-List
Possible values:

- Comma separated list of port, max. 251 alphanumerical characters, e.g. LAN-1 or WLAN-1. Wildcards allowed to define a range of ports, e.g. "*-*"

Default: blank

2.38.8 Protocols

This table contains the LLDP port settings for the protocols Spanning Tree and Rapid Spanning Tree.
Telnet path: Setup/LLDP/Protocols

2.38.8.1 Protocol

This parameter defines the protocol, for which the LLDP ports should be activated.
Telnet path: Setup/LLDP/Protocols/Protocol
Possible values:

- Spanning-Tree
- Rapid-Spanning-Tree

Default: Spanning-Tree, Rapid-Spanning-Tree

2.38.8.2 Port-List

This values defines the ports which are used for LLDP with the corresponding protocol (Spanning-Tree or Rapid-Spanning-Tree).
Telnet path: /Setup/LLDP/Protocols/Port-List
Possible values:

- Comma separated list of ports, max. 251 alphanumerical characters, e.g. LAN-1 or WLAN-1. Wildcards allowed to define a range of ports, e.g. "*-*"

Default: blank

2.38.9 Immediate-Delete

This parameter enables or disables the immediate deletion of LLDP Protocol Data Units (PDUs).

Telnet path: Setup/LLDP/Immediate-Delete

Possible values:

- No
- Yes

Default: No

2.38.10 Operating

This parameter enables or disables the use of LLDP.

Telnet path: Setup/LLDP/Operating

Possible values:

- No
- Yes

Default: No

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 SCEP-Operating

Switches SCEP on or off.

Telnet path: Setup/Certificates/SCEP-Client

Possible values:

- Yes
- No

Default: No

Special values: No

2.39.1.2 CA certificate update before

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

2.39.1.3 CA-Certificate-Update-Before

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

2.39.1.7 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 alpha numeric 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 alpha numeric 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 alpha numeric characters

Default: blank

2.39.1.7.4 ChallengePwd

Password (for the automatic issue of device certificates on the SCEP server).
Telnet path: Setup/Certificates/SCEP-Client/Certificates
Possible values:

- max. 251 alpha numeric 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 KeyUsage

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 greater
- 0 (no key in use)

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-KeyUsage

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

2.39.1.8 Reinit

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 device's file system so 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

2.39.1.9 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

2.39.1.10 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

2.39.1.11 Retry-After-Error-Interval

Interval in seconds between retries after detected errors of any type.
Telnet path: Setup/Certificates/SCEP-Client
Possible values:

- max. 10 characters

Default: 22

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

2.39.1.13 Trace level

Telnet path: Setup/Certificates/SCEP client/Trace level
Description
Possible values:

- All
- Reduced
- Only-errors

Default: All

2.39.1.14 CAs

Telnet path: Setup/Certificates/SCEP client/CAs
Name: Configuration name of the CA.
URL: URL of the CA.
DN: Distinguished name of the device. With this parameter the CAs are assigned to system certificates on the one hand
(and vice versa). On the other hand this parameter is also important for evaluating whether received
or available certificates match with the configuration.
Enc-Alg: This algorithm encrypts the payload of the certificate request.

- Possible values: DES, 3-DES, Blowfish.
- Default: DES.

Identifier: CA identifier (as required by some web server to identify the CA).
RA autoapprove: Some CAs provide the option of using an earlier certificate issued by this CA as proof of authenticity for future requests. This option defines whether an existing system certificate should be used to sign new requests.

- Possible values: Yes, No.
- Default: No.

CA signature algorithm: The certificate request is signed with this algorithm.

- Possible values: MD5, SHA1.
- Default: MD5.

CA fingerprint algorithm: Algorithm for signing the fingerprint. This determines whether the CA certificate is to be checked by means of fingerprint, and which algorithm is used for this. The CA fingerprint has to agree with the checksum which results when this algorithm is applied.

- Possible values: Off, MD5, SHA1.
- Default: Off.

CA fingerprint: The authenticity of a received CA certificate can be checked by means of the checksum (fingerprint)
entered here (corresponding to the set CA fingerprint algorithm).
Use: Indicates the intended application of the specified CA. The CA entered here is only queried for the corresponding application.

- Possible values: VPN, WLAN controller, general

- Special values: General If a general CA is available then no other CA can be configured,

otherwise the choice of CA unclear.

2.39.1.14.1 Name

A freely definable name can be entered here to identify this configuration.
Telnet path: Setup/Certificates/SCEP client/Certificates/Name
Possible values:

- max. 16 alpha numeric 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. An example: http:/ /postman/certsrv/mscep/mscep.dll
Telnet path: Setup/Certificates/SCEP client/Certificates/URL
Possible values:

- max. 251 alpha numeric 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=myCompany CA/O=My Company/C=DE
Telnet path: Setup/Certificates/SCEP client/Certificates/DN
Possible values:

- max. 251 alpha numeric characters

Default: Blank

2.39.1.14.4 Enc. alg.

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:

- **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:**

Telnet path: Setup/Certificates/SCEP client/Certificates/Enc alg
Possible values:

- des
- 3des
- blowfish
- aes128

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 help 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 alpha numeric characters

Default: Blank

2.39.1.14.6 CA 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 cryptographical hash functions are relatively widespread:
MD5 (default) - Message Digest Algorithm 5 generates a 128-bit hash value.
SHA1 - Secure Hash Algorithm 1 generates a 160-bit hash value.
Telnet path: Setup/Certificates/SCEP client/Certificates/CA signature algorithm
Possible values:

- sha
- md5

Default: Off

2.39.1.14.7 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 client/Certificates/RA autoapprove
Possible values:

- Yes
- No

Default: No

2.39.1.14.8 CA 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.
Two cryptographical hash functions are relatively widespread:
MD5 (default) - Message Digest Algorithm 5 generates a 128-bit hash value.
SHA1 - Secure Hash Algorithm 1 generates a 160-bit hash value.
Telnet path: Setup/Certificates/SCEP client/Certificates/CA fingerprint algorithm
Possible values:

- Off
- sha
- md5

Default: Off

2.39.1.14.9 CA fingerprint

The CA fingerprint can be entered here. This is a hash value that is produced by the fingerprint algorithm. This hash value can be used to check the authenticity of the received CA certificate (if a CA fingerprint algorithm is a requirement). Possible delimiters are: ' :' ' -' ' ,' ' '
Telnet path: Setup/Certificates/SCEP client/Certificates/CA fingerprint
Possible values:

- max. 59 alpha numeric characters

Default: Blank

2.39.1.14.11 Loopback addr.

Enter a loopback address.
Telnet path: Setup/Certificates/SCEP client/Certificates/Loopback addr.
Possible values: Max. 16 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

2.39.2.2 CA certificates

This menu contains the settings for CA certificates.
Telnet path: /Setup/Certificates/SCEP-Client/CAs

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=Hirschmann CA/O=Hirschmann/C=DE
Telnet path: /Setup/Certificates/SCEP-CA/CA certificates/CA-Distinguished-Name
Possible values:

- Max. 251 characters

Default: Blank

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

2.39.2.2.4 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

Note: The time taken for calculation depends on the performance available from the system; the greater the number of bits, the longer it takes.

2.39.2.2.5 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

2.39.2.2.6 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

2.39.2.2.8 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=Hirschmann CA/O=Hirschmann/C=DE
Telnet path: /Setup/Certificates/SCEP-CA/CA-certificates/RA-Distinguished-Name
Possible values:

- Max. 251 characters

Default: Blank

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 PCKS12 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

2.39.2.2.11 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

2.39.2.3 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

2.39.2.4 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

2.39.2.5 Client certificates

This menu contains the settings for client certificates.
Telnet path: /Setup/Certificates/SCEP-Client/Certificates

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=Hirschmann CA/O=Hirschmann/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

2.39.2.5.4 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

2.39.2.6 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 mes-

sages 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

2.39.2.7 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

2.39.2.8 Certificate revocation lists

This item contains the certificate revocation lists.
Telnet path: /Setup/Certificates/SCEP-CA/Certificate-Revocation-Lists

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

2.39.2.8.2 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

2.39.2.9 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

2.39.2.10 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

2.39.2.10.2 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

Note: To make use of this function, the Syslog client in the device needs to be configured accordingly.

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

2.39.3 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

Note: 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.

2.39.3.4 Update-Before

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 help 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

Note: If the CRL does not load on the first attempt, new attempts are made at regular short intervals.

2.39.3.5 Prefetch period

The time period after which periodic attempts are made to retrieve a new CRL. This is 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

Note: If with regular updates the CRL cannot be retrieved, no further attempts will be started until the next regular attempt.

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 help 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.

Note: Within the time period defined here, even certificates in the CRL which have expired can still be used to maintain or establish a connection.

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

2.39.3.8 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 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

2.39.3.9 Loopback address

Here you can optionally configure a sender address to be used instead of the one used automatically for this destination address.
Telnet path: Setup/Certificates/CRLs/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.
- 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.

2.51 HiDiscovery

This menu contains the values for the HiDiscovery protocol configuration.
Telnet path: Setup

2.51.1 Server-Operating

This parameter enables or disables the use of the HiDiscovery protocol.
Telnet path: Setup/HiDiscovery
Possible values:

- Disabled
- Read-Only
- Enabled

Default: Disabled

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 device 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/Operational
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 number of the port on the serial interface that is to be used for the COM-port server.
Telnet path: Setup/COM-Ports/COM-Port-Server/Operational
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/Operational
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.
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: Setup/COM-Ports/COM-Port-Server/COM-Port-Settings
Possible values:

- All available serial interfaces.

Default: Outband

2.52.2.2.2 Port-Number

Some serial devices such as the CardBus have more than one serial port. Enter the number of the port on the serial interface that is to be used for the COM-port server.
Telnet path: 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: Setup/COM-Ports/COM-Port-Server/COM-Port-Settings
Possible values:

- 110
- 300
- 600
- 1200
- 2400
- 4800
- 9600
- 19200
- 38400
- 57600
- 115200
- 125000
- 230400

Default: 9600

2.52.2.2.5 Data-Bits

Number of data bits.
Telnet path: 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: 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: 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: 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 a 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". Moreover, the transition from the "ready" to the "not ready" states is used to establish and cancel TCP connections in client mode. There are two ways of determining whether the port is ready or not. 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: Setup/COM ports/COM-port server/COM-port settings
Possible values:

- DTR
- Data

Default: DTR

2.52.2.2.10 Ready-Data-Timeout

The timeout switches the port back to the not-ready status if not 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: 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.

2.52.2.3 Network settings

This table contains all settings that define the behavior of the COM port in the network.
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

2.52.2.3.2 Port-Number

Some serial devices such as the CardBus have more than one serial port. Enter the number of the port on the serial interface that is to be used for the COM-port server.
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 device 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-Hostname

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-Addr.

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 device 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 required. Unexpected characters may be displayed at the remote site. A side effect of using the FRC2217 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

2.52.2.3.10 Newline conversion

Telnet path: Setup/COM ports/COM-port server/Network settings/Newline conversion
Description
Possible values:

- CRLF
- CR
- LF

Default: CRLF

2.52.2.3.12 TCP retransmit timeout

Telnet path: Setup/COM ports/COM-port server/Network settings/TCP retransmit timeout
Description
Possible values:

- Numeric characters from 0 to 99

Default: 0

2.52.2.3.13 TCP retry count

Telnet path: Setup/COM ports/COM-port server/Network settings/TCP retry count
Description
Possible values:

- Numeric characters from 0 to 9

Default: 0

2.52.2.3.14 TCP keepalive

Telnet path: Setup/COM ports/COM-port server/Network settings/TCP keepalive
Description
Possible values:

- Inactive
- Active
- Proactive

Default: Inactive

2.52.2.3.15 TCP keepalive interval

Telnet path: Setup/COM ports/COM-port server/Network settings/TCP keepalive interval
Description
Possible values:

- Numeric characters from 0 to 4289999999

Default: 0

2.52.2.3.16 Binary-Mode

The COM port server supports RFC 2217 extensions for COM port parameter settings, which in turn build on top of the Telnet option negotiation. The COM port server will also try to negotiate binary mode transmission with its peer. Using binary mode for data transfer eliminates certain character translations regarding the Telnet newline special character (ASCII sequence CR/LF). However, enabling binary mode also means that the user cannot configure anymore what the newline character will be translated to on the serial port side, and has to accept with what the Telnet client delivers as newline sequence when the user presses the 'Enter' key.
Path Telnet: Setup/COM-Ports/COM-Port-Server/Network-Settings
Possible values:

- Auto: the COM port server will assume non-binary mode and try to negotiate it with the peer via Telnet options.
- Yes: the COM port server will assume binary mode and not try to negotiate it with the peer via Telnet options.
- No: the COM port server will assume non-binary mode and not try to negotiate it with the peer via Telnet options. This a variant not possible with the old setting.

Default: Auto

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

2.52.4 Serial configuration

This menu contains the settings for the auto configuration of WLAN point-to-point links over a serial connection.
Telnet path: /Setup/COM-Ports

2.52.4.1 Bit rate

This item sets the bit rate for communications between the devices when a serial connection is used for the automatic configuration of WLAN point-to-point links.
Telnet path: /Setup/COM-Ports
Possible values:

- 1200
- 2400
- 4800
- 9600
- 19200
- 38400
- 57600
- 115200

Default: 9600

Note: It is imperative that the same bit rate is set in all devices communicating over serial connections to be used for the automatic configuration of WLAN point-to-point links.

2.53 Temperature monitor

Telnet path: Setup/Temperatur monitor
Description

2.53.1 Upper-limit degrees

Telnet path: Setup/Temperatur monitor/Upper-limit degrees
Description
Possible values:

- Numeric characters from 0 to 127

Default: 70

2.53.2 Lower-limit degrees

Telnet path: Setup/Temperature monitor/Lower-limit degrees
Description
Possible values:

- Numeric characters from 0 to 127

Default: 0

2.54 Tacacs+

Telnet path: Setup/TACACS+

2.54.1 Authentication

Activates authentication via TACACS+ server. If TACACS+ authentication is activated, all authentication data is transmitted via TACACS+ protocol to the configured TACACS+ server.
Telnet path: Setup/TACACS+
Possible values: Activated, deactivated
Default: Deactivated

Note: 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 device. The fallback to local users must be deactivated for devices without a root password. Otherwise, a user cannot access a password if the network connection is lost (TACACS+ server available).

2.54.2 Authorization

Activates authorization via TACACS+ server. If TACACS+ authorization is activated, all authorization data is transmitted via TACACS+ protocol to the configured TACACS+ server.
Telnet path: Setup/TACACS+
Possible values:

- Activated
- Deactivated

Default: Deactivated

Note: 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.

2.54.3 Accounting

Activates accounting via TACACS+ server. If TACACS+ accounting is activated, all accounting data is transmitted via TACACS+ protocol to the configured TACACS+ server.
Telnet path: Setup/TACACS+
Possible values: Activated, deactivated
Default: Deactivated

Note: TACACS+ accounting will only activate if the defined TACACS+ server is available.

2.54.6 Shared secret

The password for encrypting the communications between NAS and TACACS+ servers.
Telnet path: Setup/TACACS+
Possible values: 31 alphanumerical characters
Default: Blank

Note: The password must be entered identically into the device and the TACACS+ server. We recommend that you do not operate TACACS+ without encryption.

2.54.7 Encryption

Activates or deactivates the encryption of communications between NAS and TACACS+ servers.
Telnet path: Setup/TACACS+
Possible values:

- Activated
- Deactivated

Default: Activated

Note: 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.

2.54.9 Server

Telnet path: Setup/TACACS+

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.

Server address

Address of the TACACS+ server to which requests for authentication, authorization and accounting are to be forwarded.

Possible values: Valid DNS resolvable name or valid IP address.

Default: Blank

Loopback address

Optionally you can configure a loopback address here.

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

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.

Possible values: Activated, deactivated

Default: Deactivated

2.54.9.1 Server address

Telnet path: Setup/TACACS+/Encryption/Server address

Description

2.54.9.2 Loopback address

Telnet path: Setup/TACACS+/Encryption/Loopback address

Description

2.54.9.3 Compatibility mode

Telnet path: Setup/TACACS+/Encryption/Compatibility mode
Description
Possible values:

- Deactivated
- Activated

Default: Deactivated

2.54.10 Fallback to local users

Should the defined TACACS+ server be unavailable, it is possible to fallback to local user accounts on the device. This allows for access to the device even if the TACACS+ connection is unavailable, e.g. when deactivating the usage of TACACS+ or for correcting the configuration.
Telnet path: Setup/TACACS+
Possible values:

- Allowed
- Prohibited

Default: Allowed

Note: The fallback to local user accounts presents a potential security risk if no root password is set for the device. 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.

2.54.11 SNMP-GET requests authorization

This parameter allows the regulation of the behavior of 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.

Telnet path: Setup/TACACS+

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

2.54.12 SNMP-GET requests accounting

Numerous network management tools use SNMP for requesting information from network devices. LANmonitor also uses SNMP to access the 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 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.

Telnet path: Setup/TACACS+

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

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.

2.54.13 Bypass-TACACS-for-CRON/Scripts/Action table

This option allows a bypassing of TACACS+ for cron jobs, scripts and actions from the action table. This is helpful if you run a script on the ip configuration, for example.
Path WEBconfig: SE Menu Tree/Setup/TACACS+/
Possible values:

- deactivated
- activated

Default: deactivated

Note: This setting has influence on the TACACS+ settings for the whole system. Restrict the use of cron-jobs, the action-table and scripts to a small group of admins.

2.54.14 Include value into authorization request

If you deactivate this function, TACACS+ only checks the rights of the user at the login. Afterwards the user is able to change values without being checked if he got the permission to change them.
Telnet path: Setup/Tacacs+/Include value into authorization request
Possible values:

- activated: TACACS+ checks the user's permission to change values, if he tries to change them.
- deactivated: TACACS+ only checks the identity of the user at the login

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 us 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

Note: 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 us 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

Note: This option is set to "inactive" in the Security Settings Wizard or the Basic Settings Wizard.

Note: 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 deactivated the reset switch.

2.59 WLAN management

This menu is used to configure the WLAN management.

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 addr.

This is where you can configure an optional sender address for use instead of that 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.
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 called "DMZ", its address will be taken in this case.

- LB0 ... LBF for the 16 loopback addresses.
- Furthermore, any IP address can be entered in the form x.x.x.x.

Note: The sender address specified here is used **unmasked** for every remote station.

2.59.120 Log entries

No description is available for this parameter yet.
Telnet path: Setup/WLAN management/Log entries
Default: 200

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

Note: 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.

Note: 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 firm-

ware 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

Caution: 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

Note: 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

Note: 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

2.60.1.2.2 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

Note: The TFTP or HTTP(S) client loads the file entered here only if the LoadConfig 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.

2.60.1.3 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

2.60.1.3.2 URL

Specify the URL of the script that is to be uploaded over the network using the LoadScript command.
Telnet path: /Setup/Autoload/Script/URL
Possible values:

- Max. 127 characters beginning with "tftp://", "http://" or "https://"

Default: Blank

Note: The TFTP or HTTP(S) client loads the file entered here only if the LoadScript 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.

2.60.1.4 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 theses 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

Note: 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

us 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

Note: 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 us 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

Note: This option is set to "inactive" in the Security Settings Wizard or the Basic Settings Wizard.

Note: 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 deactivated the reset switch.

2.61 Profinet

This menu is used to set up the Profinet settings.
Telnet path: /Setup

Note: This function is available on those devices only, where the manufacturer has activated Profinet in the delivery status.

2.61.1 Admin-State

This option enables or disables the Admin-State for Profinet in the device. Enable the Admin-State to integrate the device into an Profinet structure. If the Admin-State is disabled, the device cannot be seen in a Profinet structure.
Telnet path: /Setup/Profinet
Possible values:

- Disabled
- Enabled

Default: Disabled

Note: This function is available on those devices only, where the manufacturer has activated Profinet in the delivery status.

2.61.2 Device-Name

Enter the name of the device which will be used in the Profinet structure. This name has to match the name as entered in the PLC for this device.
Telnet path: /Setup/Profinet
Possible values:

- Maximum 255 alphanumerical characters

Default: empty

Note: This function is available on those devices only, where the manufacturer has activated Profinet in the delivery status.

2.62 EtherNetIP

This menu is used to set up the Ethernet/IP settings.
Telnet path: /Setup

Note: This function is available on those devices only, where the manufacturer has activated Ethernet/IP in the delivery status.

2.62.1 Operating

This option enables or disables Ethernet/IP on this device.
Telnet path: /Setup/EtherNetIP
Possible values:

- Yes
- No

Default: No

Note: This function is available on those devices only, where the manufacturer has activated Ethernet/IP in the delivery status.

3 Firmware

This menu contains the actions and settings options for managing the device firmware.
Telnet path: Firmware

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 Ifc

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/Firmsafe table

3.2.1 Position

Position in memory space of the current entry.
Telnet path: Firmware/Firmsafe table/Position

3.2.2 Status

Status of the current entry.
Telnet path: Firmware/Firmsafe table/Status
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.

Default: active

3.2.3 Version

Version descriptor of the firmware for the current entry.
Telnet path: Firmware/Firmsafe table/Version

3.2.4 Date

Release date of the firmware for the current entry.
Telnet path: Firmware/Firmsafe table/Date

3.2.5 Size

Size of the firmware for the current entry.
Telnet path: Firmware/Firmsafe table/Size

3.2.6 Index

Index for the current entry.
Telnet path: Firmware/Firmsafe table/Index

3.3 Firmsafe mode

Telnet path: Firmware/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:

  1. The new firmware is uploaded successfully and it then becomes active as desired. Everything is OK.

  2. After uploading the firmware the device no longer responds. If the upload is unsuccessful, the device will automatically activate the previous firmware and will restart.

- Login: If the first attempt to upload is unsuccessful, there is a second option to upload and immediately activate the firmware.

  1. 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.

  2. 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.

3.4 Firmsafe timeout

The time in seconds for testing new firmware.
Telnet path: Firmware/Firmsafe timeout
Possible values:

- 0 to 99999 seconds.

Default: 300 seconds

3.7 Feature word

Displays the feature bits that provide information on the options activated in the device.
Telnet path: Firmware/Firmsafe word

4 Other

This menu contains additional functions from the LCOS menu tree.
Telnet path: Other

4.1 Manual dialing

This menu contains the actions for manual connection establishment.
Telnet path: Other/Manual dialing

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

4.1.2 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

4.2 System boot

This action is used to manually reboot the device.
Telnet path: Other/Manual dialing/System boot

4.5 Cold boot

This action is used to reboot the device.
Telnet path: Other/Cold boot