



Addendum LCOS 8.60

LCOS
[LANCOM OPERATING SYSTEM]

LANCOM
Systems

Contents

1 Addendum to LCOS version 8.60.....	3
1.1 LCOS.....	3
1.1.1 View contents of all subdirectories.....	3
1.1.2 Configurable action for alive test.....	7
1.1.3 Output filter for command-line entries.....	10
1.1.4 Line-by-line display of table entries.....	11
1.1.5 Support for TLS 1.1 / 1.2.....	11
1.1.6 LCOSCAP: Wireshark-compatible data capture at the CLI.....	12
1.2 LCMS.....	14
1.2.1 Exporting CSV data sets.....	14
1.2.2 Importing from a data source.....	16
1.2.3 Flexible group configuration with LANconfig.....	23
1.2.4 Better overview in LANconfig with more columns.....	30
1.2.5 Checking the system-time source in the customized Rollout Wizard.....	32
1.3 WLAN.....	35
1.3.1 WLAN RF optimization.....	35
1.3.2 Group key per VLAN.....	37
1.3.3 How the 40-MHz mode works.....	39
1.3.4 Point-to-point partners.....	40
1.3.5 Adjustable rate adaption algorithm.....	41
1.4 Public Spot.....	42
1.4.1 Using hidden fields on the login form in Public Spot page templates.....	42
1.4.2 Public Spot user administration.....	42
1.4.3 Advanced redirection URL.....	48
1.4.4 Variable station table.....	49
1.5 VPN.....	49
1.5.1 Improved phase 1 rekeying.....	49
1.5.2 MPPE encryption for PPTP tunnels.....	50
1.6 SIP ALG: Proxy for bypassing NAT in the router.....	50
1.6.1 SIP ALG: Basics.....	50
1.6.2 SIP ALG: Features.....	51
1.6.3 SIP ALG: Configuration.....	51
1.6.4 Additions to the Setup menu.....	52
1.6.5 Additions to the Status menu.....	53
1.7 Voice over IP – VoIP.....	57
1.7.1 Restricting or preventing SIP registration over WAN connections.....	57
1.7.2 Additions to the Setup menu.....	58
1.7.3 Additions to the Status menu.....	59

1 Addendum to LCOS version 8.60

The addendum describes the changes and additions to LCOS version 8.60 over the previous version.

1.1 LCOS

1.1.1 View contents of all subdirectories

The parameter `-r` causes the shell commands `dir`, `ls`, `list` and `ll` to display all subdirectories and the tables in them.

```
admin@:/
> dir -r status/ppp
```

PPP-Phases	TABINFO: 2 x [Ifc,Phase,LCP,IPCP,CCP,IPV6CP]
LCP	MENU:
PAP	MENU:
CHAP	MENU:
IPCP	MENU:
CCP	MENU:
Rx-Options	MENU:
Tx-Options	MENU:
Delete-Values	ACTION:
IPV6CP	MENU:

```
[rek] PPP-Phases:
```

Ifc	Phase	to	LCP	IPCP	CCP
IPV6CP					
DSL-CH-1	DEAD		Initial	Initial	Initial
Initial					
EXT	DEAD		Initial	Initial	Initial
Initial					

```
[rek] LCP:
```

Rx-Errors	INFO:	0
Rx-Discarded	INFO:	0
Rx-Config-Request	INFO:	0
Rx-Config-Ack.	INFO:	0
Rx-Config-Nak.	INFO:	0
Rx-Config-Reject	INFO:	0
Rx-Terminate-Request	INFO:	0
Rx-Terminate-Ack.	INFO:	0
Rx-Code-Reject	INFO:	0
Rx-Protocol-Reject	INFO:	0
Rx-Echo-Request	INFO:	0
Rx-Echo-Reply	INFO:	0
Rx-Discard-Request	INFO:	0
Tx-Config-Request	INFO:	0
Tx-Config-Ack.	INFO:	0
Tx-Config-Nak.	INFO:	0

```

Tx-Config-Reject      INFO:      0
Tx-Terminate-Request  INFO:      0
Tx-Terminate-Ack.     INFO:      0
Tx-Code-Reject        INFO:      0
Tx-Protocol-Reject    INFO:      0
Tx-Echo-Request       INFO:      0
Tx-Echo-Reply         INFO:      0
Tx-Discard-Request    INFO:      0
Delete-Values         ACTION:

[rek] PAP:

Rx-Discarded          INFO:      0
Rx-Request            INFO:      0
Rx-Success            INFO:      0
Rx-Failure            INFO:      0
Tx-Retry              INFO:      0
Tx-Request            INFO:      0
Tx-Success            INFO:      0
Tx-Failure            INFO:      0
Delete-Values         ACTION:

[rek] CHAP:

Rx-Discarded          INFO:      0
Rx-Challenge          INFO:      0
Rx-Response           INFO:      0
Rx-Success            INFO:      0
Rx-Failure            INFO:      0
Tx-Retry              INFO:      0
Tx-Challenge          INFO:      0
Tx-Response           INFO:      0
Tx-Success            INFO:      0
Tx-Failure            INFO:      0
Delete-Values         ACTION:

[rek] IPCP:

Rx-Discarded          INFO:      0
Rx-Config-Request     INFO:      0
Rx-Config-Ack.        INFO:      0
Rx-Config-Nak.        INFO:      0
Rx-Config-Reject      INFO:      0
Rx-Terminate-Request  INFO:      0
Rx-Terminate-Ack.     INFO:      0
Rx-Code-Reject        INFO:      0
Tx-Config-Request     INFO:      0
Tx-Config-Ack.        INFO:      0
Tx-Config-Nak.        INFO:      0
Tx-Config-Reject      INFO:      0
Tx-Terminate-Request  INFO:      0
Tx-Terminate-Ack.     INFO:      0
Tx-Code-Reject        INFO:      0

MORE [Q(uit)]>

```

Command-line commands

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



Supervisor rights are necessary to execute some commands.

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

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

Command	Description
writeflash	Load a new firmware file (only via TFTP)
!!	Repeat last command
!<num>	Repeat command <num> times
!<prefix>	Repeat last command beginning with <prefix>
#<blank>	Comment

■ **PATH:**

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

■ **VALUE:**

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

■ **NAME:**

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

- All commands and directory/parameter names can be entered using their short-forms as long as they are unambiguous. For example, command "sysinfo" can be shortened to "sys" and "cd Management" to "c ma". Input "cd /s" is not valid, however, since it corresponds to both "cd /Setup" and "cd /Status".
- Names that contain spaces must be enclosed within quotation marks ("").
- A command-specific help function is available for actions and commands (call the function with a question mark as the parameter). For example, 'ping ?' shows the options of the integrated ping command.
- Enter '?' on the command line for a complete listing of the console commands available.

1.1.2 Configurable action for alive test

Until now, the alive test only allowed for a cold or warm start in the event of failure. In some cases it may be preferable to execute an action, e.g. to reset a WLAN module. This type of action can significantly reduce the interruption time compared to a cold or warm start.

Additions to the menu system

Alive test

This menu contains the settings for the alive test. The alive test sends a ping to a destination address at configurable intervals. If there is no response from the destination, the device performs a reboot or other action according to defined criteria.

To configure the alive test you have to define the target address, the action to be performed, the combination of pings and retries, and the threshold for triggering the defined action. The parameters required for this have the following default values:

- Fail limit: 10
- Test interval: 10
- Retry interval: 1
- Retry count: 1

These settings cause the device to transmit a ping every 10 seconds (test interval). If this ping is not answered, the device repeats the ping after 1 second (retry interval) and exactly one time (retry count). If this ping also goes unanswered, the device considers the series to have failed. If 10 series in a row fail (fail limit) then the device triggers the defined action, in this case after 10 x 10 seconds = 100 seconds.

SNMP ID: 2.7.21

Telnet path: Setup/TCP-IP

Action

Enter the action to be performed by the device if the target address is unreachable. You can use the same actions as used in the cron table, i.e. executing CLI commands, HTTP requests, or sending messages.



The action set here will only be executed if the boot type is set to the value **Action**. The boot type is configured under /Setup/TCP-IP/Alive-test/Boot-type (also see [Boot type](#)).

SNMP ID: 2.7.21.7

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

Possible values:

- 251 characters

Default: Blank

Boot type

The device executes this action if the ping to the target address was unsuccessful.

SNMP ID: 2.7.21.6

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

Possible values:

- Cold boot: The device performs a cold boot.
- Warm boot: The device performs a warm boot.
- Action: The device performs a configurable action. Configure the action under /Setup/TCP-IP/Alive-Test (also see [Action](#)).

Default: Warm boot

Fail limit

This parameter defines the number of consecutive failed test series before the device is rebooted or the configured action is executed.



The product of the error limit and test interval defines the overall duration until rebooting or executing the action.

SNMP ID: 2.7.21.5

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


Possible values:

- 0 to 4294967295

Default: 10

Test interval

The time interval in seconds, in which the device sends a ping to the target address. If the ping is unanswered, the device optionally repeats a set number of pings in the defined interval. With this configuration, the device forms a "series" of ping attempts. Only when all pings go unanswered is the complete series evaluated as unsuccessful.


 The product of the error limit and test interval defines the overall duration until rebooting or executing the action.

SNMP ID: 2.7.21.2

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

Possible values:

- 0 to 4294967295 seconds

 Select the test interval as a time which is greater than the product of the retry interval and retry count, so that the desired number of retries can be performed within the test interval.

Default: 10

Retry interval


If a ping goes unanswered, this value defines the time interval before the device repeats the ping to the target address.

SNMP ID: 2.7.21.4

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

Possible values:

- 0 to 4294967295

 Set the retry interval to a number such that the product of retry interval and retry count is less than the test interval. This ensures that the desired number of retries can be performed within the test interval.

Default: 1

Special values: With a retry interval of 0 the device sends no repeat pings.

Retry count


If a ping goes unanswered, this value defines the number of times that the device will repeat the ping to the target address.

SNMP ID: 2.7.21.3

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

Possible values:

- 0 to 4294967295

 Set the retry count to a number such that the product of retry interval and retry count is less than the test interval. This ensures that the desired number of retries can be performed within the test interval.

Default: 1

Special values: With a retry count of 0 the device sends no repeat pings.

Target address

The target address to which the device sends a ping.

SNMP ID: 2.7.21.1

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

Possible values:

- Valid IP address.

1.1.3 Output filter for command-line entries

The command-line commands `show`, `dir` and `ls` generates large amounts of output. The filters allow you to sift out the information that is important for you from all the information.

To enable the filters, extend the commands to include the parameter "@", which initiates the following filter definition. The following operators apply to filter definitions:

Operator	Description
(space)	OR operator: The filter applies when one of the parameters occurs in the output
+	AND operator: The filter applies when the operand occurs in the output
-	NOT operator: The filter applies when the operand does not occur in the output
"	The output must exactly match the search filter

Any string combination can be used to specify the operands, such as the names of remote stations, protocols or ports. The filter then processes these data according to the rule of the operators used, in a similar way to Internet search engines.

❗ The filter enhances the preceding command one time only. If you invoke the command again without specifying a filter, the output appears unfiltered again.

❗ No filter is available for the following features:

- `show bootlog`
- `show ethswitch rmon`
- `show mem`
- `show random`
- `show ssh idkeys`
- `show tls fingerprints`
- `show tls heap`

The command `show vpn` displays all current VPN connections. The filter `show vpn @ "sales_ger"` reduces the display to the connections with a name containing the string "sales_ger" (i.e. sales representatives in Germany).

The command `ls /Setup/IP-Router/IP-Routing-Table` shows the parameters to be used for accessing configured networks or remote sites. The filter `ls /Setup/IP-Router/IP-Routing-Table @ -"192.168."` suppresses the display of stations in this private IP address range.

1.1.4 Line-by-line display of table entries

When working with the command line, displaying tables with several columns is often confusing because the standard line length is 80 characters. Useful for large tables, you can go directly to the any row by entering a row index when invoking the `cd` command. In this way, the commands `dir` and `ls` display the content of the line in a three-column table:

- **Left column:** Property
- **Middle column:** Type
- **Right column:** Value

❗ If the specified row does not exist an error message is displayed. If another working directory has been specified, then a column parameter is ignored.

In this three-column view, you can use the shell command `set <property> <value>` directly to write a new value into the corresponding field.

❗ The `set` command also processes complete paths. Enter the table entries that begin with the characters "..", "/" and "\" between quotes.

1. The command `cd Status/LAN/Interfaces` takes you to the overview of the LAN interfaces.
2. The `ls` command lists all the information about the interfaces in a table:

Ifc	Queue-Packets	Link-Active
LAN-1	0	Yes
LAN-2	0	No
LAN-3	0	No
LAN-4	0	No

3. With the command `cd lan-4` you move to the corresponding table row.
4. The `ls` command lists the content of this row only:

Ifc	INFO:	LAN-4
Queue-Packets	INFO:	0
Link-Active	INFO:	No

1.1.5 Support for TLS 1.1 / 1.2

The encryption protocol SSL or TLS ("Secure Sockets Layer" or "Transport Layer Security") supports secure data communication between two communication partners. For this purpose, SSL or TLS uses, for example, encryption, authentication and verification of certificates that have been sent. Although it is mainly used to secure HTTP connections (as "HTTPS" or "HTTP over SSL"), SLS or TLS serve as a basis for secure communications for many other transfer protocols.

LCOS uses the TLS protocol in the following modules:

- HTTP over SSL
- Telnet over SSL
- RADSEC
- CAPWAP/DTLS
- EAP-TLS/PEAP/TLS

The TLS encryption protocol has been under development since 1999 and up to the current version TLS 1.2. To use the enhanced functionality of clients and web browsers, LANCOM devices support the TLS protocol of the versions 1.0, 1.1 and 1.2 for secure data transmission.

In the LCOS versions prior to 8.60, the encryption protocols SSL 3.0 and TLS 1.0 were always enabled by default. As of LCOS version 8.60 you can also select between the TLS versions 1.1 or 1.2 for HTTPS connections.

Additions to the menu system

SSL versions

This setting allows you to opt for the latest encryption protocols for HTTPS connections.



Please note that the encryption protocols set here only apply for HTTPS connections. For other protocols, the available encryption algorithms are fixed:

- EAP/TLS/TTLS/PEAP is set to TLS 1.0
- CAPWAP is set to DTLS 1.0 (which is based on TLS 1.1)
- Telnet/SSL is set to 'SSL 3.0+TLS 1.0 + TLS 1.1 + TLS 1.2'
- RADSEC is set to 'SSL 3.0+TLS 1.0'

SNMP ID:

221.18

Telnet path:

Setup > HTTP > SSL-Versions

Possible values:

SSLv3

TLSv1

TLSv1.1

TLSv1.2

Default:

SSLv3

TLSv1

1.1.6 LCOSCAP: Wireshark-compatible data capture at the CLI

The analysis tool "Wireshark" analyzes data traffic over a network connection, and presents the results in graphical form. "Wireshark" can analyze an ongoing connection, or it can analyze connection data that was stored previously.

With "LCOSCAP" you have the option to record and store the data traffic in a format compatible with Wireshark. You operate LCOSCAP from the command line interface by appending the appropriate parameters.

The following parameters control LCOSCAP:

- `-o`: Target file that contains the recording.
- `-p`: Root password of the LANCOM device on which the traffic is recorded.
- `-i`: Interface of the LANCOM device whose data is recorded.



If you omit the `-i` parameter, LCOSCAP outputs the device's interface list.

- `-b`: Switch to include beacons in the data traffic (for WLAN only).

- `-h`: Switch which limits the recording to 802.11 headers. If you do not set this switch, the recording includes the full packet including 802.11 headers (for WLAN only).
- `-l`: Specifies the maximum size of the capture file. LCOSCAP creates a new file once the current file has reached the maximum size. The files are sequentially numbered.
- `-n`: Specifies the number of files generated by LCOSCAP. LCOSCAP overwrites the first file once the number of files has reached the maximum.

With `lcoscapy --h` you invoke LCOSCAP's Help function.

Enter the following command to record the data traffic for a device:

```
lcoscapy -i LAN-1 -p lancom -o d:\lancom.pcap 192.168.1.1
```

- The device in this example has the IP address "192.168.1.1".
- The password is "lancom".
- You are recording the data traffic on the interface "LAN-1".
- File name and location are "d:\lancom.pcap".

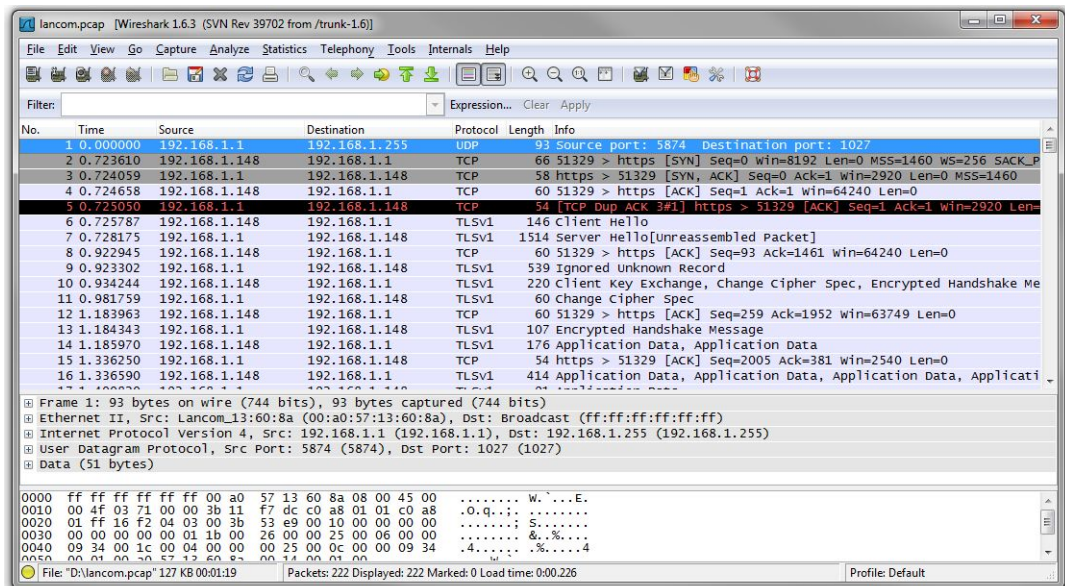
Use the keyboard shortcut "Ctrl + C" to stop the recording.

```
C:\Windows\system32\cmd.exe
D:\>lcoscapy --h
LCOSCAP V8.60 (C) 2011 LANCOM Systems, Germany
usage: lcoscapy [options] <ip address>

options:  -o <file>      : send output to <file> instead of stdout
          -b             : include beacons in trace
          -p <passwd>    : device password
          -i <ident>     : select probe (omit for probe list)
          -h             : only include 802.11 headers, omit payload
          -l <size>      : rotate capture files after <size> MBytes
          -n <count>     : # of files to keep when rotating capture files (default 10)

D:\>lcoscapy -i LAN-1 -p lancom -o d:\lancom.pcap 192.168.1.1
LCOSCAP V8.60 (C) 2011 LANCOM Systems, Germany
capture finished: received 223 packets, 130174 bytes
```

For the analysis, open the file generated by LCOSCAP with "Wireshark".



Additions to the menu system

Packet capture

This setting controls the use of the LCOSCAP function to record network traffic.

SNMP ID:

263

Telnet path:

Setup > Packet-Capture

LCOSCap operating

This setting activates the LCOSCAP function.

SNMP ID:

263.1

Telnet path:

Setup > Packet-Capture > LCOSCap-Operating

Possible values:

Yes

No

Default:

Yes

LCOSCap port

This setting specifies the port used by LCOSCAP.

SNMP ID:

263.2

Telnet path:

Setup > Packet-Capture > LCOSCap-Port

Possible values:

5 characters from '0123456789'

Default:

41.047

1.2 LCMS

1.2.1 Exporting CSV data sets

You can export the list of devices found on the network and later import them into LANconfig in one go. LANconfig stores the list of managed devices in a CSV file.

To export the data, proceed as follows:

1. Select the menu item **File > Export device list**.
2. Set the location to save the file.
3. Enter a file name.
4. Specify the column separator, which separates the various device parameters.
5. Start saving by clicking on **Save**.

6. A dialog confirms the number of data sets stored.
7. Close the dialog by clicking **OK**.

The CSV file that is generated contains the following data:

```
DEVICE_PATH;DEVICE_INTERFACE;DEVICE_ADDRESS;DEVICE_TIMEOUT;DEVICE_STARTUP;
DEVICE_PROTOCOLS;DEVICE_PORTS;DEVICE_ADMIN;DEVICE_PASSWORD;DEVICE_NAME;
DEVICE_DESCRIPTION;DEVICE_TYPE;DEVICE_SERNO;DEVICE_HWADDR;DEVICE_HWREL;
DEVICE_LOCATION;DEVICE_COMMENT;DEVICE_BACKUP;DEVICE_VPN
Group1;IP;192.168.2.35;10;1;263;;admin;Ht34bd5L;Etagel;L-54ag;LANCOM
L-54ag Wireless;008520600482;00a0570bc9bf;B;;;
Group1;IP;192.168.2.34;10;1;263;;admin;Ht34bd5L;Etag2;L-54ag;LANCOM
L-54ag Wireless;008520600843;00a05719a8fb;B;;;
```

The first row contains the name of the device parameters. Each row that follows contains the parameter values for one device. If 2 semicolons appear in direct succession, then the enclosed parameter value is blank.

The variable name in the first row correspond to the following LANconfig entries:

- **DEVICE_PATH**: Path name in the folder view
- **DEVICE_INTERFACE**: Connection type
- **DEVICE_ADDRESS**: IP address or domain name and COM port or telephone number respectively
- **DEVICE_TIMEOUT**: Maximum response time of the device
- **DEVICE_STARTUP**: Device check at startup
- **DEVICE_PROTOCOLS**: Communication protocols
- **DEVICE_PORTS**: Ports
- **DEVICE_ADMIN**: Administrator name
- **DEVICE_PASSWORD**: Administrator password
- **DEVICE_NAME**: Device name
- **DEVICE_DESCRIPTION**: Description
- **DEVICE_TYPE**: Device type
- **DEVICE_SERNO**: Serial number
- **DEVICE_HWADDR**: MAC address
- **DEVICE_HWREL**: Hardware release
- **DEVICE_LOCATION**: Location
- **DEVICE_COMMENT**: Comment
- **DEVICE_BACKUP**: Storage location for the configuration backup created by LANconfig
- **DEVICE_VPN**: Parameter set for 1-Click-VPN



Use a text editor or spreadsheet to manage the list of exported devices.



If a device password is stored in LANconfig, the password is saved in plain text in the CSV file. Remember to delete these access credentials before you pass this file on or save it to a freely accessible server.

Additions to the menu system

File


The menu item 'File' is used to manage devices in general and to exit LANconfig.

Export device list

You can export the list of devices found on the network and later import them into LANconfig in one go. LANconfig stores the list of managed devices as a CSV file.

1.2.2 Importing from a data source

In LANconfig you can import a large number of devices from a script file in one go by processing the device files with an Import Wizard. You also have the option of using this device file together with a configuration template file to create a custom configuration file for each device. The template file contains variables for the values in the device file.

 The device file is saved in CSV format.

Additions to the menu system

File

The menu item 'File' is used to manage devices in general and to exit LANconfig.

Devices/configurations from CSV file...

In LANconfig you can import a large number of devices from a script file in one go by processing the device files with an Import Wizard. You also have the option of using this device file together with a configuration template file to create a custom configuration file for each device. The template file contains variables for the values in the device file.

Example application: Importing from a single data source

This scenario describes how to use a script file and a simple CSV-format device file to generate your own data source for importing data.

Content of the CSV file

The CSV file contains device-related data records, which LANconfig can import. This provides you with a convenient method of managing this data on the network.

The following is an example of a simple CSV file:

```
CONFIG_FILENAME;DEVICE_PATH;DEVICE_INTERFACE;DEVICE_ADDRESS;DEVICE_LOCATION;DEVICE_NAME;KEY;USER
Fil52146.lcs;Affiliate/NRW;IP;192.168.1.1;Wuerselen;Fil52146;secret1;user1@internet
Fil80637.lcs;Affiliate/BAY;IP;192.168.2.1;Muenchen;Fil80637;secret2;user2@internet
```

The header contains the names of the device parameters. The following lines itemizes the various devices line by line, and their parameters are separated by semicolons. If 2 semicolons appear in direct succession, then the enclosed parameter value is blank.

The parameter names on the first line can be freely defined. If you decide to use the standard LANCOM variable names, LANconfig automatically allocates the device parameters during the import.

- **DEVICE_PATH**: Path name in the folder view
- **DEVICE_INTERFACE**: Connection type
- **DEVICE_TIMEOUT**: Maximum response time of the device
- **DEVICE_STARTUP**: Device check at startup
- **DEVICE_PROTOCOLS**: Communication protocols
- **DEVICE_PORTS**: Ports
- **DEVICE_ADMIN**: Administrator name
- **DEVICE_PASSWORD**: Administrator password
- **DEVICE_NAME**: Device name
- **DEVICE_DESCRIPTION**: Description
- **DEVICE_BACKUP**: Storage location for the configuration backup created by LANconfig

- **DEVICE_VPN**: Parameter set for 1-Click-VPN

If you choose not to use the LANCOM default variable names, you may need to manually assign the values to the appropriate device properties in LANconfig during the import.

Content of the configuration template file

The template file contains Telnet commands that Telnet executes sequentially. This is why this template file is also referred to as a script file.



For an overview of the available Telnet commands see the Reference Manual chapter "Configuration with different tools" under "Telnet".

A configuration template file can appear as follows:

```
lang English
flash No
set /Setup/Name "$DEVICE_NAME$"
set /Setup/SNMP/Location "$DEVICE_LOCATION$"
cd /Setup/TCP-IP/Network-list
tab Network-name IP-Address IP-Netmask VLAN-ID Interface Src-check Type
  Rtg-tag Comment
add "INTRANET" $DEVICE_ADDRESS$ 255.255.255.0 0 any loose Intranet 0
"local intranet"
cd /
cd /Setup/WAN/PPP
tab Peer Authent.request Authent-response Key Time Try Conf Fail Term
  Username Rights
add "INTERNET" none PAP "$KEY$" 6 5 10 5 2 "$USER$" IP
cd /
cd /Setup/WAN/DSL-Broadband-Peers
del *
tab Peer SH-Time AC-name Servicename WAN-layer ATM-VPI ATM-VCI MAC-Type
  user-def.-MAC DSL-ifc(s) VLAN-ID
add "INTERNET" 9999 " " " " "PPPOEOA" 1 32 local 000000000000 " " 0
cd /
cd /Setup/IP-Router/IP-Routing-Table
tab IP-Address IP-Netmask Rtg-tag Peer-or-IP Distance Masquerade Active
  Comment
add 255.255.255.255 0.0.0.0 0 "INTERNET" 0 on Yes "default route"
cd /
flash Yes

# done
exit
```

The variables begin and end with a character or a string (here:'\$').

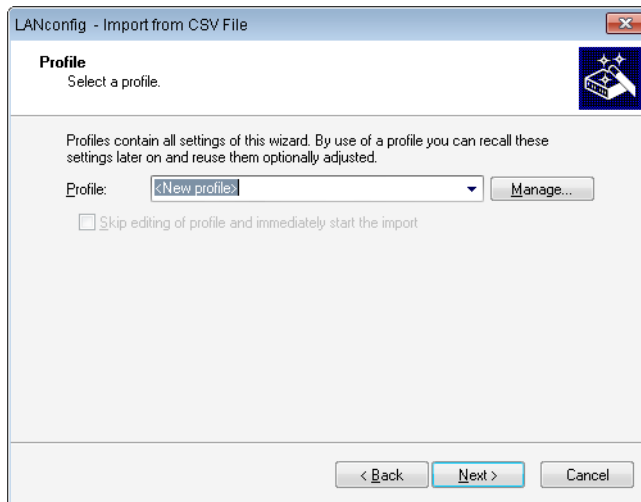
In this template file, the variables represent certain device parameters. During the import process, you associate these variables with the corresponding entries in the device file. The Configuration Wizard then replaces the variables with the associated device data from the CSV file.

Creating the configuration files

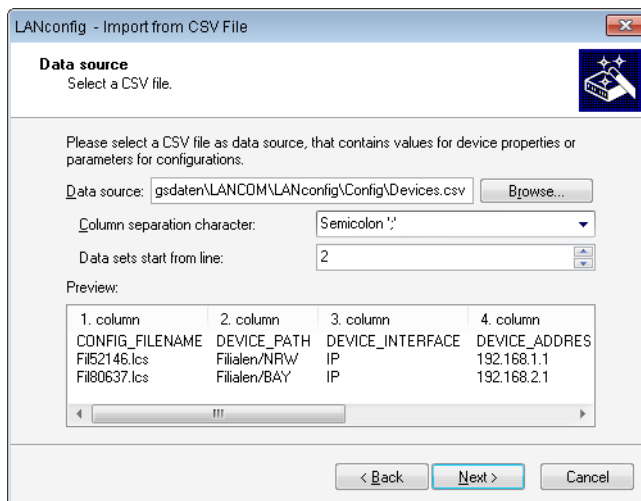
Proceed as follows to create device-specific configuration files:

1. Open the Import Wizard in the menu **File > Devices/Configurations from CSV file...**
2. If necessary, confirm the Welcome dialog with **Next**. The option to **Skip this page on next call** will suppress the appearance of the welcome screen when the Wizard is run in future.

3. If applicable, select the profile used for a previous data import. The option **Skip profile settings and start the import immediately** uses the settings in the selected profile without modification. Select **<New profile>** to use a new profile instead of an existing one. Click on **Next**.

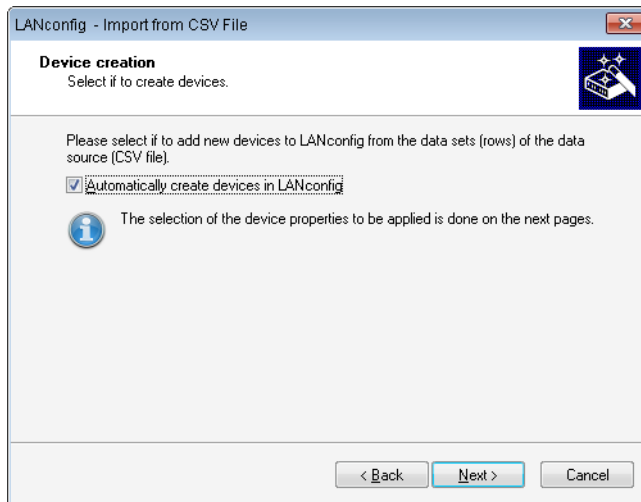


4. In the **Data source** field enter the path to the CSV file. With **Browse ...** you select the file from your local file system.



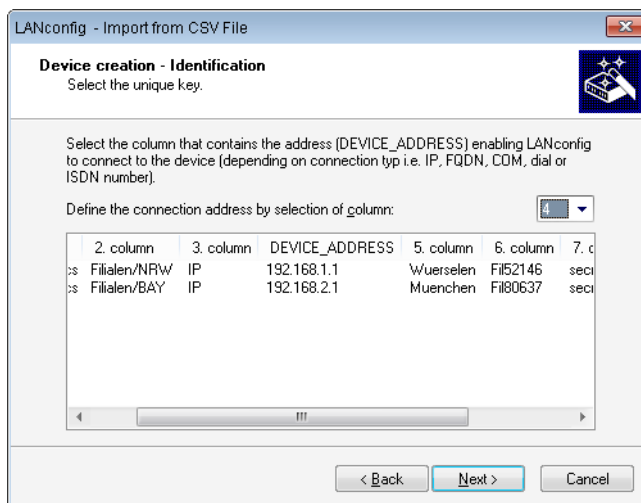
5. You can select the column delimiter in the CSV file. The default is the semicolon.
6. Set the row number where the data records start. This allows you to avoid importing any existing column headings and additional information. If a line in the CSV file contains only LANCOM default variable names (see section [Exporting CSV data sets](#)), then this line is used to assign the variables automatically. This ensures that exporting and importing the same file will function without any manual assignment. However, if a configuration is generated with additional variables, the auto-detect will not function.
7. The **Preview** field instantly shows the parameters you have selected for import. Confirm your entries with **Next**.

8. To use the data records to create new devices in LANconfig, select the option **Automatically create devices in LANconfig**. After clicking **Next**, the following pages are used to select the device properties to be carried over to LANconfig.

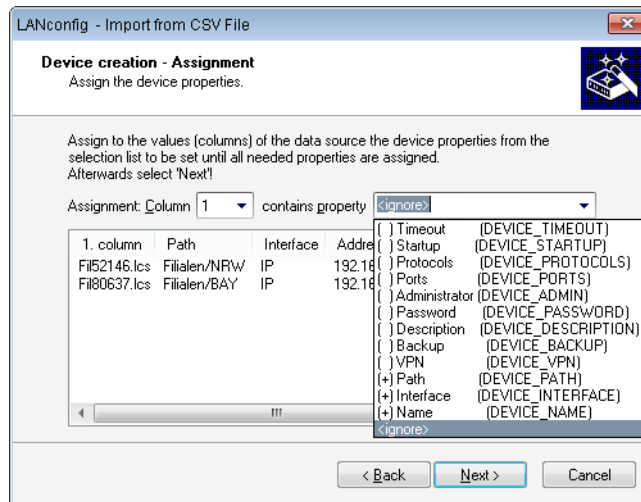


! If this option is disabled, the Wizard will skip the subsequent 2 steps.

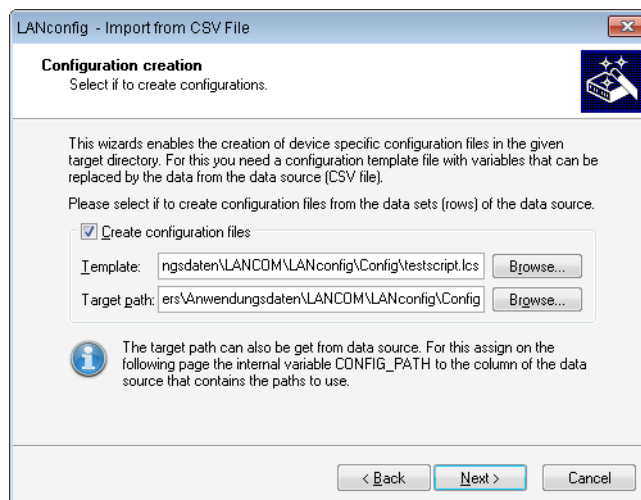
9. The devices are identified using their connection address. Use the drop-down list to select the column in the data set that contains the connection address and click on **Next**. If you use LANCOM default variable names, assignment takes place automatically.



10. Align the columns according to the relevant device properties. Properties that have been aligned are marked in the list with a preceding "+". Then click on **Next**. If you use LANCOM default variable names, assignment takes place automatically.

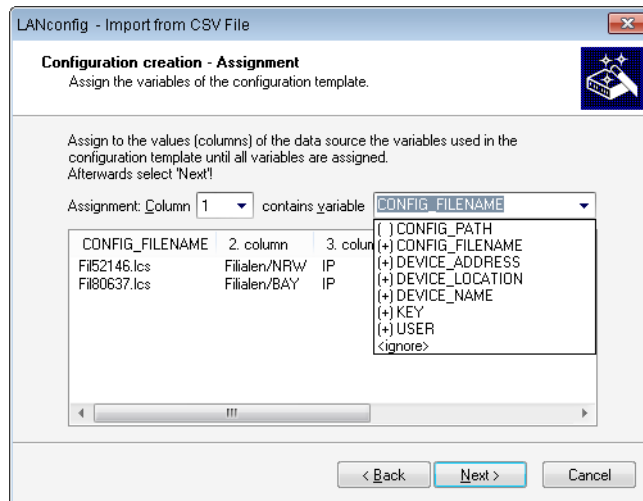


11. You have the option to create individual configuration files from the data sets. Simply activate the option **Generate configuration files**.



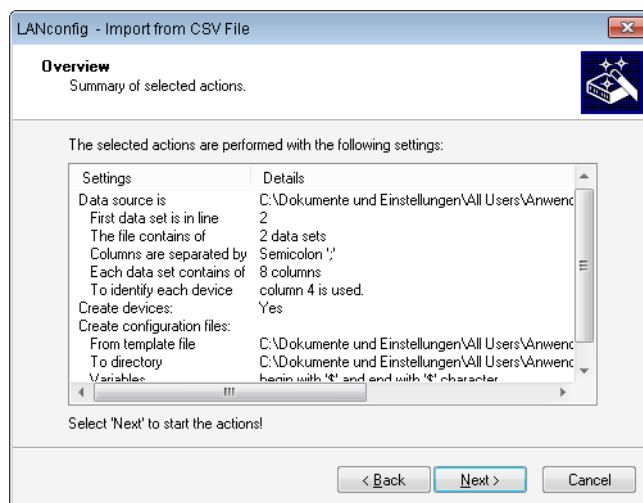
12. Use the **Template** field to set the path to the template file to be used as the basis for these configuration files. By clicking on **Browse** you open the dialog for loading a configuration script template. In the fields **Variable start** and **Variable end** you define which characters (or strings) are to mark the start and end of the variables in the template file. This enables the Wizard to identify the variables in the template file.
13. You determine the storage path in the field **Target path**. This is where LANconfig stores the new configuration files. Click on **Browse** to specify a target path on your local file system. Click on **Next**.
14. Assign the columns in the data source to the variables used in the template file. Do this by selecting the column number from the list of columns and assigning this number to a variable from the properties list. Variables are also assigned automatically if the column headings contain the same variable names as those between the start and end

characters in the script file. The column headings in the view below updates immediately with every change. To continue, click on **Next**.



! If your entries are incomplete, the Wizard alerts you about potential import problems and suggests corrections.

15. The summary informs you about the actions that are executed in the next step. If you need to make any changes, click on **Back**. This returns you to the appropriate input mask. By clicking on **Next** you start the data import.



! If the data import would overwrite a device that already exists in LANconfig, the Wizard gives you the following options:

- Overwrite the device.
- Create a configuration file anyway.
- Use this decision for all other existing devices.

16. The status dialog that follows indicates the actions performed. Click on **Copy to clipboard** to save the status message to the clipboard. Click on **Next**.
17. Finally, you have the option to save the current import settings to a profile for future actions.
18. Complete the import by clicking on **Finish**.

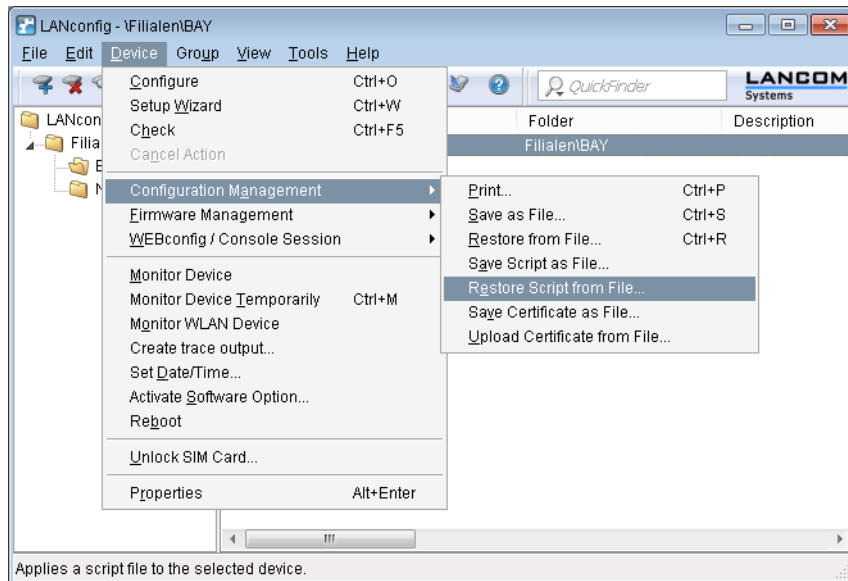
If you have opted to generate a custom configuration file, the Wizard saves a separate configuration file for each device in the specified folder. These configuration files are named according to the file name "<CONFIG_FILENAME>.lcs", which defines the CSV file:

```
lang English
flash No
set /Setup/Name "Fil52146"
set /Setup/SNMP/Location "Wuerselen"
cd /Setup/TCP-IP/Network-list
tab Network-name IP-Address IP-Netmask VLAN-ID Interface Src-check Type
  Rtg-tag Comment
add "INTRANET" 192.168.1.1 255.255.255.0 0 any loose Intranet 0 "local
intranet"
cd /
cd /Setup/WAN/PPP
tab Peer Authent.request Authent-response Key Time Try Conf Fail Term
  Username Rights
add "INTERNET" none PAP "secret1" 6 5 10 5 2 "user1@internet" IP
cd /
cd /Setup/WAN/DSL-Broadband-Peers
del *
tab Peer SH-Time AC-name Servicename WAN-layer ATM-VPI ATM-VC I MAC-Type
  user-def.-MAC DSL-ifc(s) VLAN-ID
add "INTERNET" 9999 "" "" "PPPOEOA" 1 32 local 000000000000 "" 0
cd /
cd /Setup/IP-Router/IP-Routing-Table
tab IP-Address IP-Netmask Rtg-tag Peer-or-IP Distance Masquerade Active
  Comment
add 255.255.255.255 0.0.0.0 0 "INTERNET" 0 on Yes "default route"
cd /
flash Yes

# done
exit
```

The Wizard has replaced all variables with the appropriate device parameters.

This configuration file gives you the option to use LANconfig to transfer the device settings as defined in the template file to other devices. Highlight the appropriate device and click on **Device > Configuration management > Restore script from script file**.



1.2.3 Flexible group configuration with LANconfig

! LCOS version 8.60 offers the full flexibility of the group configuration function.

Flexible group configuration helps you to manage multiple devices: You apply a carefully selected range of configuration parameters to a group of devices, in one go. This is far more convenient than manually setting the parameters in each individual device, e.g. identical SSID settings in WLAN access points. This helps you to avoid transferring complete configuration files from other devices, in which case device-specific parameters such as the IP address are also included. Group configuration with LANconfig enables the simultaneous setting of shared group-configuration parameters, thus facilitating the simultaneous administration of multiple devices.

By collecting multiple devices into a group configuration, these devices can be co-managed as a group. The group configuration files with the common parameters for a group of LANCOM devices are, just like the full configuration files, stored on hard disk or on a server. To aid the configuration of entire groups of devices, links to the group configuration files are created under LANconfig. These links provide a convenient connection between these group-configuration files and the device entries in LANconfig.

LANconfig provides general "group templates" as an aid to creating group configurations. You define which parameters are to be used for a group according to your individual needs. Use this feature to add additional configuration parameters to the group parameters, or to remove the suggested group parameters. You can store the configurations you created either as group configurations or as a customized template for the generation of further group configurations.

! Subsequently you can edit your own group configuration templates, but not the LANconfig basic templates.

The following templates for group configurations are available in LANconfig:

- **LANCOM Group Template WLAN:** Includes the parameters that are co-managed on wireless LAN devices.
- **LANCOM Group Template WLC:** Useful when operating LANCOM WLCs in a cluster, this template includes the full range of parameters that minimize the need for individual device configuration.
- **LANCOM Group Template empty:** Contains no pre-selected group parameters, and so serves as a basis for creating your own group templates which exceed the scope of the WLAN and WLC group templates. Here, the total amount

of all available configuration parameters in all device types is available for you to choose those which you want to use for your group configuration.

- **Alternative basic settings:** The LANCOM Group Templates give you the option of including the common parameters for different device types into the group template. However, some parameters overlap between different device types (e.g. DSL and DSLoL). Thus the group templates are always a compromise in which some parameters may be missing. For homogeneous groups containing just one type of device, a specific device configuration with a specific firmware version can be used as the "alternative basic settings" as a template for the group. These basic settings thus allow you to choose from precisely those configuration parameters that are required for this type of device.

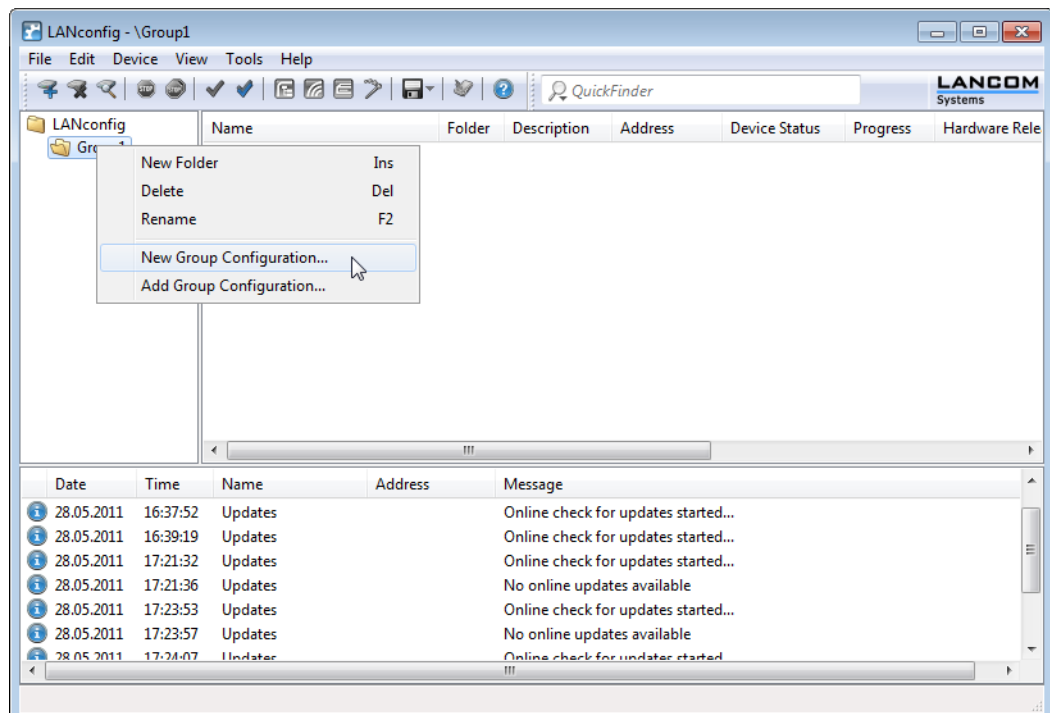
Creating a group configuration

To work with group configurations, the devices are collected into folders. These LANconfig folders contain entries for the devices that benefit from the co-management of shared group-configuration parameters and a link to the group configuration.

- ❗ A group configuration allows you to manage all device parameters that are shared by the devices in the group. An individual device configuration refers to the parameters that are device specific.

New group configuration file

1. Create a new folder for the devices to be grouped. You have two ways to create this folder:
 - Click the right mouse button on an existing folder in the folder view. Select **New folder with group configuration**. The configuration dialog initially creates a new folder as a sub-directory and then continues with the selection of the template to be used for creating a new group configuration.
 - In the folder view, click the right mouse button to the directory where you wish to create the new folder. Select the context dialog **New folder** and enter a name. Use the mouse to move the devices for grouping into the new folder. Then click on the folder with the right-hand mouse key and select the context-menu entry **New group configuration**.



2. Select a template and the appropriate firmware version and click on **OK**.

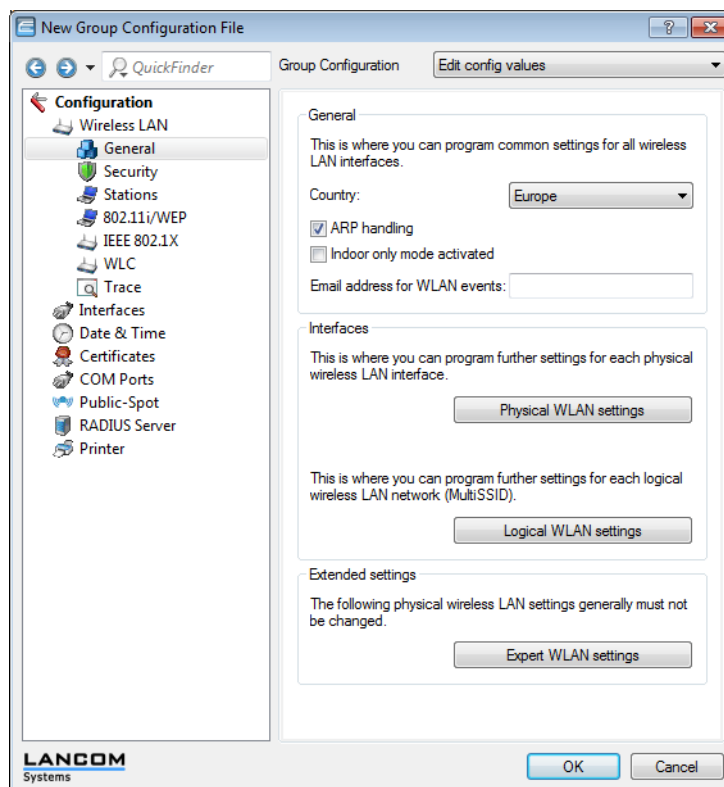
! If you have saved your own group templates previously, these will be also displayed in the list of templates.

3. You have the option of selecting the alternative basic settings if you wish to use a specific device type as the basis for the new group configuration. In this case, the new group configuration is created with the default values for the selected device type.

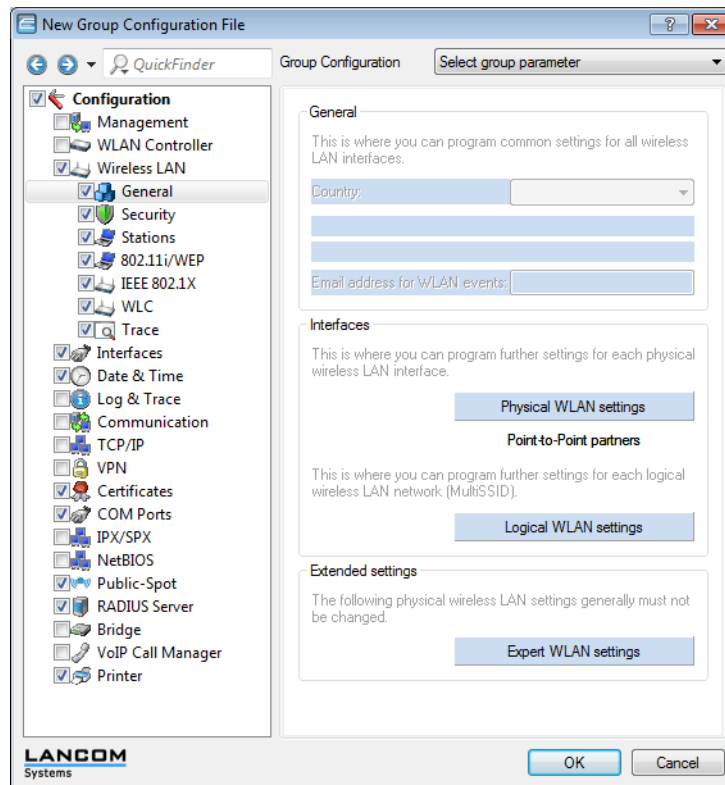
! In order to avoid inconsistent sets of configuration parameters, the alternative basic settings are based on a blank template corresponding to the "LANCOM Group Template Empty".

4. A configuration dialog opens. Two alternative processing modes are available here. Select this from the list **Group Configuration**:

- **Edit config. values** mode.
- **Select group parameters** mode.
- The configuration dialog opens in the **Edit config. values** mode. In this view, you see only the common parameters which are to be co-managed for the group. You can define the required values and content here. Parameters that apply to individual devices are hidden.



- In the **Select group parameters** mode you can select or de-select all of the parameters that you require for a customized group configuration.



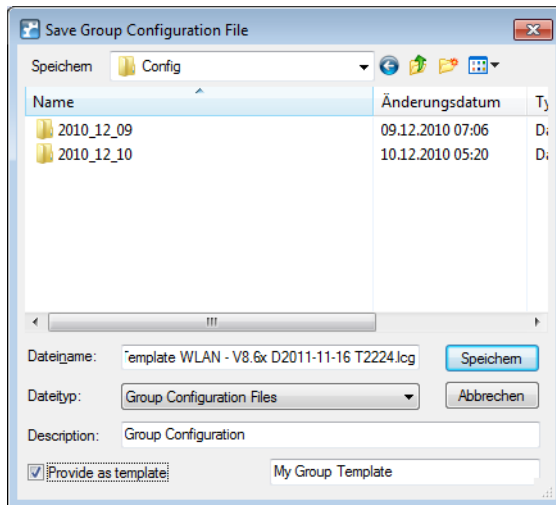
Light-blue colored items are selected for use in the group configuration. Click once with the left mouse button on an item to change its selection status.

Please note the following:

- For tables with statically specified rows (such as interface-related tables and logical WLAN settings) you additionally have the option of transferring individual parameters into the group configuration. You can access some of these parameters in LANconfig via the pull-down menus from buttons.
- For tables with dynamically generated rows (such as the routing table, for example) you can only select or de-select the entire table for the group configuration.
- Similarly, it is only possible to select or de-select the entire firewall for the group configuration.

5. Then click on **OK**.
6. Specify the storage path for the new group configuration. The default directory is the one you specified in **Tools > Options > Backup > Backup path** (default: "\\ config \")

7. As an option you can include this group configuration into the list of templates for creating further group configurations in future. Enable the option **Provide as template** and give the file a descriptive name.



- ! It is also possible to use an existing group configuration to create a template at a later time. Do this by right-clicking on the LANconfig group configuration in the appropriate folder. Then enable the context-menu option **Provide as template** and give the file a descriptive name.

8. Click on **Save** to conclude the action.

- ! The group configuration saves all parameters in a group configuration file, including parameters with preset default values. Use the scripting function to read out only the non-default settings from a device and, if applicable, transfer them to other devices.

The associated group configuration file appears in the list of entries and has the description **Group configuration**. To change the name of the group configuration, access the file's properties. To do this, click on the entry with the right-hand mouse key and select **Properties** from the context menu.

- ! In LANconfig you have the option of creating multiple references to the same group configuration. A change to this effects the devices in all of the folders if a group configuration is assigned to different LANconfig folders.

Using an existing group configuration file

In some cases it may be useful to use a different structure of devices managed with LANconfig than required by the group configuration. For example, devices in different site-specific folders may belong to the same groups. In order to avoid redundant group configuration files for every folder, you may want to create links to a shared file in multiple folders.

To use an existing group configuration file for a group of devices, use the mouse to right-click on the appropriate folder. In the context menu select **Add group configuration**.

In the subsequent dialog, select the existing group configuration file to create a link to this file in the folder.

- ! Please note that changes to the group configuration file will lead to changes in that group configuration in various folders.

If you create additional devices in a group folder, or if you modify an existing group configuration, LANconfig informs you that an update to the appropriate devices is available. This update can be carried out either directly afterwards or at any later time by using the context menu.

Additions to the menu system

Group

Group configurations are managed under the menu item 'Group'.

For further information please refer to section [Flexible group configuration with LANconfig](#).

New group configuration

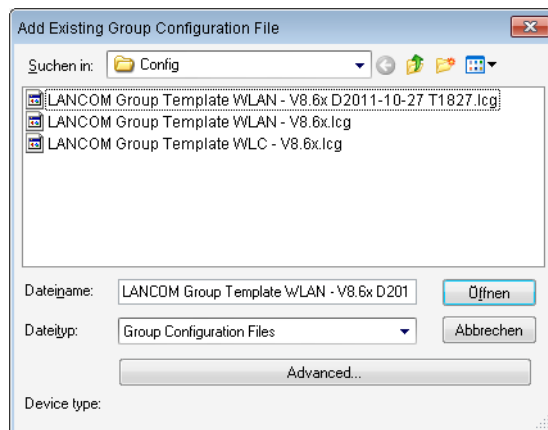
Under **Group > New group configuration** you create a new group configuration in the current folder.

New folder with group configuration

Under **Group > New folder with group configuration** you create a new sub-folder with a new group configuration in the current folder.

Add group configuration

Under **Group > Add group configuration** you can save an existing group configuration to the active folder. Select the relevant file to do this.



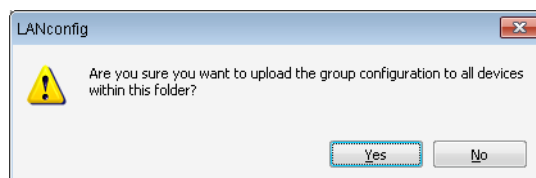
Edit group configuration

Under **Group > Edit group configuration** you have the option to edit the highlighted group configuration.

The parameters set here must be valid for the entire group. When the configuration dialog is closed, LANconfig will request that you save the group configuration file to a location of your choice.

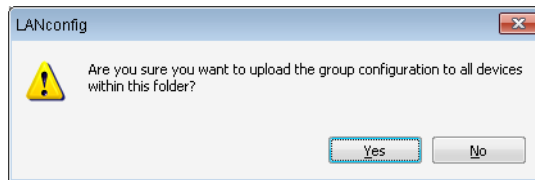
Refresh all devices

Under **Group > Update all devices** you have the option to use the selected and activated group to update all of the devices in the current folder.



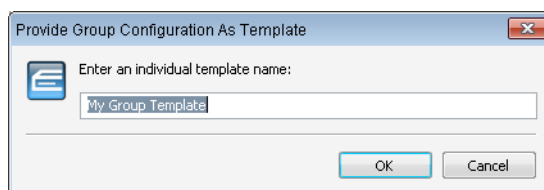
Update recommended devices

Under **Group > Update recommended devices** you have the option to use the selected and activated group to update the recommended devices in the current folder.



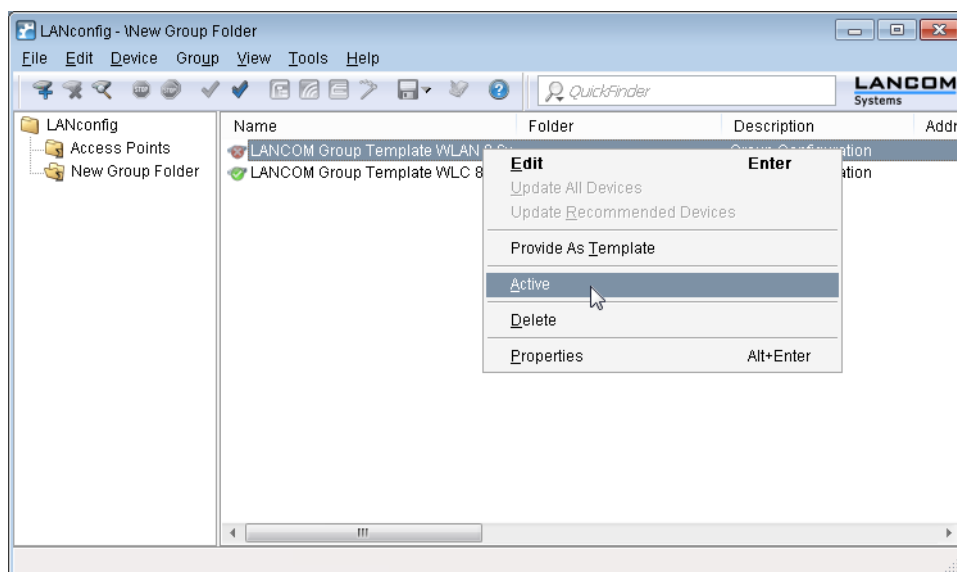
Provide as template

Under **Group > Provide as template** you have the option to set the highlighted group configuration as a template for future group configurations.



Active

Enable or disable the selected group configuration with the menu item **Group > Active**.



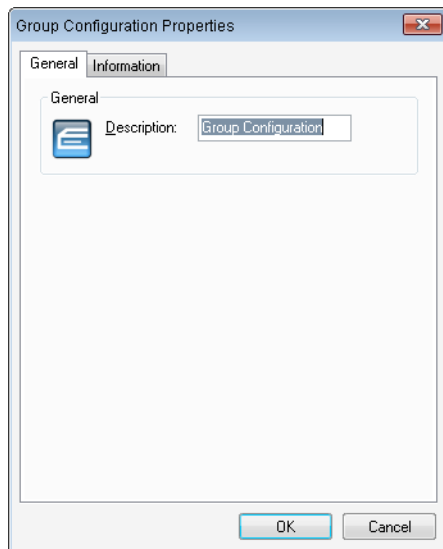
Delete

With **Group > Delete** you can delete the highlighted group configuration.

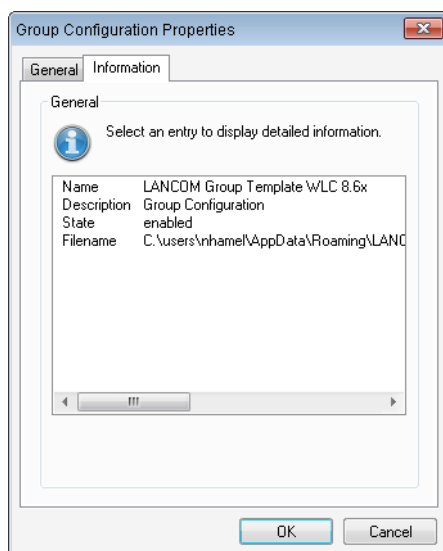
Features

Under **Group > Properties** you can view information about an existing group configuration. Select the relevant file to do this.

The **General** tab displays the description of the group configuration.



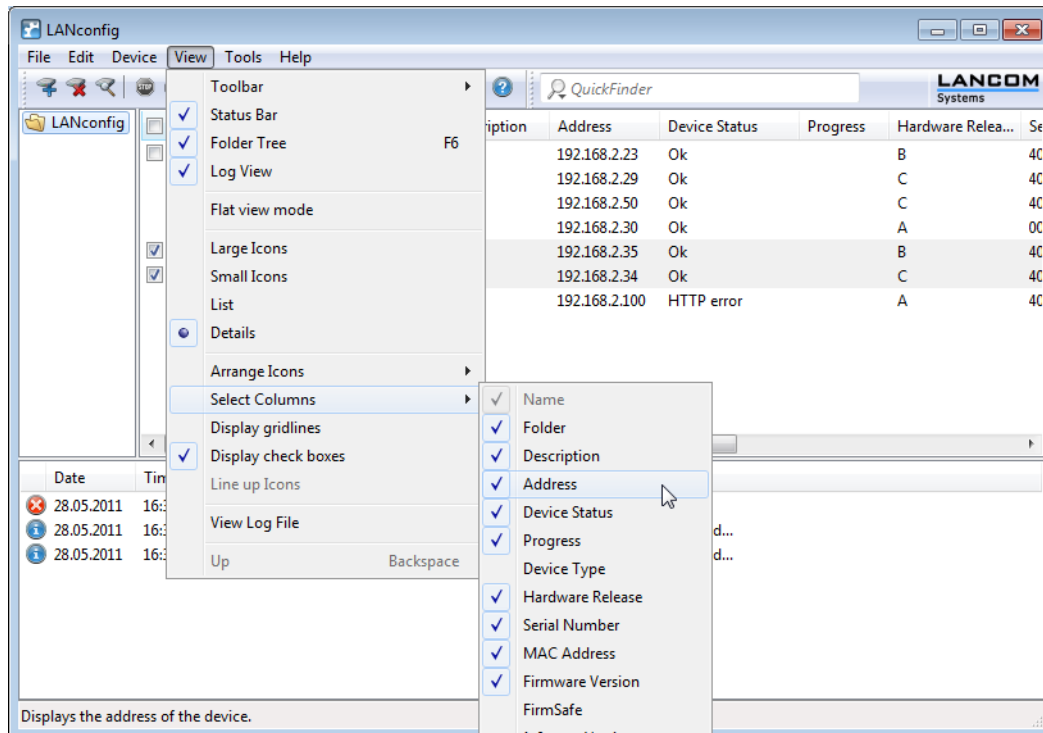
The **Information** tab shows the name, status, and the file name of the group configuration.



1.2.4 Better overview in LANconfig with more columns

As a help for large-scale projects, LANconfig provides a better overview and quicker orientation with its columns featuring device-related details that can be shown or hidden according to your needs. Choose the columns to be displayed from **View > Select columns**. The menu item **View > Arrange icons** allows you to sort the items as you prefer.


- ! Sort the view by clicking with the left mouse button in the appropriate column heading. Each new click reverses the sorting.



The following details can be displayed in the various columns:

- Name
- Folder
- Description
- Comment
- Address
- Location
- Device status
- Progress
- Device type
- Product code
- Hardware release
- Serial number
- MAC address
- Firmware version
- FirmSafe
- 1) Image version
- 2) Image version

With **Select all** or **Hide all** you can show or hide all columns with just one click.

 The column **Comment** contains the information in comment field 1 for the device.

System data	Device status	Syslog
Name:	LCWLC-4025	
Location:	Conference room	
Administrator:		
Comments:	Stock 01 and 02	
Device type:	LANCOM WLC-4025	
Hardware release:	C	
Firmware version:	8.60.0086 / 25.10.2011	
Serial number:	084191800018	

1.2.5 Checking the system-time source in the customized Rollout Wizard

The field `check_time` contains the new attribute `source` to verify the source of the system time.

Fields and attributes

The wizard uses fields in order to display information to the user and to give the user the option to enter information. Each field corresponds to an internal variable.

The wizard defines a field by specifying the appropriate key word, followed by an internal variable on the same line. Additional lines that follow can optionally contain the attributes for the field.

An example of a field definition in the wizard:

```
selection_buttons select_inet
description str.inet_Selection
button_text str.inet_PPPoE, str.inet_IPoE
```

This field generates a group of radio buttons, only one of which can be activated by the user. The wizard places the text defined in the string table `str.inet_Selection` as a description next to the field. For the radio buttons themselves, the wizard displays the text under `str.inet_PPPoE` and `str.inet_IPoE`. After an option was selected by the user, the wizard writes the selected value to the internal variable `wizard.select_inet`.

You can use the following fields in the wizard:

`check_local_ip`: This field checks if the wizard previously changed the device's IP address and redirects the user to the corresponding HTML page. Possible attributes:

- `destination`: Target for forwarding as a FQDN or IPv4 address.
- `timeout`: Wait time before forwarding.

`check_time`: This field verifies if the device has valid time information. Possible attributes:

- `success_jump`: Label of the page that the wizard opens if the check is successful.
- `fail_jump`: Label of the page that the wizard opens if the check fails.

- **limit**: Maximum number of checks before the wizard considers the test to have failed. Set the limit to the value '0' to continue the checks without limit.
- **timeout**: Wait time between two checks.
- **source**: The system-time source to be checked. If system time is obtained from another source, the test is evaluated as failed. Possible entries:
 - RAM
 - NTP
 - CAPWAP
 - RTC
 - ISDN
 - LANCONFIG
 - manual

entryfield_hex: This field is used for entering hexadecimal values, such as MAC addresses. Possible attributes:

- **description**: Field description in the HTML display
- **max_len**: Maximum number of characters that the user can enter into this field
- **never_empty**: A value of '1' for this attribute denotes a field that the user must fill out.
- **add_to_charset**: Adds extra characters to the default input character set.
- **default_value**: Default value

entryfield_ipaddress: This field is used to enter IPv4 addresses. Possible attributes:

- **description**: Field description in the HTML display
- **never_empty**: A value of '1' for this attribute denotes a field that the user must fill out.
- **never_zero**: A value of '1' for this attribute denotes a field that may not contain the value '0'.
- **add_to_charset**: Adds extra characters to the default input character set.
- **default_value**: Default value

entryfield_numbers: This field is used to enter telephone numbers. Possible attributes:

- **description**: Field description in the HTML display
- **max_len**: Maximum number of characters that the user can enter into this field
- **never_empty**: A value of '1' for this attribute denotes a field that the user must fill out.
- **add_to_charset**: Adds extra characters to the default input character set.
- **default_value**: Default value

entryfield_numeric: This field is used to enter numbers. Possible attributes:

- **description**: Field description in the HTML display
- **range_min**: Minimum value that the user can enter in this field
- **range_max**: Maximum value that the user can enter in this field
- **signed_value**: Allows you to specify a numerical value with a sign
- **never_empty**: A value of '1' for this attribute denotes a field that the user must fill out.
- **add_to_charset**: Adds extra characters to the default input character set.
- **default_value**: Default value
- **unit**: The unit of value shown after the input field in the wizard's HTML display.

entryfield_text: This field is used to enter text. The attribute **hidden** is for fields used to enter passwords. Possible attributes:

- **description**: Field description in the HTML display
- **hidden**: Identifies a field used by the user to enter a password.
- **add_to_charset**: Adds extra characters to the default input character set.

- `convert_to_upper`: Converts user input into uppercase letters
- `max_len`: Maximum number of characters that the user can enter into this field
- `min_len`: Minimum number of characters that the user can enter into this field
- `never_empty`: A value of '1' for this attribute denotes a field that the user must fill out.
- `unit`: The unit of value shown after the input field in the wizard's HTML display.

`entryfield_textwithlist`: This field is used to enter text. The user also has the option of selecting from a set of predefined values. Possible attributes:

- `description`: Field description in the HTML display
- `default_value`: Default value
- `max_len`: Maximum number of characters that the user can enter into this field
- `item_value`: List of predefined values that the user can select for this field

`onoff_switch`: This field creates a simple check box. Possible attributes:

- `description`: Field description in the HTML display
- `value_list`: List of the two values that the check box may take on
- `default_selection`: Default value

`page_switch`: This field creates a link with which the user can switch to one of the wizard's several other HTML pages. Possible attributes:


- `page_description`: Comma-separated list of text strings or references to strings that describe the possible link targets.
- `page_label`: Comma-separated list or page labels of the possible link targets.
- `description`: Field description in the HTML display

`ping_barrier`: This field stops the wizard from being executed until a ping to the target was answered successfully. Possible attributes:

- `destination`: Target address for the ping.
- `loopback`: Loopback address used by the ping instead of the default reply address
- `success_jump`: Label of the page that the wizard opens if the ping is successful.
- `fail_jump`: Label of the page that the wizard opens if the ping fails.
- `limit`: Maximum number of pings before the wizard considers the test to have failed. Set the limit to the value '0' to continue sending pings without limit.
- `timeout`: Wait time between two pings.

`popup`: This field opens the entered target address in a popup window. Possible attributes:

- None

 The target address can contain variables.

`readonly_text`: This field creates a read-only field. The wizard can use these fields to display text. The wizard can use `hidden` attributes to define internal variables. Possible attributes:

- `description`: Field description in the HTML display
- `unit`: The unit of value shown after the input field in the wizard's HTML display
- `hidden`: Identifies a hidden field.

`selection_buttons`: This field generates a group of radio buttons, only one of which can be activated by the user. Possible attributes:

- `description`: Field description in the HTML display

- **button_text**: Comma-separated list of text strings or references to strings that describe the individual radio buttons.
- **button_value**: Comma-separated list of text strings with the values of the individual radio buttons.

selection_list: This field generates a drop-down selection list for the user to select a value. Possible attributes:

- **description**: Field description in the HTML display
- **item_text**: Comma-separated list of text strings or references to strings that describe the individual list entries.
- **item_value**: Comma-separated list of text strings with the values of the individual list entries.
- **default_selection**: Default value

static_text: This field creates static text on the HTML page following the field name as a reference to a text string. Possible attributes:

- None

1.3 WLAN

1.3.1 WLAN RF optimization

LCOS version 8.60 features an improved wireless RF optimization:

- The WLAN controller no longer assigns the channels in the random order that the individual access points registered at the controller. Instead it assesses the channel interference between the access points and assigns the WLAN channels in descending order, starting with the access point with the strongest interference.
- RF optimization is now also available for access points transmitting in the 5-GHz band.



In this case you should ensure that the "indoor-only" mode is activated in these devices.

Automatic radio-field (RF) optimization with LANCOM WLAN controllers

Selecting the channel from the channel list defines a portion of the frequency band to be used by an access point for its logical wireless LANs. The WLAN clients connected to an access point have to share the same channel on the same frequency band. Channels 1 to 13 are available (depending on the country) in the 2.4-GHz band, and in the 5-GHz band channels 36 to 64 are available. On each of these channels, only one access point at a time can actually transfer data. In order to operate another access point within radio range with maximum bandwidth, each access point must use a separate channel—otherwise all of the participating WLANs would have to share a single channel's bandwidth.



With a completely empty channel list, the access points could automatically select channels which overlap in some areas, so reducing signal quality. Similarly, the access points might select channels which the WLAN clients cannot use due to the country settings. To direct access points towards certain channels, the non-overlapping channels 1, 6, 11 can be activated in the channels list.

In larger installations with several access points it can be difficult to set a channel for every access point. With automatic radio-field (RF) optimization, the LANCOM WLAN controllers provide an automatic method of setting the optimum channels for access points that work in the 2.4-GHz band and 5-GHz band.

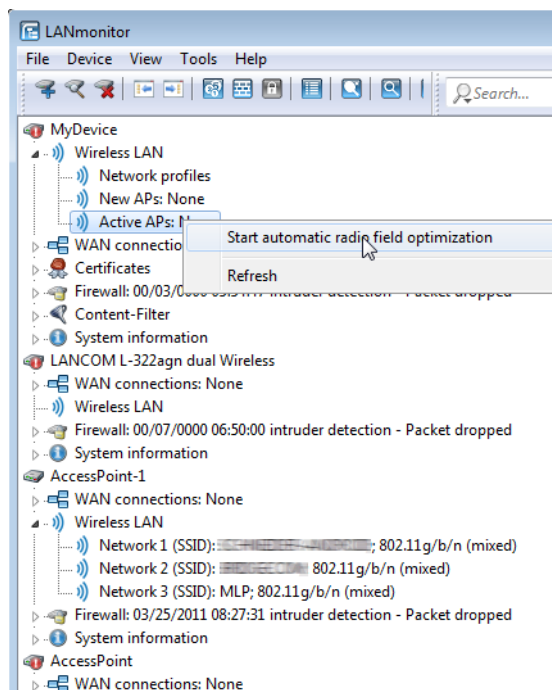


You should ensure that access points transmitting in the 5-GHz band are set to the "indoor only" mode.

WEBconfig: **Setup > WLAN-Management > Start-automatic-radio-field-optimization**

! You can invoke optimization for a single access point only by entering its MAC address as a parameter for the action.

LANmonitor: Right-click on the list of active access points or on a specific device, and in the context menu select **Start automatic RF optimization**.



Optimization is then carried out in the following stages:

1. The WLAN controller assigns the same channel to all access points. The selected channel is the one being used by the majority of access points.
2. The access points carry out a background scan and report the results to the WLAN controller.
3. Based on the devices found by the background scan, the WLAN controller sets an interference value for each access point.
4. It then deletes the AP channel list for all access points. With the channel list now empty, each access point receives a configuration update with a new channel list for its respective profile.
5. The wireless controller disables the radio modules of all access points.
6. The individual access points now go through the following sequence. This begins with the access point with the highest interference value being the first to select a channel.
7. In the order of the interference values the WLAN controller enables the radio modules in the access points, which then start their automatic calibration. Each access point automatically searches for the best channel from the channel list assigned to it. To determine which channel is the best, the access point scans for interference to determine the signal strengths and channels occupied by other access points. Because the former list in the WLAN controller's configuration was deleted, this is now the profile channel list. If the profile channel list is empty, then the access point has freedom of choice from the channels that are not occupied by other radio modules. The selected channel is then communicated back to the WLAN controller and entered into the AP channel list there. Thus the access point receives the same channel the next time a connection is established. The AP channel list thus has a higher weighting than the profile channel list.

! If an access point has multiple radio modules, each module goes through this process in succession.

1.3.2 Group key per VLAN

The following section provides explanations for the management of group keys in the VLAN.

Introduction

In a VLAN environment, the central network administration generally assigns a unique VLAN ID to each virtual network. Which VLAN a client belongs to is mostly decided by the physical connection between the client and the network.

The central instance that manages the network (e. g. a VLAN-capable switch) internally assigns its ports to certain VLAN IDs. A data packet arriving at a port is internally passed on only to the ports with the corresponding VLAN IDs. Packets are not sent to the other network nodes that are connected to ports with different (or no) VLAN IDs.

In the case of multiple VLANs that offer various service levels, data communications are channeled through different logical wireless LANs (SSIDs). For example, employees receive access to the corporate network and the Internet via a specific SSID. Guests receive a different SSID that offers access limited to the Internet.

LANCOM access points also maintain VLAN network tables, which control the assignment of wireless LAN clients to individual VLANs. In large network environments, a RADIUS server usually handles the rights management and the assignment of clients to the VLANs. After successful authentication, the RADIUS server returns the data to the corresponding access point. For the duration of the client association, this data is stored in the AP's VLAN network table.

If necessary, the different WLAN clients associated with the same access point obtain different VLAN IDs. This is handled by the dynamic VLAN network tables in the access points. VLAN-internal communication is protected by a session key negotiated when logging onto the access point. This ensures that data communications by clients in different VLANs remain isolated from each other even though the various clients are using the same logical wireless LAN (SSID) to communicate with the access point.

A client associating with an access point in a wireless LAN is also assigned with a group key for the reception of broadcast or multicast messages.

Broadcast and multicast messages do not support VLAN tagging. This is why wireless LAN clients that are located in an isolated VLAN cannot be excluded from receiving these messages. In the ideal case, the wireless clients ignore broadcast and multicast messages from outside the VLAN.

Since these messages are increasingly being used for network configuration, the following problems arise:

- Network protocols such as "UPnP" and "Bonjour" use these messages to announce new services in the network.

Theoretically, wireless LAN clients could set up access to servers that they have no access to at all.

- The Internet standard IPv6 uses multicast broadcasting to transmit router information to the clients.

There is a risk that wireless LAN clients from outside the VLAN can use this information to evade access to the VLAN for which they are actually registered.

The widespread use of IPv6 will lead to an increase in this type of client problem.

To avoid these problems, the access point can assign a separate group key to each VLAN, instead of one that applies to all wireless LAN clients. Thus the access point sends its broadcast and multicast transmissions not to all existing wireless clients, but solely to a specific VLAN and the clients registered there. The wireless LAN clients in other VLANs therefore cannot decrypt these broadcasts.



The IEEE 802.11 standard provides for the administration of 4 different keys. One key is always reserved for the secure unicast communication between the access point and a wireless LAN client.

Thus in principle a maximum of 3 separate VLANs can be managed with their own group keys. Each group key is either managed automatically by the access point or manually by the network administrator. When the wireless LAN client logs on to the network, the access point sends it the corresponding VLAN group key to decrypt the broadcast and multicast transmissions for that VLAN.

This results in 2 possible scenarios:

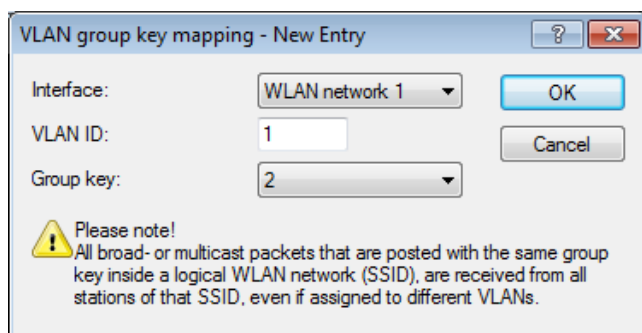
- No more than 3 VLANs are set up in the area of an access point: These VLANs are securely separated from each other by the 3 VLAN group keys.
- More than 3 VLANs exist within range of an access point: In this case, at least two VLANs share a group key. The administrator must find the optimal distribution of the shared group keys between the VLANs.

VLAN group keys are managed in 2 tables:

- The configuration table in which the assignment is carried out manually by the administrator.
- The status table in which the automatic group key assignment by the access point can be viewed.

Managing VLAN group keys

If you want to use different VLAN IDs on a single logical wireless LAN network (SSID), you have the option to assign the appropriate group key for broadcast and multicast transmissions. This setting in LANconfig is found under **Wireless LAN > 802.11i/WEP > Extended settings > VLAN group key mapping**



The automatic assignment of group keys is carried out in the following steps:

1. When a wireless LAN client logs on, the access point checks whether its VLAN ID is already listed in the status table and assigned to a group key accordingly.
2. If not, the access point consults the configuration table to check whether there is a manual assignment. Should this be the case, then it creates a mapped entry in this table.
3. If there is no manual assignment either, the access point adds a new entry for this client and assigns the group key with the fewest users.

The status table displaying the current automatic VLAN group key assignments for each SSID can be found at **LCOS menu tree > Status > WLAN > VLAN groupkey mapping**

Additions to the menu system

VLAN group key mapping

This table contains the mapping of VLAN group keys to the logical WLAN networks.

SNMP ID:

12/2/1970

Telnet path:

Setup > WLAN > VLAN-groupkey-mapping

Network

Contains the name of a WLAN network registered in the device.

SNMP ID:

2.12.70.1

Telnet path:**Setup > WLAN > VLAN-groupkey-mapping****VLAN ID**

Contains the VLAN ID assigned to the logical WLAN network.

SNMP ID:

2.12.70.2

Telnet path:**Setup > WLAN > VLAN-groupkey-mapping****Possible values:**

1 to 4094

Default:

1

Group key index

The table contains the group key index:

SNMP ID:

2.12.70.3

Telnet path:**Setup > WLAN > VLAN-groupkey-mapping****Possible values:**

1 to 3

1.3.3 How the 40-MHz mode works

Additions to the menu system**Allow 40MHz**

The default setting automatically optimizes the value for bandwidth. If the momentary operating conditions allow, a bandwidth of 40MHz will be enabled, which is otherwise limited to 20MHz.

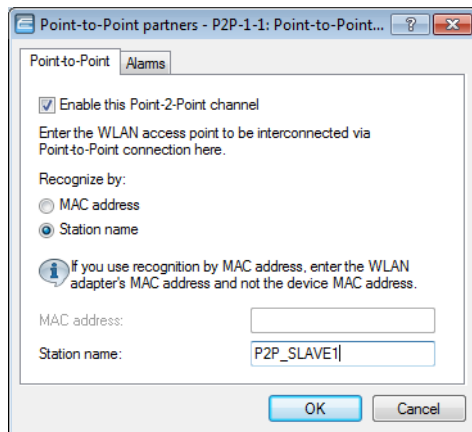
You also have the option of switching this mechanism off, so limiting the bandwidth to the narrower 20MHz.

The 802.11n standard specifies a channel bonding from 20MHz to 40MHz.

Telnet path:/Setup/Interfaces/WLAN/Radio-Settings/Allow-40MHz


1.3.4 Point-to-point partners

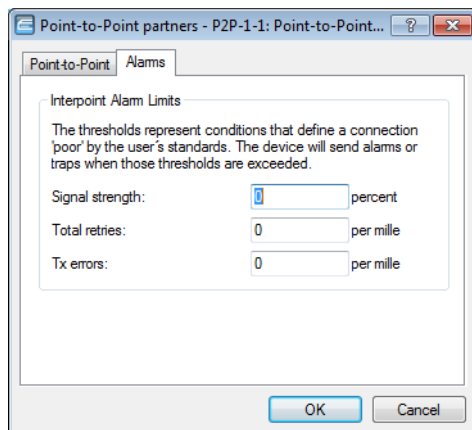
Up to 16 point-to-point connections can be activated for each WLAN module. In LANconfig you find these settings under **Wireless LAN > General > Interfaces > Point-to-point partners**



Proceed as follows to set up a point-to-point link:

1. Select the option **Enable this point-2-point channel**.
2. Select whether the P2P peer is to be identified by its **MAC address** or its **Station name**.
3. The corresponding text box is activated. Enter the MAC address or station name.

 If you work with detection by MAC address, enter the MAC address of the WLAN module here and not that of the device itself.



On the **Alarm** tab, you can set threshold values for **signal strength**, **total repetitions** and **Tx errors** for the point-to-point connection. If the value exceeds or falls below this value, the access point sets off alarms or traps.

Conclude your entries by clicking on **OK**.

Additions to the menu system

Interpoint peers

Here you enter the wireless base stations that are to be networked via the point-to-point connection.

SNMP ID: 223.20.12

Telnet path: /Setup/Interfaces/WLAN

1.3.5 Adjustable rate adaption algorithm

Unlike an Ethernet connection, a wireless connection uses variable bit rates. Higher bit rates provide a better throughput, but they require a high signal quality at the receiver end. This is essential for error-free decoding. WLAN devices adapt their bit rate the first time a connection is made or if there is a change to the properties of the medium. This ensures that the device uses the best available bit rate.

Unlike the standard algorithm, the well-known Minstrel algorithm checks not only the neighboring bit rates, but all available bit rates. This is a quicker way of determining the optimal bit rate.

Additions to the menu system

Method

You have the option to set the desired rate adaptation algorithm.

SNMP ID:

2.12.51.1

Telnet path:

Setup > WLAN > Rate-Adaptation

Possible values:

standards

Minstrel

Default:

Minstrel

Initial rate

The initial rate determines the starting bit rate that the algorithm uses to determine the optimal bit rate.

SNMP ID:

2.12.51.2

Telnet path:

Setup > WLAN > Rate-Adaptation

Possible values:

Minimum

RSSI-derived

Default:

Minimum

Minstrel averaging factor

The averaging factor used for recalculating the net rates for each bit rate according to the Minstrel method.

SNMP ID:

2.12.51.3

Telnet path:

Setup > WLAN > Rate-Adaptation

Possible values:

0 to 99

Default:

75

Standard averaging factor

The averaging factor used for recalculating the net rates for each bit rate according to the standard method.

SNMP ID:

2.12.51.4

Telnet path:

Setup > WLAN > Rate-Adaptation

Possible values:

0 to 99

Default:

0

1.4 Public Spot

1.4.1 Using hidden fields on the login form in Public Spot page templates

General speaking, the Public Spot's page templates use the special identifier `<pbelem loginform>` in the syntax for designing login pages. The login pages generated in this way contain hidden fields such as the original URL.

In some applications you may want to avoid using `<pbelem loginform>` and construct the login pages differently. If you still wish to include the original URL on the login page, you can integrate the identifier `<pbelem hiddenfields>` in the page template. When drawing the login pages, the contents of the hidden fields (in particular the original URL) is automatically integrated into the source code.


1.4.2 Public Spot user administration

The Setup Wizards provide you with an easy method of managing Public Spot users.

Adding new Public Spot users with a single click

In WEBconfig, you can register new Public Spot users with the setup wizard **Create Public Spot Account**. This wizard is preset with default values, so you can set up a new user with a single click on **Save & Print**.

The following settings can be configured if required:

- **Starting time for account:** Sets the time when the voucher becomes valid. Possible values are:
 - **First login (default):** The time starts running when the user logs in for the first time
 - **Immediately:** The time starts running when the user is created
 - **Validity period:** Enter the overall time period within which the voucher can remain valid.
-
-  If the access is to be valid immediately, it is not possible to enter a validity period.
- **Duration:** Set how long access is to be available after registration or the first login.

- **SSID (network name):** Select the wireless LAN network for which the access applies. The default network name is already highlighted. This SSIDs listed here are managed in the SSID table.

! Press the "Ctrl" key to select multiple entries.

- **Number of vouchers:** Specify how many vouchers you want to create at a time (default: 1).
- **Time budget (minutes):** Specify the amount of time after which access to the Public Spot is closed.

! Depending on the chosen expiry method, access time is limited either to the time budget (incremental) or to the set voucher validity period (absolute).

- **Volume budget (MByte):** Specify the available data volume after which access is closed.
- **Comment (optional):** Add a comment.
- **Prints comment on voucher:** Check this option if the comment is to appear on the voucher.
- **Print:** Check this option to print the vouchers as soon as they are registered (default: on)

! If this option is disabled, the wizard displays a summary of the new Public Spot users after they have been registered. You then have the opportunity to print the vouchers again.

You can configure the default values that are to be used when creating new Public Spot accounts in the following menus:

- LANconfig: **Public Spot > Public Spot Wizard**
- WEBconfig: **LCOS Menu Tree > Setup > Public-Spot module > Add user wizard**

Wizard for Public Spot user management

You can manage registered Public Spot users with WEBconfig by using the Setup Wizard **Manage Public-Spot Accounts**. The wizard shows you a table of data of all registered users.

192.168.2.34 - Manage Public Spot Account

LANCOM
Systems
... connecting your business

Save as CSV

Show 10 entries per page Search:

Page	User-Name	Password	Comment	Expiry-Type	Abs.-Expiry	Rel.-Expiry	Time-Budget	Volume-Budget
All	user21391	afzysb	pubSpUser edited by mhdshon on 11/10/2011 12:02:29 ()	Absolute and Relative	10/30/2012 18:42:51	3600	0	0
	user359	p6awuk	pubSpUser edited by msahm on 01.11.2011 17:39:33 ()	Absolute and Relative	10/30/2012 18:42:51	3600	0	0
	user56491	y6_nzs	pubSpUser edited by msahm on 01.11.2011 17:39:32 ()	Absolute and Relative	10/30/2012 18:42:53	3600	0	0
	user3130	wybrg4	pubSpUser edited by msahm on 01.11.2011 17:39:30 ()	Absolute and Relative	10/30/2012 18:42:54	3600	0	0
	user43752	vnqpcu	pubSpUser edited by msahm on 01.11.2011 17:39:29 ()	Absolute and Relative	10/30/2012 18:42:55	3600	0	0
	user63935	ghd94z	pubSpUser edited by msahm on 01.11.2011 17:39:28 ()	Absolute and Relative	10/30/2012 18:42:56	3600	0	0
	user14196	k8vj3s	pubSpUser edited by msahm on 01.11.2011 17:39:27 ()	Absolute and Relative	10/30/2012 18:42:58	3600	0	0
	user9794	vkrdh7	pubSpUser edited by msahm on 01.11.2011 17:39:26 ()	Absolute and Relative	10/30/2012 18:42:59	3600	0	0
	user18501	8myyug	pubSpUser edited by msahm on 01.11.2011 17:39:24 ()	Absolute and Relative	10/30/2012 18:43:01	3600	0	0

Back to Main-Page Save Delete Print

User-Name	Password	Comment	Expiry-Type	Abs.-Expiry	Rel.-Expiry	Time-Budget	Volume-Budget
-----------	----------	---------	-------------	-------------	-------------	-------------	---------------

In the **Show ... entries per page** drop-down list you set how many entries are displayed per page (default: 10 entries). The corresponding pages are accessed via the page navigation at the lower right:

- **First page:** Shows the page with the first entries.
- **Previous page:** Moves back one page.
- **Page numbers (1, 2, 3,...):** Move directly to the selected page.
- **Next Page:** Moves forward one page.
- **Last page:** Shows the page with the last entries.

With **Search** you can filter the displayed entries. The filter immediately searches for entered strings.

You export highlighted entries with **Save as CSV**.

The column headers have the following meaning:


- **Page/All:** This column is used to select the user for the desired action (print, delete, save). To select all entries on the current page, select **Page**. To select all of the entries, select **All**.
- **User name:** Displays the user name assigned automatically by the system.
- **Password:** Displays the password assigned by the system.
- **Comment:** Includes the comment entered at registration (in brackets) and any changes to the user data (automatically documented by the system).
- **Expiry type:** Indicates whether the validity period of this user account is absolute (e.g. expires on a set date) or relative (expires after the time lapsed since the first successful login).
- **Abs. expiry:** If "absolute" has been selected as the expiry type, this user account becomes invalid at the time defined by this field.
- **Rel. expiry:** If "relative" has been selected as the expiry type, this user account becomes invalid after this time period has expired since the user logged in for the first time.
- **Time budget:** Specifies the maximum 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.
- **Volume budget:** Specifies 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.

The buttons at the bottom of the window have the following functions:

- **Print:** Print out the voucher for the selected user.
- **Delete:** Delete the selected user.
- **Save:** Store the changes.
- **Back to main page:** Return to the main page; all unsaved changes will be lost.

You can edit the following user information by changing the contents of the corresponding fields:

- **Expiry type**
- **Abs. expiry**

 Click on **Save** after making any changes. Unsaved changes are lost once you finish this wizard.

Managing Public Spot users via the web API

As an alternative to using the Setup Wizard, entering a special URL in the address bar gives you the option of displaying, creating or deleting Public-Spot users directly.

URL structure

The URL is structured as follows:

```
http://<Device-URL>/cmdpbspotuser/
?action=actiontodo&parameter1=value1&parameter2=value2
```

The following actions are available:

- **action=addpbspotuser:** Creates one or more new Public Spot users and then prints out the required number of vouchers.
- **action=delpbspotuser:** Deletes the Public Spot user with the specified user ID.
- **action=editpbspotuser:** Displays the Public Spot user with the specified user ID. You can then print out the user's voucher again.

The required parameters and their values depend on the action specified.

- ! The Wizard ignores incorrect parameter information and accepts only the correct parameters. If you omit a required parameter or specify it incorrectly, the wizard displays an input mask. Enter the correct parameter values here.

Adding a Public Spot user

To register a new Public Spot user, simply enter the following URL:

```
http://<device-URL>/cmdpbspotuser/  
?action=addpbspotuser&parameter1=value1&parameter2=value2&...
```

The following parameters are available:

comment

Comment on the registered user

If it is possible to enter multiple comments for a Public Spot user, you can enter the comments and their corresponding comment-field names as follows:

```
&comment=<Content1>:<FieldName1>;<Content2>:<FieldName1>;  
...;<Content5>:<FeildName5>
```

If there is just one comment field per user, then the comment is entered as follows:

```
&comment=<Comment>
```

- ! Special characters such as German umlauts are not supported.

- ! The maximum number of characters for the comment parameter is 191 characters.

print

Automatic print-out of the voucher.

If this parameter is omitted, the wizard displays a button that you can use to print the voucher.

printcomment

Print the comment on the voucher.

If this parameter is omitted, no comment will appear on the voucher (default setting).

nbguests

The number of Public Spot users to be created.

If this parameter is omitted, the wizard creates one user only (default setting).

defaults

Use default values

The wizard replaces missing or incorrect parameters with default values.

expiretype

Combined output of expiry type and validity period of the voucher.

Specify this parameter as follows:

```
&expiretype=<Value1>+validper=<Value2>
```

The parameter values have the following meaning:

- Value1: Expiry type (absolute, relative, absolute and relative, none)
- Value2: Expiration period of the voucher

If these parameters are omitted or set with incorrect values the wizard will apply the default values.

ssid

Network name

If this parameter is omitted, the wizard uses the default network name (default setting).

unit

Access time

Specify this parameter as follows:

```
&unit=<Value1>+runtime=<Value2>
```

The parameter values have the following meaning:

- Value1: Unit used to measure runtime. Possible values are: Minute, hour, day
- Value2: Runtime

timebudget

Time budget

If this parameter is omitted, the wizard uses the default value.

volumebudget

Volume budget

If this parameter is omitted, the wizard uses the default value.



If the Public Spot administration contains no default values to replace missing parameters, the wizard opens a dialog. Enter the missing values here.

Deleting a Public Spot user

Delete one or more Public Spot users simply by entering the following URL:

```
http://<deviceURL>/cmdpbspotuser/  
?action=delpbspotuser&pbspotuser=<User1>+<User2>+...
```

If the wizard finds the specified user in the user list, the user is deleted and the wizard displays a confirming message.

If the wizard cannot find the specified user, it displays a table of registered Public Spot users. Mark the entries for deletion here.

Editing a Public Spot user

Edit one or more Public Spot users simply by entering the following URL:

```
http://<device-URL>/cmdpbspotuser/  
?action=editpbspotuser&parameter1=value1&parameter2=value2&...
```

The following parameters are available:

pbspotuser

Name of the Public Spot user

Specify multiple users in the form `&pbspotuser=<User1>+<User2>+...`

If the wizard cannot find the specified user, you have the option to search for a user.

After making your changes, accept these and print them out if necessary.

expiretype

Combined output of expiry type and validity period of the voucher.

Specify this parameter as follows:

```
&expiretype=<Value1>+validper=<Value2>
```

The parameter values have the following meaning:

- Value1: Expiry type (absolute, relative, absolute and relative, none)
- Value2: Expiration period of the voucher

unit

Access time

Specify this parameter as follows:

```
&unit=<Value1>+runtime=<Value2>
```

The parameter values have the following meaning:

- Value1: Unit used to measure runtime. Possible values are
 - Minute
 - Hour
 - Day
- Value2: Runtime

timebudget

Time budget

If this parameter is omitted, the wizard uses the default value.

volumebudget

Volume budget

If this parameter is omitted, the wizard uses the default value.

print

Automatic print-out of the voucher.

If this parameter is omitted, the wizard displays a button. Use this to print out the voucher.



If the Public Spot administration contains no default values to replace missing parameters, the wizard opens a dialog. Enter the missing values here.

Additions to the menu system

SSID table

This table contains the list of network names available for Public Spot users.

SNMP ID:

224.19.11

Telnet path:

Setup > Public Spot module > Add User Wizard > SSID table

Network name

Enter here the name of a logical WLAN (stored in the device) for which access is to be provided to Public Spot users by means of billable vouchers.

SNMP ID:

2.24.19.11.1

Telnet path:

Setup > Public Spot module > Add User Wizard > SSID table

Possible values:

Maximum 32 alphanumerical characters

from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()*+,-./:;<=>?[\]^_.0123456789

Default

Blank

Default

Specifies the name of the wireless LAN as the default value. The Create Public Spot Account Wizard will automatically suggest this value in the list of available WLAN networks. If need be, you can change this value in the Wizard's input mask.

SNMP ID:

2.24.19.11.2

Telnet path:

Setup > Public Spot module > Add User Wizard > SSID table

Possible values:

No

Yes

Default

No

SSID

Enter the SSID that Public Spot Add-User wizard prints out on the form for the user.

SNMP ID: 224.19.4

Telnet path: Setup/Public-Spot-Module/Add-User-Wizard

English description: SSID

Possible values:

- Max. 32 alphanumerical characters

Default: Blank



If you leave this field blank, the Public Spot Add-User wizard fills out the form with the SSID of the first logical WLAN with an activated Public Spot.

1.4.3 Advanced redirection URL

Additions to the menu system

URL

URL of the page that your customers can use without logging in.

SNMP ID: 224.8.2

Telnet path: /Setup/Public-Spot-Module/Page-Table/URL

Possible values:

- Max. 100 characters

Default: By default, different HTML pages stored on the device file system can be displayed, depending on the page chosen by the user.

1.4.4 Variable station table

The station table is used to restrict or increase the maximum number of users logged on to the Public Spot according to various conditions such as the device type or application scenario. The maximum number of users is 65536. This setting is to be found in LANconfig under **Public Spot > Public Spot users > Users and authentication servers > Maximum entries in station table**.

Additions to the menu system

Station table limit

You can increase the maximum number of clients up to 65,536.

SNMP ID:

224.26

Telnet path:

Setup > Public-Spot-Module > Station-Table-Limit

Possible values:

16 to 65536

Default:

8.192



While the device is operating, changes to the station table only come into immediate effect if the table has been extended. Restart the access point in order to immediately reduce the size of the station table.

1.5 VPN

1.5.1 Improved phase 1 rekeying

Throughout the operation of an active VPN connection, the stations constantly check whether communications are subject to a previously agreed security association (SA). If the framework conditions change (e. g. a change of the client's IP address through relocation to a different radio cell), you must renegotiate this security association. This is done with "rekeying".

As of version 2.30, the LANCOM Advanced VPN Client transmits a special identification number (ID) during phase 1 rekeying. A LANCOM VPN gateway detects rekeying based on this ID and links the previous security association with the client. This makes re-authentication unnecessary.

1.5.2 MPPE encryption for PPTP tunnels

The encryption protocol MPPE (Microsoft Point-To-Point Encryption) secures data transmission over PPP and VPN connections with key lengths of up to 128 bit.

MPPE uses the "stateless mode" for encryption to ensure that both communication partners are synchronized. In this mode, the session key changes with each transmitted data packet. The two stations also synchronize their encryption tables (where the keys are stored for data encryption) each time.

VPN-capable devices from LANCOM use MPPE to encrypt data transfer by PPTP tunnel.

In LANconfig you find this setting under **Communication > Protocols > PPTP list**

If you have enabled the MPPE encryption protocol, connections to clients are established only under the following conditions:

- The client establishes a connection secured with MPPE. The router rejects the request for other protocols.
- The client uses as a minimum the key length specified in the router. With shorter key lengths the router refuses to connect and, with stronger encryption, the router switches to the appropriate key length.

Additions to the menu system

Encryption

Enter the key length here.

SNMP ID:

2.2.21.7

Telnet path:

Setup > WAN > PPTP-peers

Possible values:

Off

40 bit

56 bit

128 bit

Default:

Off

1.6 SIP ALG: Proxy for bypassing NAT in the router

The following sections provide explanations on the SIP ALG.

1.6.1 SIP ALG: Basics

SIP is increasingly becoming established as the basis for modern real-time communication in IP networks. Unified Communications (UC) and collaboration, IP telephony, video streaming, camera surveillance, intercoms, paging systems, and audio recordings increasingly rely upon SIP and RTP for switching and transmission.

The NAT (Network Address Translation) typically carried out by the access router at the edge of the LAN presents a barrier to SIP communications. This is because of the addresses transmitted during SIP signaling and also because of the dynamically negotiated media sessions and the UDP-based RTP connections that depend upon them.

Restrictive firewall configurations prevent communications even where client/server-side mechanisms such as STUN, ICE and TURN are used to overcome NAT.


The SIP ALG (Application Layer Gateway) for LCOS detects SIP connections and the RTP-based media streams that they depend upon and transforms these in line with the NAT rules in the access router.

Also, the SIP ALG monitors the bandwidths of the SIP connections and so provides QoS.


1.6.2 SIP ALG: Features

The SIP-ALG for LCOS has the following features:

- **No local registration:** The SIP proxy does not provide registration for SIP endpoints. Instead, it mediates the registrations directly to the approved SIP domains.

 This means that it is impossible to set up a line backup over alternative voice lines (analog, ISDN).

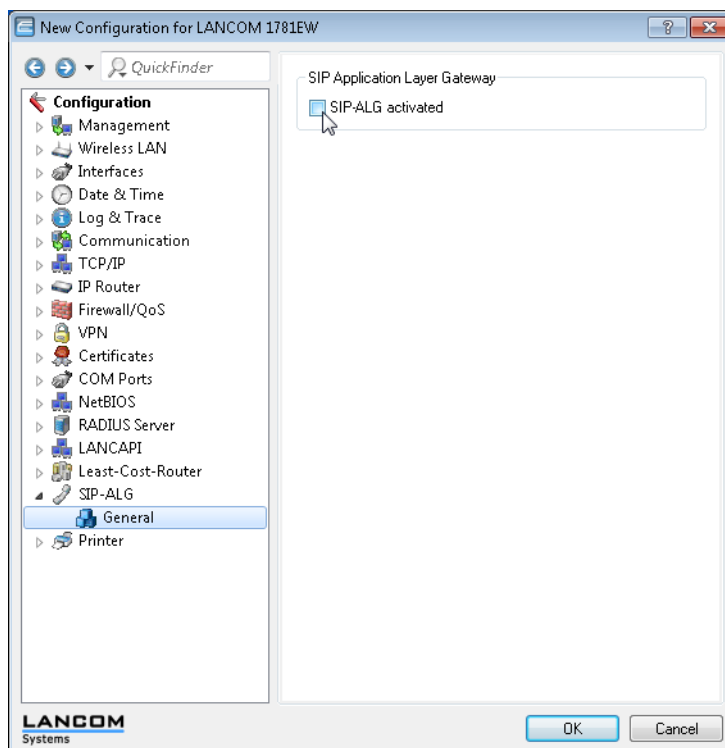
- **Transparency for SIP extensions:** The SIP ALG also transmits unknown, non-standard header elements to enable the SIP messages to be communicated between terminal devices and SIP PBXs.

 The SIP ALG determines an unambiguous destination for every SIP message. Forking (communication between multiple devices of the same identity) is handled upstream. The SIP-ALG merely provides transparent forwarding of these data packets.

1.6.3 SIP ALG: Configuration

The following sections provide explanations for the configuration of the SIP ALG.

! The SIP ALG is disabled in the default settings.



SIP ALG: Configuration by LANconfig

1. Start LANconfig, for example from the Windows start menu with **Start > Programs > LANCOM > LANconfig**. LANconfig now automatically searches the local network for devices. As soon as LANconfig has completed its search, it presents a list of all the devices it found, if possible with a brief description, the IP address and the status.
2. Double-click on the entry for the device on which the SIP ALG is to be configured. LANconfig opens the Configuration Wizard and displays the current configuration of the device.
3. In the Configuration Wizard, switch to the menu **SIP-ALG > General**.
4. If necessary, highlight the option **SIP ALG activated**. This option is already enabled in the default setting.
5. Close the configuration by clicking on **OK**.

1.6.4 Additions to the Setup menu

SIP ALG

Configure the settings for the SIP ALG here.

SNMP ID:

2.200

Telnet path:

Setup

Operating

This setting determines whether the SIP ALG is enabled.

SNMP ID:

2.200.1

Telnet path:

Setup > SIP-ALG

Possible values:

Yes

No

Default:

No

1.6.5 Additions to the Status menu

SIP ALG

This directory contains the status information provided for the SIP ALG (application layer gateway)

SNMP ID:

1.201

Telnet path:

Status

Calls

This table shows all current calls being routed via the SIP ALG.

SNMP ID:

1.201.3

Telnet path:

Status > SIP-ALG

Call ID

The call ID of the call.

SNMP ID:

1.201.3.2

Telnet path:

Status > SIP-ALG > Calls

SIP destination address

The IP address of the call destination.

SNMP ID:

1.201.3.3

Telnet path:

Status > SIP-ALG > Calls

SIP source address

The IP address of the call source.

SNMP ID:

1.201.3.4

Telnet path:

Status > SIP-ALG > Calls

SIP source port

The port used by the call source.

SNMP ID:

1.201.3.5

Telnet path:

Status > SIP-ALG > Calls

WAN address

The WAN address from which the call is made.

SNMP ID:

1.201.3.6

Telnet path:

Status > SIP-ALG > Calls

SIP WAN port

The WAN port from which the call is made.

SNMP ID:

1.201.3.7

Telnet path:

Status > SIP-ALG > Calls

RTP destination address

The destination address used by RTP.

SNMP ID:

1.201.3.8

Telnet path:

Status > SIP-ALG > Calls

RTP source port

The destination port used by RTP.

SNMP ID:

1.201.3.9

Telnet path:**Status > SIP-ALG > Calls****RTP source address**

The source address used by RTP.

SNMP ID:

1.201.3.10

Telnet path:**Status > SIP-ALG > Calls****RTP source port**

The source port used by RTP.

SNMP ID:

1.201.3.11

Telnet path:**Status > SIP-ALG > Calls****RTP WAN port**

The WAN port used to communicate by RTP.

SNMP ID:

1.201.3.12

Telnet path:**Status > SIP-ALG > Calls****Registrations**

This table shows all current registrations.

SNMP ID:

1.201.2

Telnet path:**Status > SIP-ALG****SIP-ID**

The SIP ID of the subscriber is the phone number of the SIP account or the user's name (SIP URI).

SNMP ID:

1.201.2.2

Telnet path:**Status > SIP-ALG > Registrations****Registrar domain**

This shows the domain where the SIP ID is registered.

SNMP ID:

1.201.2.3

Telnet path:

Status > SIP-ALG > Registrations

Registrar address

The IP address which the registrar can be reached.

SNMP ID:

1.201.2.4

Telnet path:

Status > SIP-ALG > Registrations

Client address

The IP address of the SIP client.

SNMP ID:

1.201.2.5

Telnet path:

Status > SIP-ALG > Registrations

Client port

The port used by the SIP client.

SNMP ID:

1.201.2.6

Telnet path:

Status > SIP-ALG > Registrations

WAN address

The WAN address used by this SIP ID.

SNMP ID:

1.201.2.7

Telnet path:

Status > SIP-ALG > Registrations

WAN port

The WAN port used by this SIP ID.

SNMP ID:

1.201.2.8

Telnet path:

Status > SIP-ALG > Registrations

Register method

This is the method used to establish a new connection.

SNMP ID:

1.201.2.9

Telnet path:**Status > SIP-ALG > Registrations****Possible values:**

REGISTER
INVITE
OPTIONS
NOTIFY
PUBLISH
SUBSCRIBE
INFO

Expiration time

The time in seconds before re-registration is required. This value does not indicate the time remaining but the time period negotiated during registration.

SNMP ID:

1.201.2.10

Telnet path:**Status > SIP-ALG > Registrations****Operating**

This value indicates whether the SIP ALG is enabled or not.

SNMP ID:

1.201.1

Possible values:

Yes
No

1.7 Voice over IP – VoIP

1.7.1 Restricting or preventing SIP registration over WAN connections

As of LCOS version 8.60 RC2, you can restrict the registration of SIP users at the Voice Call Manager over a WAN link, or prevent this altogether. The configuration for the SIP user now includes a new parameter that controls this. You can allow unrestricted registration over the WAN, via VPN only, or you can prohibit this altogether.

Additional security for the registration is provided by a count of the number of times that a SIP user authenticates incorrectly. Once the counter reaches a threshold value, the device locks the SIP user's account for a certain time. During

this period the SIP user cannot log on to the Voice Call Manager. You can freely set the values for the threshold and the duration of the lock.

1.7.2 Additions to the Setup menu

Access from WAN

This item determines whether and how SIP clients can register via a WAN connection.

SNMP ID:

2.33.3.1.1.8

Telnet path:

Setup > Voice-Call-Manager > Users > SIP-User > Users

Possible values:

Yes

No

VPN

Default:

Yes

Lock minutes

Determines for how many minutes a SIP user will be blocked after authentication has failed due to incorrect login data.

SNMP ID:

233.2.17

Telnet path:

Setup > Voice-Call-Manager > General > Lock-Minutes

Possible values:

0 to 255 minutes

Special values:

0: Lock off

Default:

5

Login errors

This value specifies the number of failed attempts before a SIP user is locked for a certain time.

SNMP ID:

233.2.18

Telnet path:**Setup > Voice-Call-Manager > General > Login-Errors****Possible values:**

0 to 255

Special values:

0: The first false login triggers the lock.

Default:

5

1.7.3 Additions to the Status menu

Local register

This column indicates whether the individual SIP users are registered locally, not registered, incorrectly authenticated or blocked.

SNMP ID:

153.3.6

Telnet path:**Status > Voice-Call-Manager > Users > Local-register****Possible values:**

Registered

Not-registered

Auth-failure

Blocked

Default:

Blank

Index

C

- Column headers [32](#)
- Columns [32](#)
- Custom Rollout Wizard
 - [32](#)
 - Attribute [32](#)
 - Fields [32](#)

D

- Device groups [24](#)

F

- File [15–16](#)

G

- Group [28](#)
- Group configuration [24](#), [28](#)
- Group configuration file [28](#)
- Grouping of devices [28](#)
- Group of devices [24](#)

M

- Managing many devices [24](#)
- Managing multiple devices [24](#)

W

- Working with the group configuration [28](#)