Addendum to LCOS version 8.50

The addendum describes the new functions and changes from LCOS version 8.50 and the previous version.

Contents:

1 LCOS

1.1 The commands LoadFirmware, LoadConfig, LoadScript and LoadFile

Various applications, such as loading configurations, firmware versions, scripts, and verifying server identity with certificates, require files to be stored to a device. You can to upload these files to a device with LANconfig or WEBconfig. Alternatively, you can use Telnet or SSH to issue a command from the command line to download the files directly from a server (TFTP, HTTP or HTTPS) and into the device. This process simplifies device administration in larger installations that rely on regular updates to the firmware and/or configurations.

The following commands are used to upload different file types to the device:

- LoadConfig: Uploads a configuration file (with file extension *.lcf) into the device.
- LoadFirmware: Uploads a firmware file (with file extension *.upx) into the device.
- LoadScript: Uploads a script (file extension *.lcs) to the device, e.g. for partial configurations.
- LoadFile: Uploads various types of file to the device.

The following descriptions use 'LoadCommand' to describe the upload commands in general.

The upload commands can use the protocols TFTP, HTTP and HTTPS to upload the selected file. A TFTP server is identical to an FTP server in terms of functionality, but uses a different protocol for data transmission. When using an HTTPS server, a certificate used to check the identity of the server can be stored on the device.

The LoadFile command in LCOS version 8.50 supports the protocols HTTP and HTTPS only.

The load commands are invoked from the command line interface with the following syntax:

```
LoadCommand <parameters>
```

The parameters are used to control the behavior of the commands. The parameters can be used in any combination. The only requirement is for a URL to be specified.

Values for condition, URL, or minimum version entered at the command line overwrite (once only) the values set under /Setup/Autoload/Network. Conversely, the values defined in the setup act to supplement the command-line commands if no parameters are entered manually.

General parameters for the load commands:

- -a: This parameter defines the sender address that the device sends to the server when downloading a file. Enter the sender address in one of the following forms:
  - Any valid IP address
  - INT for the address of the first intranet
  - DMZ for the address of the first DMZ
  - LB0 to LBF for the 16 loopback addresses

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

- <URL>: This parameter specifies the the URL for downloading a file from a TFTP or HTTP(S) server. Enter the URL in the following form:

  ```
  LoadCommand protocol://Server/Directory/Filename.ext
  ```

  For password-protected file access, enter the data in the following form:

  ```
  LoadCommand protocol://username:password@Server/Directory/
  Filename.ext
  ```

- -s: When downloading a file from a TFTP server, this parameter specifies its DNS name or IP address. Use this syntax as an alternative to specifying a URL.
- -f: When downloading a file from a TFTP server, this parameter specifies the name of the required file. Use this syntax as an alternative to specifying a URL.

If the parameters <URL> or -s and -f are not specified, the device executes the commands LoadFirmware, LoadConfig or LoadScript with the default values for the URL as defined under /Setup/Autoload/:

Use these default values if the latest configurations, scripts and firmware versions are always stored under the same name in the same location. If this is the case, the commands LoadConfig, LoadFirmware and LoadScript can be used very easily to load the relevant files automatically.

The following parameters are of particular importance for automatic uploading:

-Cn: This parameter checks if the file referenced by the LoadFirmware command is **newer** than the firmware on the device.

- -Cd: This parameter checks if the file referenced by the LoadFirmware, LoadConfig or LoadScript command is **different** to the firmware or configuration on the device, or newer than the last executed script. When the LoadScript command is used, this parameter updates the checksum stored in the device for the most recently executed script.
- -u: This parameter disables the version checking. The file referenced by the LoadFirmware, LoadConfig or LoadScript command is uploaded and executed unconditionally. When the LoadScript command is used, this parameter does not change the checksum stored in the device for the most recently executed script.
- -m: This value defines the minimum version of the firmware. The firmware referenced by the command must be at least of this version in order for the command LoadFirmware to execute.

The default setting for the conditions under /Setup/Autoload/Network are "Unconditionally". In the default setting, **no** version checking is carried out when the commands LoadFirmware and LoadConfig upload firmware, or when LoadScript executes a script file.

The parameter -u always has priority over other parameters entered in a command.

When transferring files from an HTTPS server to a client device, the network components check the identity of the remote site by using certificates. For the automatic loading from HTTPS servers, additional parameters are available for downloading and subsequently checking the certificates:

- -o <Path/Filename.ext>: This parameter specifies the destination when downloading a file from an HTTP(S) server with the LoadFile command. For example, you can use this option to save a certificate on your device for future identity verification when accessing an HTTPS server.
- -c <Path/Filename.ext>: This parameter specifies the name of the certificate used by the device to check the identity of an HTTPS server when downloading a file.
- -p <Path/Filename.ext>: When downloading a file from an HTTPS server, this parameter specifies the name of the PKCS#12 container. The PKCS#12 container can contain multiple CA certificates, and thus supports the identity checking of HTTPS servers with certificate chains. A PKCS#12 container can additionally contain a device certificate and the corresponding private key, so that it can confirm the identity of the device to the HTTPS server if this server requires authentication by certificate.
- -d: The device uses this passphrase to encrypt an unencrypted PKCS#12 container.
- -n: This parameter disables the server-name check when downloading a file from an HTTPS server using the LoadFile command. If you use the download URL to specify the server as a DNS name (and not as an IP address), then the device additionally communicates the server name when sending its request to the server. If the HTTPS server is a virtual server, then this server can respond with the appropriate certificates for the reported DNS name. Without this parameter, the device checks whether the DNS name in the download URL agrees with the common name of the submitted certificates. The unit will start the download only if this check is successful.

Use one of the two following notations to specify a file in the file system of the device:

- Specify a location in the device's internal file system with the path '/minifs/filename.ext'.
- Specify a location on an external USB data medium with the path '/mountpoint/directory/filename.ext'. The available mount points are listed under '/status/file-system/volumes'.

In file names that include the path, you can use the following general variables:

- `%m`: The LAN MAC address of the device (hexadecimal, lowercase letters, no separators)
- `%s`: The device serial number.
- `%n`: The device name
- `%l`: The location of the device ('location' – from the configuration)
- `%d`: The device type

ⓘ You can use these variables in the load commands, but you cannot change the values for the variables.

In addition to these general variables, you can also use the following environment variables that relate to the device for more flexibility when executing the load commands. All predefined environment variables begin with two underscores: When entering commands on the command line, the variables are preceded by a dollar sign.

- `__BLDDEVICE`: The sub-project of the device. This environment variable stands for the second part of the value for `PROJECT` if you execute the command `#sysinfo#` from the command line. The sub-project generally consists of a string without spaces and it stands for the hardware model of the current device.
- `__DEVICE`: The type of the device, for example as displayed in LANconfig or on the device type label.
- `__FWBUILD`: The build number of the firmware currently used in the device. The build number is a number
- `__FWVERSION`: The version number of the firmware currently used in the device, in the form 'x.yy'. The firmware version consists of the major release before the dot and the minor release after it.
- `__LDRBUILD`: The build number of the firmware currently operating in the device. The build number is a four-digit number.
- When requested for the loader build number, older loaders return an empty string.

- `__LDRVERSION`: The version number of the loader currently installed in the device, in the form 'x.yy'. The loader version consists of the major release before the dot and the minor release after it.
- `__MACADDRESS`: The type of the device, given as a 12-digit string of hexadecimal values with lowercase letters and no separators.
- `__SERIALNO`: The device serial number.
- `__SYSNAME`: The system name of the device.

ⓘ If you have already used a name from the environment variables as a user-defined variable in a section of the configuration, then both the configuration and the commands on the command line work primarily with the values of the user-defined variables.

Use the following commands in the CLI to display or modify the environment variables:

- `printenv`: Displays all environment variables and their current values. If you have set one or more environment variables with the command `setenv`, the output of the command `printenv` shows the user-defined value at the top and the default value below it.
- `echo __device`: Displays the current values of a single environment variable, in this example the value for the variable '__DEVICE'.
- `setenv __device MeinWert`: Sets the value of an environment variable to the desired value.
- `unsetenv __device`: Sets the value of an environment variable to the default value.

Examples of load commands:

- With the following Telnet command, the device loads a firmware file named 'LC-1811-5.00.0019.upx' into the device from directory 'LCOS/850' on the TFTP server with IP address '192.168.2.200':

  ```
  LoadFirmware -s 192.168.2.200 -f LCOS/850/LC-1811-8.50.0019.upx
  ```

- With the following Telnet command, the device loads a script intended for a certain MAC-address (named, for example, '00a0571735da.lcs') from the TFTP server with IP address '192.168.2.200':

  ```
  LoadScript -s 192.168.2.200 -f %m.lcs
  ```

- With the following Telnet command, the device loads a firmware file named 'LC-1811-5.00.0019.upx' into the device from directory 'download' on the HTTP server 'www.myserver.com'. At the same time the identity of the server is checked with the certificate 'sslroot.crt':

  ```
  LoadFirmware -c sslroot.crt https://www.myserver.com/download/LC-
  1811-8.50.0019.upx
  ```

- With the following Telnet command, the device loads a script intended for the specified serial number and the current firmware. The device reads the values for serial number and firmware from the corresponding environment variables:

  ```
  Loadscript $__SERIALNO-$__FWVERSION.lcs
  ```

1.1.1 Example applications

Regularly updating configuration and firmware

This scenario describes how to regularly update the configuration and the firmware of a device every 24 hours.

Requirements:

- The device is currently equipped with firmware version '8.30' and a corresponding configuration.
- The HTTP server contains the new firmware version in the form of a file 'LCOS.upx' and the corresponding configuration in the form of a file 'LCOS.lcs'.

Configuration:

1. Specify the path that the 'LoadFirmware' command uses to source the upload if no other parameters are available. For example, enter the following command to load the firmware from an HTTP server:

   ```
   set /setup/Setup/Autoload/Network/Firmware/URL http://
   www.mycompany.de/firmware/LCOS.upx
   ```

2. Set the conditions for loading the firmware such that only firmware that is newer than that in the device is loaded:

   ```
   set /Setup/Autoload/Network/Firmware/Condition if-newer
   ```

3. Specify the path that the 'LoadConfig' command uses to source the upload if no other parameters are available. For example, enter the following command to load the configuration from an HTTP server:

   ```
   set /setup/Setup/Autoload/Network/Firmware/URL http://
   www.mycompany.de/configuration/LCOS.lcf
   ```

4. Set the conditions for loading the configuration such that only a configuration that is different from that in the device is loaded:

   ```
   set /Setup/Autoload/Network/Config/Condition if-different
   ```

5. Create a cron job that regularly runs the command 'LoadFirmware' at 23:55h:

   ```
   cd /Setup/Config/Cron-Table
   set 1 * * * 55 23 * * * LoadFirmware
   ```

6. Create a cron job that regularly runs the command 'LoadConfig' at 23:59h:

   ```
   set 2 * * * 59 23 * * * LoadConfig
   ```

Update configuration after first updating firmware

This scenario describes a potential situation within a project whereby a firmware update is to be carried out followed by an update of the configuration by script.

Requirements:

- The device is currently equipped with firmware version '8.30' and a corresponding configuration.
- The HTTP server contains the new firmware version in the form of a file 'LCOS-850.upx' and the corresponding configuration in the form of a file '<Serial number>-850.lcs'.

! In this scenario, the configuration script is only to be applied once the device has been equipped with the appropriate firmware.

Configuration:

1. Specify the path that the 'LoadFirmware' command uses to source the upload if no other parameters are available. For example, enter the following command to load the firmware from an HTTP server:

   ```
   set /setup/Setup/Autoload/Network/Firmware/URL http://
   www.mycompany.de/firmware
   ```

2. Set the conditions for loading the firmware such that only firmware that is newer than that in the device is loaded:

   ```
   set /Setup/Autoload/Network/Firmware/Condition if-newer
   ```

3. Specify the path that the 'LoadConfig' command uses to source the upload if no other parameters are available. For example, enter the following command to load the configuration from an HTTP server:

   ```
   set /setup/Setup/Autoload/Network/Firmware/URL http://
   www.mycompany.de/configuration
   ```

4. Set the conditions for loading the configuration such that only a configuration that is different from that in the device is loaded:

   ```
   set /Setup/Autoload/Network/Config/Condition if-different
   ```

5. Create a cron job that regularly runs the command 'LoadFIRMWARE' every 10 minutes:

   ```
   cd /Setup/Config/Cron-Table
   set 1 * * * 10 * * * * LoadFirmware
   ```

6. Create a cron job that regularly runs the command 'LoadScript' every 10 minutes:

   ```
   set 2 * * * 10 * * * * LoadScript\ $__SERIALNO-$__FWVERSION.lcs
   ```

The result:

With this configuration, the device always initially loads the latest firmware.

If the device executes the command 'LoadScript' after initially uploading the firmware and configuration script from the HTTP server, then the environment variable '__FWVERSION' is set with the value '8 .30 ' at this time. The command `LoadScript\ $__SERIALNO-$__FWVERSION.lcs` does not find a suitable configuration script at this time. The device then executes the command `LoadFirmware LCOS.upx` and after rebooting, the environment variable '__FWVERSION' is set to the value '8.50 '. The command `LoadScript\ $__SERIALNO-$__FWVERSION.lcs` then finds a suitable script to update the configuration. In the cron command `Loadscript\ $__SERIALNO-$__FWVERSION.lcs`, the space between the load script command and the environment variables is protected with a backslash. Trying to use the alternative notation of enclosing the entire command in quotation marks will result in an error. LCOS treats environment variables in quotation marks as normal text, so the any variables would be ignored.

1.2 Enhanced Sysinfo

To determine whether changes have been made to the configuration, and to find the time/date when a change was made, Sysinfo contains additional entries in the field CONFIG_STATUS.

The devices store the value CONFIG_STATUS each time a change is made to the configuration (via the command line, via SNMP or by loading a script or complete configurations).The value CONFIG_STATUS consists of the following components:

- Hash value of the device configuration as a unique identifier of configuration status.
- Timestamp of the last change to the configuration in the format HHMMSSddmmyyyy based on Coordinated Universal Time UTC. The reference to UTC guarantees unique values without being influenced by time zone or daylight-saving settings.
- Counter of configuration changes, sequential.

The field CONFIG_STATUS contains, along with a value for the configuration status switches and a value for the configuration flash status, the additional components in the form <Hash>.<Date>.<Counter>.

Changes to the configuration can be implemented in the appropriate files or scripts (e.g. with LCMS) or on the devices directly (by command line or WEBconfig). The content of CONFIG_STATUS is influenced by the method by which configuration changes are made.

The device configuration hash value

Hash values are calculated solely by LCOS, the operating system used by the devices. The hash value differs for every state of configuration, and a modified hash value indicates that a device configuration has been changed.

LCOS stores the calculated hash value to the device during the flash process.

Timestamp of the last configuration change

Both LCOS and LCMS can set the timestamp, assuming that they have a valid time.

If the chosen method of configuration does not have a valid time, the device sets the timestamp to the value '00: 00:00 0000-00-00'.

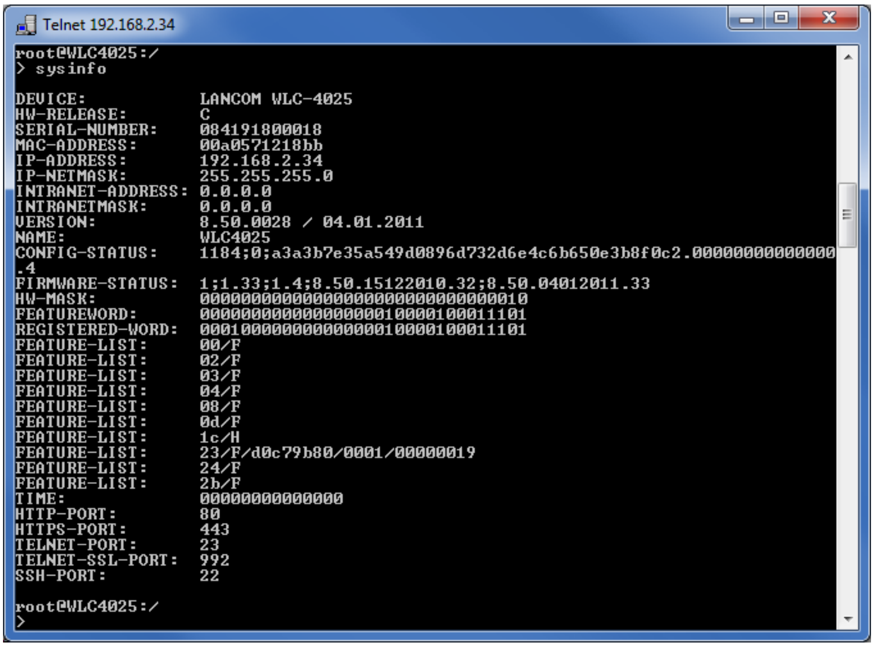
Configuration changes counter

When the devices are shipped, the counter of configuration changes is set to '0'. Every configuration change after this increases the value by 1. The configuration-changes counter allows changes to the current version of the configuration to be determined, even if no valid time of configuration was available and the timestamp is therefore set to '00: 00:00 0000-00-00'.

A configuration counter that shows '0' after changes have been made to the configuration indicates an error while reading or writing the counter during flashing.

Displaying CONFIG_STATUS

To display the value for CONFIG_STATUS, enter the command `sysinfo` on the command line for the device.



```
root@WLC4025:/
> sysinfo

DEVICE:            LANCOM WLC-4025
HW-RELEASE:        C
SERIAL-NUMBER:     084191800018
MAC-ADDRESS:       00a0571218bb
IP-ADDRESS:        192.168.2.34
IP-NETMASK:        255.255.255.0
INTRANET-ADDRESS:  0.0.0.0
INTRANETMASK:      0.0.0.0
VERSION:           8.50.0028 / 04.01.2011
NAME:              WLC4025
CONFIG-STATUS:     1184;0;a3a3b7e35a549d0896d732d6e4c6b650e3b8f0c2.00000000000000
.4
FIRMWARE-STATUS:   1;1.33;1.4;8.50.15122010.32;8.50.04012011.33
HW-MASK:           00000000000000000000000000000010
FEATUREWORD:       00000000000000000010000100011101
REGISTERED-WORD:   00010000000000000010000100011101
FEATURE-LIST:      00/F
FEATURE-LIST:      02/F
FEATURE-LIST:      03/F
FEATURE-LIST:      04/F
FEATURE-LIST:      08/F
FEATURE-LIST:      0d/F
FEATURE-LIST:      1c/H
FEATURE-LIST:      23/F/d0c79b80/0001/00000019
FEATURE-LIST:      24/F
FEATURE-LIST:      2b/F
TIME:              00000000000000
HTTP-PORT:         80
HTTPS-PORT:        443
TELNET-PORT:       23
TELNET-SSL-PORT:   992
SSH-PORT:          22

root@WLC4025:/
>
```

Picture 1: “Displaying system information on the command line”

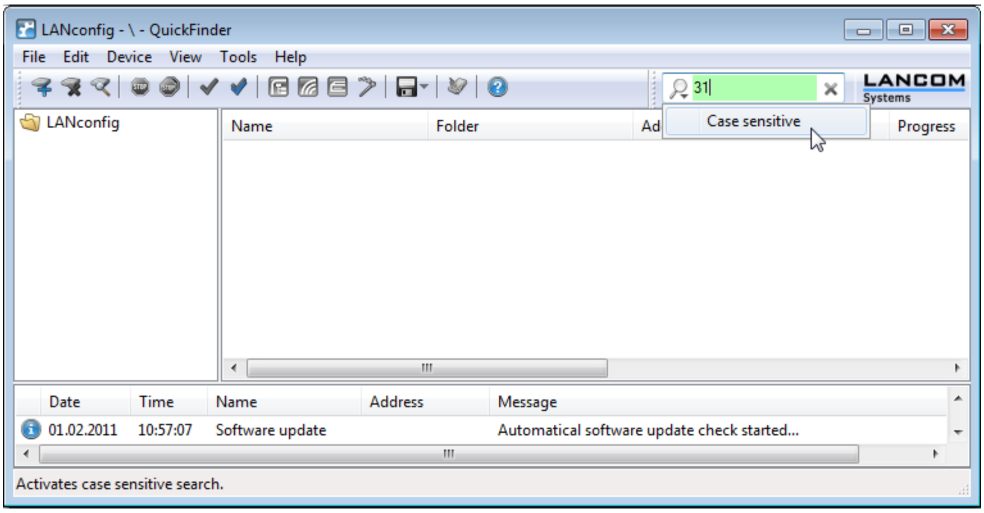
2 LCMS

2.1 LANCOM QuickFinder

The configuration dialogs in LANconfig, LANmonitor and WLANmonitor include numerous sections, parameters and their values, as well as tables.

LANCOM QuickFinder in LANconfig

In the main view of LANconfig you will find the LANCOM QuickFinder in the toolbar. Entering a search term in the search window reduces the number of available devices in the list. LANconfig searches through all the values available in the columns in the device list, including any hidden columns. Click on the icon next to the magnifying glass to make the search case sensitive.



Date	Time	Name	Address	Message
01.02.2011	10:57:07	Software update		Automatical software update check started...

Activates case sensitive search.

If you are looking for a particular value or term in LANconfig or in the configuration, LANCOM QuickFinder quickly displays all of the locations where the string occurs in the LANconfig dialogs. For example, your configuration may contain settings for your Internet provider. To find these you just have to enter the name to find all of the places in the configuration that refer to this provider.

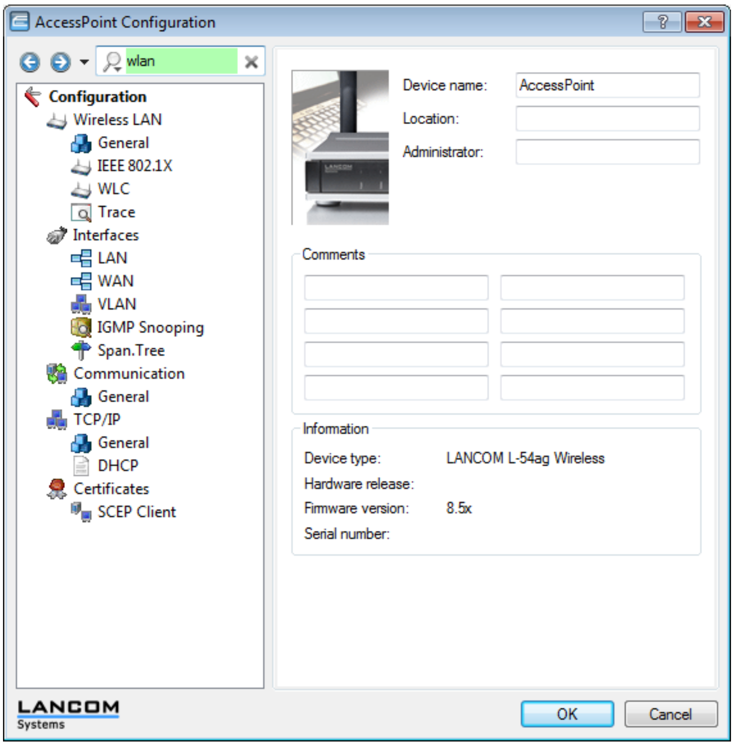
You can search for text from the following areas:

- Entries in the configuration tree
- Names of the sections in each configuration dialog
- Parameters
- Values of the parameters
- Explanatory texts in the dialogs
- Table names
- Column names in tables

To use the search in LANconfig proceed as follows:

1. Start LANconfig.
2. Open the device configuration that you want to search through.
3. In the search box, type the phrase that you are looking for (e.g. 'wlan'). Searching is not case-sensitive. You can enter parts of words or numbers, as well as complete strings. If there are spaces in the search string, then only strings containing the matching spaces will be searched for. The search function does not support wildcards.

The configuration tree in the left pane of LANconfig is now reduced to just those sections that feature the search string:



Device name: AccessPoint

Location:

Administrator:

Comments

Information

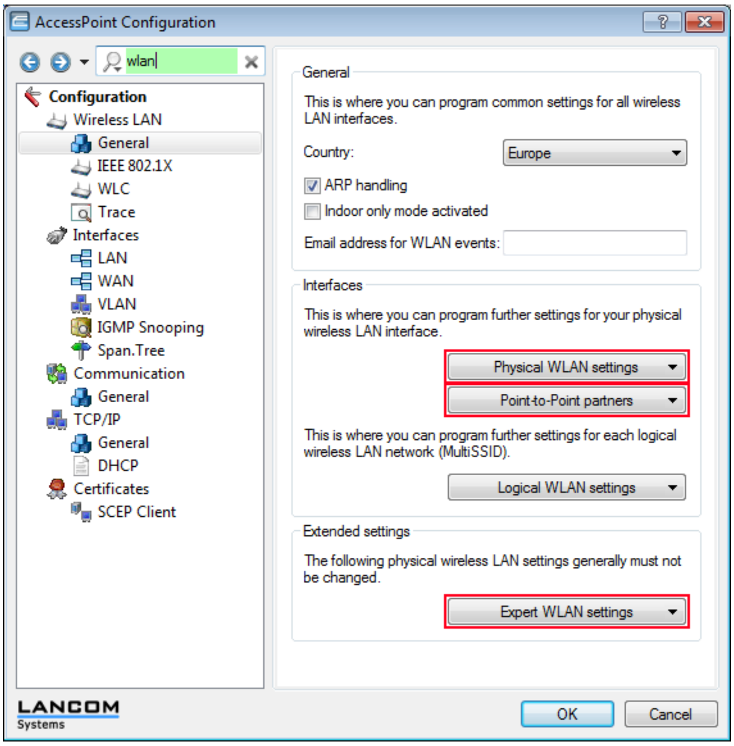
Device type: LANCOM L-54ag Wireless

Hardware release:

Firmware version: 8.5x

Serial number:

Select an area in the configuration (e.g. 'WLAN/General') to view the relevant search results framed in color in the configuration dialog:



General

This is where you can program common settings for all wireless LAN interfaces.

Country: Europe

☑ ARP handling

☐ Indoor only mode activated

Email address for WLAN events:

Interfaces

This is where you can program further settings for your physical wireless LAN interface.

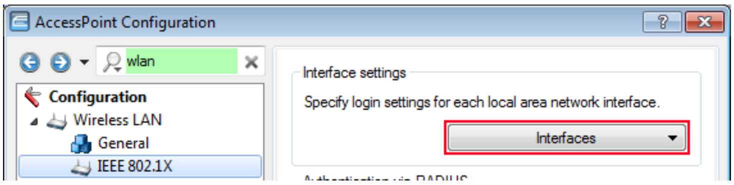
This is where you can program further settings for each logical wireless LAN network (MultiSSID).

Extended settings

The following physical wireless LAN settings generally must not be changed.

In LANconfig version 8.50, the search results in the firewall section are not displayed in color.

Use the navigation buttons 'forwards' and 'back' to move between the most recently visited dialogs:

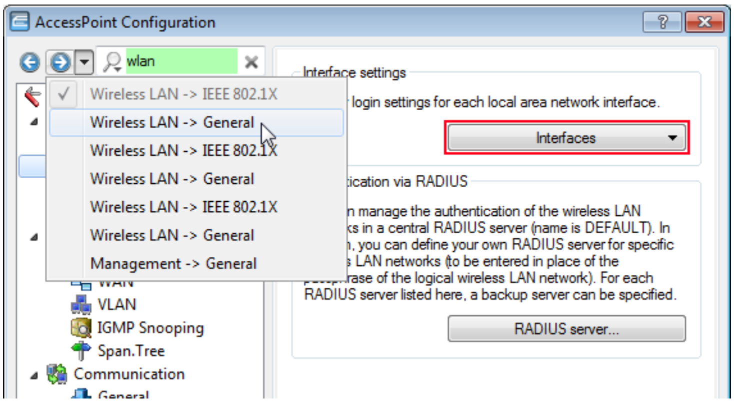


Interface settings

Specify login settings for each local area network interface.

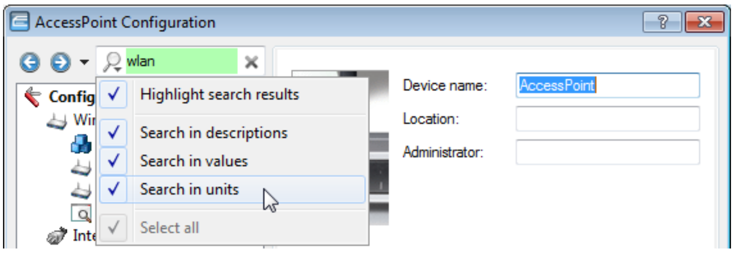
Authentication via RADIUS

For quick access to the last 10 visited dialogs, click on the arrow to the right of the 'forwards' button:


AccessPoint Configuration
wlan
Wireless LAN -> IEEE 802.1X
Wireless LAN -> General
Wireless LAN -> IEEE 802.1X
Wireless LAN -> General
Wireless LAN -> IEEE 802.1X
Wireless LAN -> General
Management -> General
WAN
VLAN
IGMP Snooping
Span.Tree
Communication
General
Interface settings
login settings for each local area network interface.
Interfaces
ication via RADIUS
n manage the authentication of the wireless LAN
s in a central RADIUS server (name is DEFAULT). In
, you can define your own RADIUS server for specific
LAN networks (to be entered in place of the
rase of the logical wireless LAN network). For each
RADIUS server listed here, a backup server can be specified.
RADIUS server...

Click on the 'x' to the right of the search box to clear the search and display all entries in the configuration again.

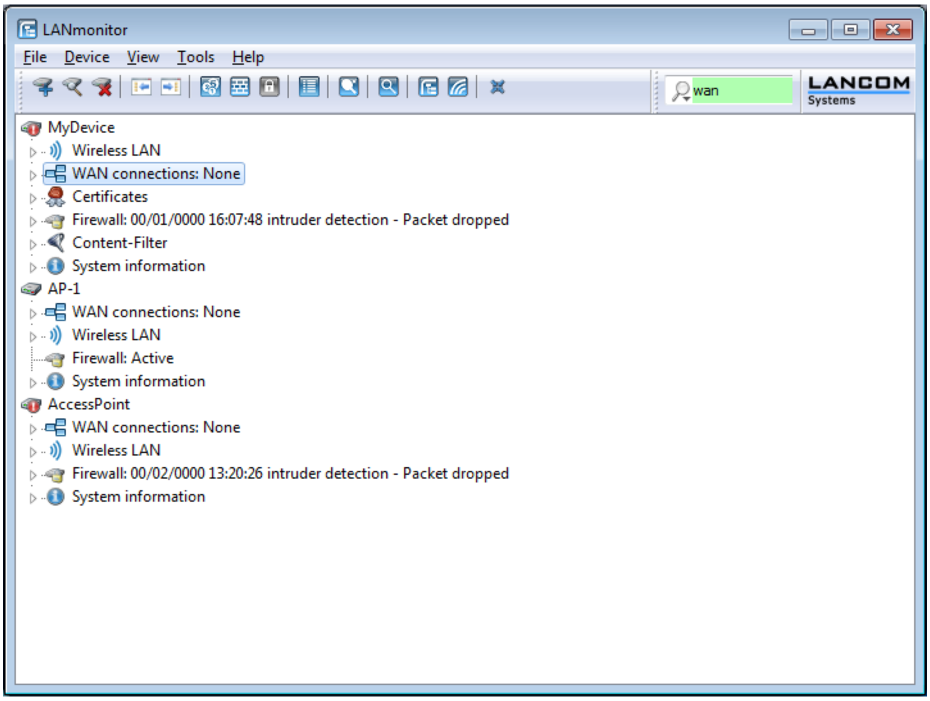
An option to reduce the number of search results is to select the sections where LANconfig should limit the search to. Click on the magnifying glass to the left of the search box and select or deselect the required categories. Here you can also specify whether the search should highlight the results in color, or whether the configuration tree is to be reduced to the relevant dialogs only:



LANconfig resets the search settings and the list of recent dialogs when the configuration is closed.

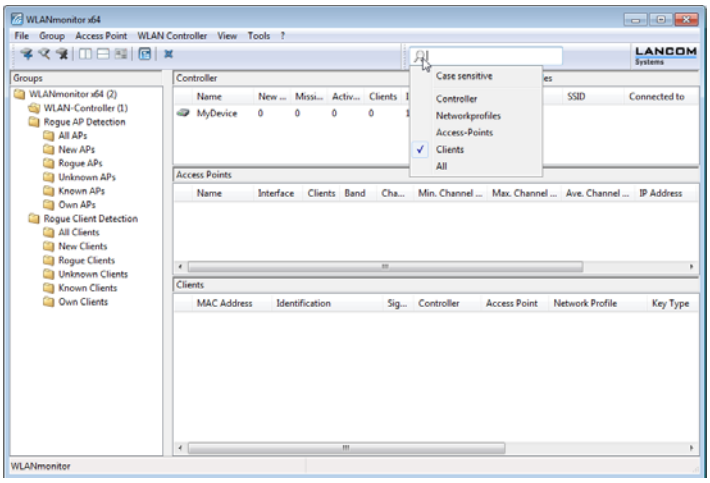
LANCOM QuickFinder in LANmonitor

Depending on the application, LANmonitor can display multiple devices with entries containing the searched term. After starting the search LANmonitor initially highlights the first finding. You can move between the search results either by using the arrow keys to the right of the search window, or by pressing Ctrl+F3 for the next occurrence and Ctrl+Shift+F3 to the previous occurrence.



LANCOM QuickFinder in WLANmonitor

WLANmonitor includes access points and WLAN clients. Clicking on the magnifying glass on the left side of the search window opens a context menu to select the type of search. Depending on the application you can search for access points only, clients only, or all entries.



2.2 Tracing with LANconfig and LANmonitor

Traces can be executed very easily with LANconfig or LANmonitor. Simply click on the entry for the device with the right-hand mouse key and select Traces from the context menu.

Telnet-access to the device must be enabled to carry out trace requests with LANconfig or LANmonitor. When starting the trace dialog, LANconfig or LANmonitor first attempts to establish an SSL-encrypted Telnet connection to the device. If the device does not support SSL connections, LANconfig or LANmonitor automatically switches to unencrypted Telnet. If access to the device configuration is password-protected, the access data for an administrator with trace rights is also required.

2.2.1 Introduction

The trace function in LANconfig and LANmonitor exceeds the standard trace functions available from Telnet and offers greater convenience in the generation and analysis of traces.For example, the current trace configuration for activating the necessary trace commands can be stored to a configuration file. An experienced service technician can set up a trace configuration and provide it to a less experienced user for executing specialized trace requests for a device. The trace results can also be stored in a file and returned to the technician for analysis.

To open the trace window for a device, right-click the device entry in LANconfig or LANmonitor and select “Traces” from the context menu.

LANmonitor has the following buttons for operating the trace module:

Opens a pre-defined configuration for the trace command. This allows you to carry out trace commands precisely as required by the service technician, for example.

Stores the current trace configuration to be passed on to a user.

Clears the current display or trace results.

▶

Starts outputting the trace results as produced by the current configuration and automatically switches to the trace-result display mode. As soon as the trace results are returned, the other buttons are deactivated.

STOP

Stops the output of trace results.

Switches to the mode for configuring the trace output.

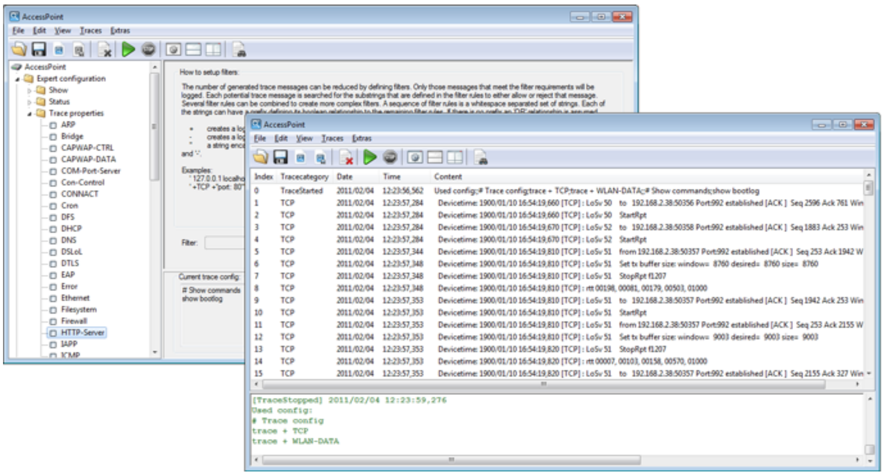
Switches to the mode for displaying the trace output.

Switches to the split-screen mode to display the trace results in two parallel windows.

Opens the window to search through the trace results.

Starts the time-stamp based synchronization of the two traces in the split-screen display.

Stops the synchronization of the two traces in the split-screen display.



How to setup filters:

The number of generated trace messages can be reduced by defining filters. Only those messages that meet the filter requirements will be logged. Each potential trace message is searched for the substrings that are defined in the filter rules to either allow or reject that message. Several filter rules can be combined to create more complex filters. A sequence of filter rules is a whitespace separated set of strings. Each of the strings can have a prefix defining its boolean relationship to the remaining filter rules. If there is no prefix an 'OR' relationship is assumed.

- creates a lo
- creates a lo
- a string enc

and '-'.

Examples:
'127.0.0.1 localho
'+TCP +'port: 80'

# Show commands
show bootlog

Index	Tracecategory	Date	Time	Content
0	TraceStarted	2011/02/04	12:23:56,562	Used config:;# Trace config;trace + TCP;trace + WLAN-DATA;;# Show commands;show bootlog
1	TCP	2011/02/04	12:23:57,284	Devicetime: 1900/01/10 16:54:19,660 [TCP] : LoSv 50 to 192.168.2.38:50356 Port:992 established [ACK] Seq 2596 Ack 761 Win
2	TCP	2011/02/04	12:23:57,284	Devicetime: 1900/01/10 16:54:19,660 [TCP] : LoSv 50 StartRpt
3	TCP	2011/02/04	12:23:57,284	Devicetime: 1900/01/10 16:54:19,670 [TCP] : LoSv 52 to 192.168.2.38:50358 Port:992 established [ACK] Seq 1883 Ack 253 Win
4	TCP	2011/02/04	12:23:57,284	Devicetime: 1900/01/10 16:54:19,670 [TCP] : LoSv 52 StartRpt
5	TCP	2011/02/04	12:23:57,344	Devicetime: 1900/01/10 16:54:19,810 [TCP] : LoSv 51 from 192.168.2.38:50357 Port:992 established [ACK] Seq 253 Ack 1942 W
6	TCP	2011/02/04	12:23:57,348	Devicetime: 1900/01/10 16:54:19,810 [TCP] : LoSv 51 Set tx buffer size: window= 8760 desired= 8760 size= 8760
7	TCP	2011/02/04	12:23:57,348	Devicetime: 1900/01/10 16:54:19,810 [TCP] : LoSv 51 StopRpt f1207
8	TCP	2011/02/04	12:23:57,348	Devicetime: 1900/01/10 16:54:19,810 [TCP] : rtt 00198, 00081, 00179, 00503, 01000
9	TCP	2011/02/04	12:23:57,353	Devicetime: 1900/01/10 16:54:19,810 [TCP] : LoSv 51 to 192.168.2.38:50357 Port:992 established [ACK] Seq 1942 Ack 253 Win
10	TCP	2011/02/04	12:23:57,353	Devicetime: 1900/01/10 16:54:19,810 [TCP] : LoSv 51 StartRpt
11	TCP	2011/02/04	12:23:57,353	Devicetime: 1900/01/10 16:54:19,810 [TCP] : LoSv 51 from 192.168.2.38:50357 Port:992 established [ACK] Seq 253 Ack 2155 W
12	TCP	2011/02/04	12:23:57,353	Devicetime: 1900/01/10 16:54:19,810 [TCP] : LoSv 51 Set tx buffer size: window= 9003 desired= 9003 size= 9003
13	TCP	2011/02/04	12:23:57,353	Devicetime: 1900/01/10 16:54:19,820 [TCP] : LoSv 51 StopRpt f1207
14	TCP	2011/02/04	12:23:57,353	Devicetime: 1900/01/10 16:54:19,820 [TCP] : rtt 00007, 00103, 00158, 00570, 01000
15	TCP	2011/02/04	12:23:57,353	Devicetime: 1900/01/10 16:54:19,820 [TCP] : LoSv 51 to 192.168.2.38:50357 Port:992 established [ACK] Seq 2155 Ack 327 Win

```
[TraceStopped] 2011/02/04 12:23:59,276
Used config:
# Trace config
trace + TCP
trace + WLAN-DATA
```

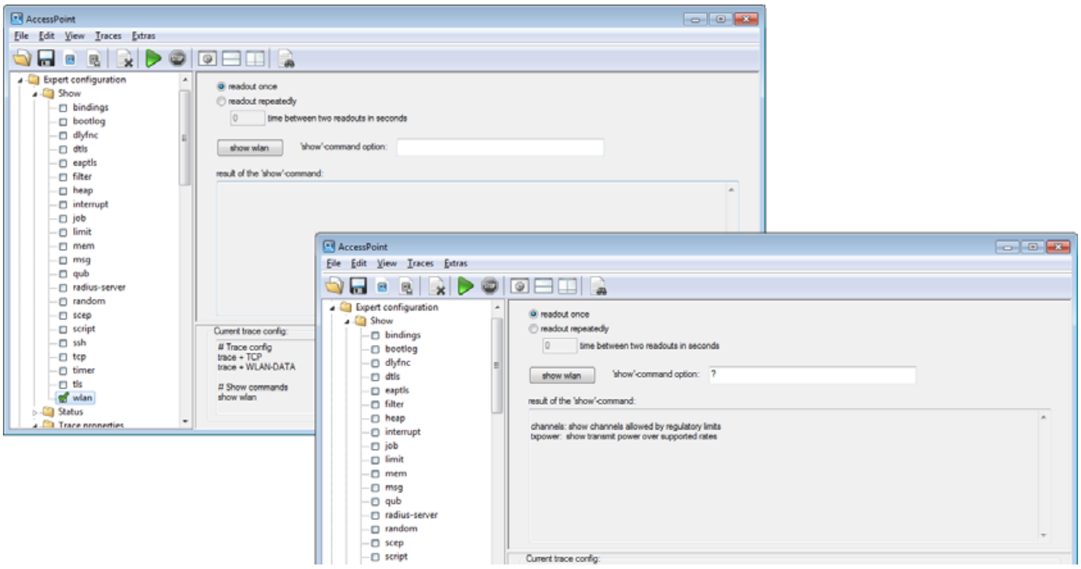
2.2.2 Expert configuration of the trace dumps

Going beyond the settings of the Wizard, traces and other displays can be set up precisely using the Expert Configuration. The Expert Configuration is divided into three areas:

Show

Particular information can be retrieved for every device type using a Show command. Show commands are usually used on the command line (Telnet).The call of this Show command is very convenient from the graphical Windows interface in the advanced configuration of the trace. To access the current dump of the Show command, click the name of a Show command in the left-hand area of the trace dialog and then the Show button. You may have to/be able to specify additional parameters depending on the entry selected. Enter a question mark in the input field and then click the Show button for information on these parameters. To accept the dump of the Show command into the trace data, click the appropriate checkbox to the left of the entry name. For every Show command enabled, it is possible to set whether it is only run once on start of the trace or whether it is run at regular intervals (set in seconds).

The settings of the Show commands are stored in the trace configuration together with the actual trace settings.



● readout once
○ readout repeatedly
0 time between two readouts in seconds
'show'-command option:
result of the 'show'-command:

Current trace config:

```
# Trace config
trace + TCP
trace + WLAN-DATA

# Show commands
show wlan
```

● readout once
○ readout repeatedly
0 time between two readouts in seconds
'show'-command option: ?
result of the 'show'-command:

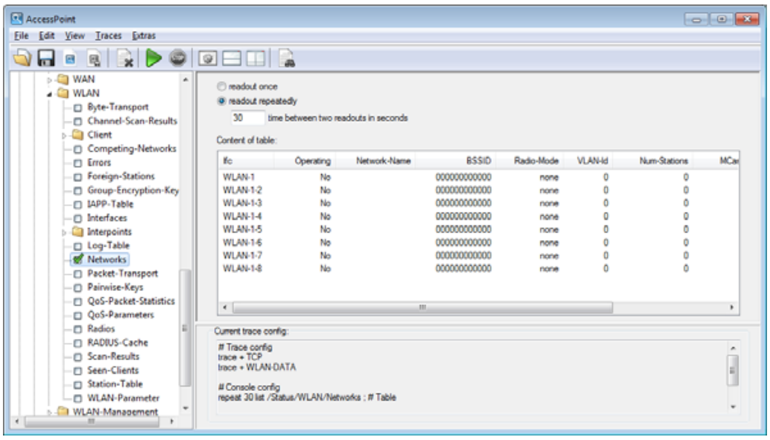
```
channels: show channels allowed by regulatory limits
txpower:  show transmit power over supported rates
```

Current trace config:

Status

Comprehensive status information and statistics on a device can be accessed from the command line (Telnet) or via WEBconfig. All available status information can also be shown via the trace dialog. Tables and individual values are shown using special icons. To display the current contents of the table or value, click the name of a status entry in the left-hand area of the trace dialogue. To accept the dump of the Status entry into the trace data, click the appropriate checkbox to the left of the entry name. For every Status entry enabled, a setting defines whether it is read out once only on starting the trace or whether it is read out at regular intervals (set in seconds).

The settings of the Status information are stored in the trace configuration together with the actual trace settings. Status information is stored together with the actual trace data.



○ readout once
● readout repeatedly
30 time between two readouts in seconds

Content of table:

Ifc	Operating	Network-Name	BSSID	Radio-Mode	VLAN-Id	Num-Stations	MCa
WLAN-1	No		000000000000	none	0	0	
WLAN-1-2	No		000000000000	none	0	0	
WLAN-1-3	No		000000000000	none	0	0	
WLAN-1-4	No		000000000000	none	0	0	
WLAN-1-5	No		000000000000	none	0	0	
WLAN-1-6	No		000000000000	none	0	0	
WLAN-1-7	No		000000000000	none	0	0	
WLAN-1-8	No		000000000000	none	0	0	

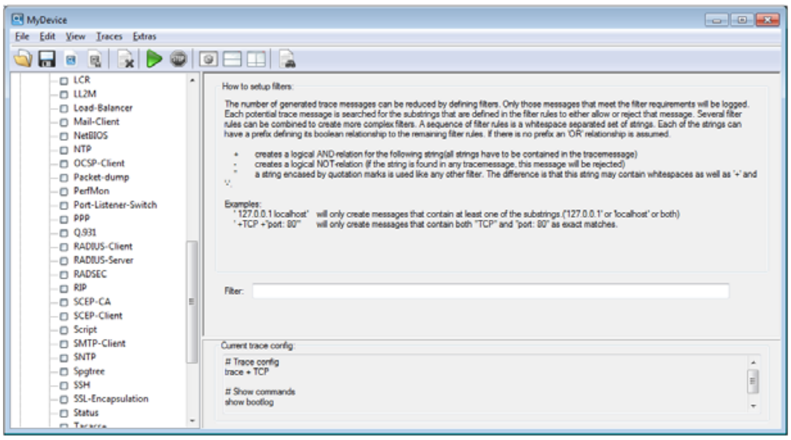
Current trace config:

```
# Trace config
trace + TCP
trace + WLAN-DATA

# Console config
repeat 30 ls /Status/WLAN/Networks ; # Table
```

Trace settings

The traces to be dumped for the current device can be enabled in the trace settings area.To include the trace commands into the trace results, click the appropriate checkbox to the left of the entry name. A filter can be entered for every trace.For example, if you want to display only the IP traces of a particular workstation, enter the appropriate IP address as a filter of the IP router trace.



How to setup filters:

The number of generated trace messages can be reduced by defining filters. Only those messages that meet the filter requirements will be logged. Each potential trace message is searched for the substrings that are defined in the filter rules to either allow or reject that message. Several filter rules can be combined to create more complex filters. A sequence of filter rules is a whitespace separated set of strings. Each of the strings can have a prefix defining its boolean relationship to the remaining filter rules. If there is no prefix an 'OR' relationship is assumed.

+ creates a logical AND-relation for the following string(all strings have to be contained in the tracemessage)
- creates a logical NOT-relation (if the string is found in any tracemessage, this message will be rejected)
" a string encased by quotation marks is used like any other filter. The difference is that this string may contain whitespaces as well as '+' and '-'.

Examples:
' 127.0.0.1 localhost' will only create messages that contain at least one of the substrings ('127.0.0.1' or 'localhost' or both)
' +TCP +"port: 80"' will only create messages that contain both "TCP" and "port: 80" as exact matches.

Filter:

Current trace config:

```
# Trace config
trace + TCP

# Show commands
show bootlog
```

2.2.3 Display of the trace results

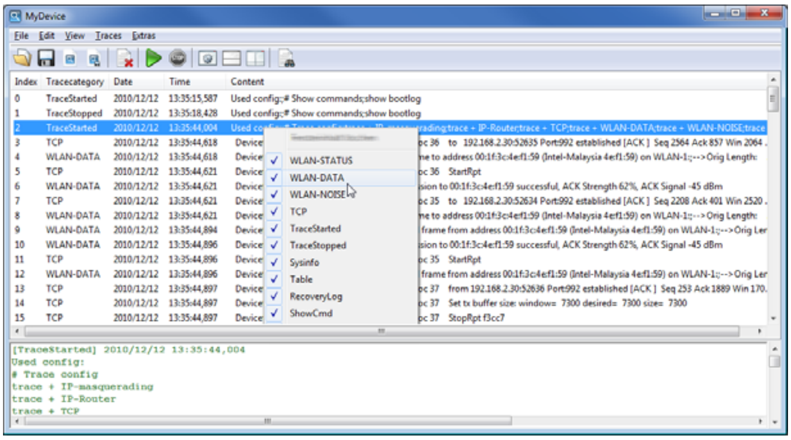
The entire trace configuration is shown in the lower area of the dialog where all active Trace, Status and Show entries are listed with the respective filters and parameters.

To start the dump of the trace data, change to Display mode with the Start button. The ongoing trace dumps are displayed in this view:

- The upper section lists the results for the executed trace commands chronologically line by line.
- Since the results for a single trace command can be very long, the lower section shows a more detailed breakdown of the result selected in the upper section.

For easier navigation within long trace dumps, click a trace event in the upper area. The appropriate result is then enabled in the list and highlighted in the lower section in green. Right-clicking a trace event opens up a context menu from where individual trace results can be shown/hidden.

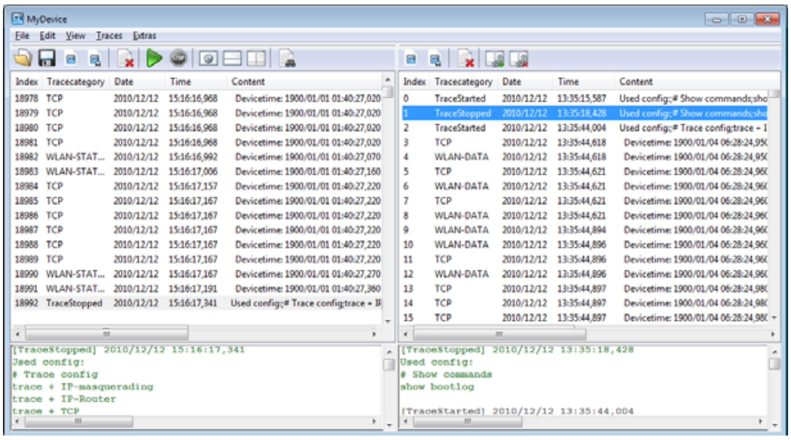
Trace data is collected as long as the trace dump is enabled. To prevent overloading the main workstation memory using LANconfig or LANmonitor, trace data is automatically written to a backup file. The time intervals and the maximum size of a backup file can be set with 'Extras > Other Settings > Trace backup'.



Index	Tracecategory	Date	Time	Content
0	TraceStarted	2010/12/12	13:35:15,587	Used config;# Show commands;show bootlog
1	TraceStopped	2010/12/12	13:35:18,428	Used config;# Show commands;show bootlog
2	TraceStarted	2010/12/12	13:35:44,004	Used co rading;trace + IP-Router;trace + TCP;trace + WLAN-DATA;trace + WLAN-NOISE;trace
3	TCP	2010/12/12	13:35:44,618	Device pc 36 to 192.168.2.30:52635 Port:992 established [ACK] Seq 2564 Ack 857 Win 2064 .
4	WLAN-DATA	2010/12/12	13:35:44,618	Device ne to address 00:1f:3c:4e:f1:59 (Intel-Malaysia 4e:f1:59) on WLAN-1:;--> Orig Length:
5	TCP	2010/12/12	13:35:44,621	Device pc 36 StartRpt
6	WLAN-DATA	2010/12/12	13:35:44,621	Device sion to 00:1f:3c:4e:f1:59 successful, ACK Strength 62%, ACK Signal -45 dBm
7	TCP	2010/12/12	13:35:44,621	Device pc 35 to 192.168.2.30:52634 Port:992 established [ACK] Seq 2208 Ack 401 Win 2520 .
8	WLAN-DATA	2010/12/12	13:35:44,621	Device ne to address 00:1f:3c:4e:f1:59 (Intel-Malaysia 4e:f1:59) on WLAN-1:;--> Orig Length:
9	WLAN-DATA	2010/12/12	13:35:44,894	Device frame from address 00:1f:3c:4e:f1:59 (Intel-Malaysia 4e:f1:59) on WLAN-1:;--> Orig Ler
10	WLAN-DATA	2010/12/12	13:35:44,896	Device sion to 00:1f:3c:4e:f1:59 successful, ACK Strength 62%, ACK Signal -45 dBm
11	TCP	2010/12/12	13:35:44,896	Device pc 35 StartRpt
12	WLAN-DATA	2010/12/12	13:35:44,896	Device frame from address 00:1f:3c:4e:f1:59 (Intel-Malaysia 4e:f1:59) on WLAN-1:;--> Orig Ler
13	TCP	2010/12/12	13:35:44,897	Device pc 37 from 192.168.2.30:52636 Port:992 established [ACK] Seq 253 Ack 1889 Win 170.
14	TCP	2010/12/12	13:35:44,897	Device pc 37 Set tx buffer size: window= 7300 desired= 7300 size= 7300
15	TCP	2010/12/12	13:35:44,897	Device pc 37 StopRpt f3cc7

```
[TraceStarted] 2010/12/12 13:35:44,004
Used config:
# Trace config
trace + IP-masquerading
trace + IP-Router
trace + TCP
```

If you want to compare the results of two traces with one another, you can display two traces side by side in the split-screen mode.



Index	Tracecategory	Date	Time	Content
18978	TCP	2010/12/12	15:16:16,968	Devicetime: 1900/01/01 01:40:27,020
18979	TCP	2010/12/12	15:16:16,968	Devicetime: 1900/01/01 01:40:27,020
18980	TCP	2010/12/12	15:16:16,968	Devicetime: 1900/01/01 01:40:27,020
18981	TCP	2010/12/12	15:16:16,968	Devicetime: 1900/01/01 01:40:27,020
18982	WLAN-STAT...	2010/12/12	15:16:16,992	Devicetime: 1900/01/01 01:40:27,070
18983	WLAN-STAT...	2010/12/12	15:16:17,006	Devicetime: 1900/01/01 01:40:27,160
18984	TCP	2010/12/12	15:16:17,157	Devicetime: 1900/01/01 01:40:27,220
18985	TCP	2010/12/12	15:16:17,167	Devicetime: 1900/01/01 01:40:27,220
18986	TCP	2010/12/12	15:16:17,167	Devicetime: 1900/01/01 01:40:27,220
18987	TCP	2010/12/12	15:16:17,167	Devicetime: 1900/01/01 01:40:27,220
18988	TCP	2010/12/12	15:16:17,167	Devicetime: 1900/01/01 01:40:27,220
18989	TCP	2010/12/12	15:16:17,167	Devicetime: 1900/01/01 01:40:27,220
18990	WLAN-STAT...	2010/12/12	15:16:17,167	Devicetime: 1900/01/01 01:40:27,270
18991	WLAN-STAT...	2010/12/12	15:16:17,191	Devicetime: 1900/01/01 01:40:27,360
18992	TraceStopped	2010/12/12	15:16:17,341	Used config:;# Trace config;trace + IF

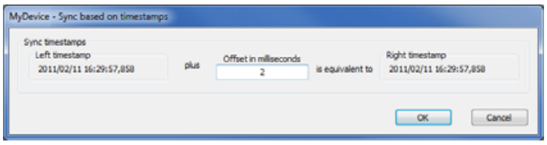
```
[TraceStopped] 2010/12/12 15:16:17,341
Used config:
# Trace config
trace + IP-masquerading
trace + IP-Router
trace + TCP
```

Index	Tracecategory	Date	Time	Content
0	TraceStarted	2010/12/12	13:35:15,587	Used config:;# Show commands;sho
1	TraceStopped	2010/12/12	13:35:18,428	Used config:;# Show commands;sho
2	TraceStarted	2010/12/12	13:35:44,004	Used config:;# Trace config;trace + I
3	TCP	2010/12/12	13:35:44,618	Devicetime: 1900/01/04 06:28:24,95
4	WLAN-DATA	2010/12/12	13:35:44,618	Devicetime: 1900/01/04 06:28:24,95
5	TCP	2010/12/12	13:35:44,621	Devicetime: 1900/01/04 06:28:24,96
6	WLAN-DATA	2010/12/12	13:35:44,621	Devicetime: 1900/01/04 06:28:24,96
7	TCP	2010/12/12	13:35:44,621	Devicetime: 1900/01/04 06:28:24,96
8	WLAN-DATA	2010/12/12	13:35:44,621	Devicetime: 1900/01/04 06:28:24,96
9	WLAN-DATA	2010/12/12	13:35:44,894	Devicetime: 1900/01/04 06:28:24,96
10	WLAN-DATA	2010/12/12	13:35:44,896	Devicetime: 1900/01/04 06:28:24,96
11	TCP	2010/12/12	13:35:44,896	Devicetime: 1900/01/04 06:28:24,96
12	WLAN-DATA	2010/12/12	13:35:44,896	Devicetime: 1900/01/04 06:28:24,96
13	TCP	2010/12/12	13:35:44,897	Devicetime: 1900/01/04 06:28:24,98
14	TCP	2010/12/12	13:35:44,897	Devicetime: 1900/01/04 06:28:24,98
15	TCP	2010/12/12	13:35:44,897	Devicetime: 1900/01/04 06:28:24,98

```
[TraceStopped] 2010/12/12 13:35:18,428
Used config:
# Show commands
show bootlog

[TraceStarted] 2010/12/12 13:35:44,004
```

Start the time-stamp based synchronization of the two traces with the button. In the following window, enter a suitable value for the offset in milliseconds and start the synchronization.



Left timestamp: 2011/02/11 16:29:57,858 plus Offset in milliseconds: 2 is equivalent to Right timestamp: 2011/02/11 16:29:57,858

2.2.4 Backing up and restoring the trace configuration

The entire configuration of the trace dump can be written to a storage medium for later re-use or for transfer to another user. Click on 'File > Store trace configuration' and re-open it later with 'File > Load trace configuration'.

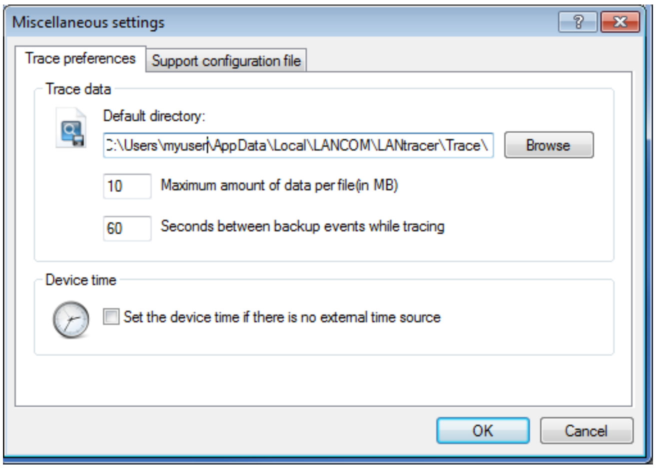
2.2.5 Backing up and restoring the trace data

For later editing, or for transfer to another user, the actual trace data can be written to a storage medium with 'File > Store trace data' and later re-opened with 'File > Load trace data'.

2.2.6 Backup settings for traces

When starting a trace with LANconfig or LANmonitor, a backup file with the current trace data is automatically saved. The settings for the trace backup can be configured with 'Extras > Other settings > Trace' backup. Enter the following parameters:

- Directory for the trace backups
- Maximum size of a trace backup file. If this file size is reached with an active trace, another trace backup file is created automatically.
- Save interval of the trace backup file. When this time has elapsed, an updated version of the trace backup file is saved automatically. The trace backup file therefore does not contain the information from the most recent backup up to the current time.
- LANmonitor can set current workstation time as a time for the trace, for example when the traced device itself does not have valid time information.



Trace data

Default directory: :\Users\myuser\AppData\Local\LANCOM\LANtracer\Trace\

10 Maximum amount of data per file(in MB)

60 Seconds between backup events while tracing

Device time

☐ Set the device time if there is no external time source

2.2.7 Filtering traces

Trace output from the command line or the LCMS Trace dialog can often be very long, because the trace receives information from the device at a very high frequency. To make the output of the traceseasier to understand, you can apply appropriate filters. The filters use a search function to analyze the trace output and present the desired information only.

In the following example, the administrator activates a simple IP router trace on a device with three Internet connections and sends pings to different destinations. The unfiltered trace output shows all packets processed by the IP router in the device:

```
root@MyDevice:/
> trace # ip-router
IP-Router ON
root@MyDevice:/
>[IP-Router] 2010/12/20 17:11:06,430
IP-Router Rx (LAN-1, INTRANET3, RtgTag: 3):
DstIP: 4.4.4.1, SrcIP: 192,168.3,100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0015, seq: 0x1cde
Route: WAN Tx (INTERNET3)
[IP-Router] 2010/12/20 17:11:06,430
IP-Router Rx (LAN-1, INTRANET1, RtgTag: 1):
DstIP: 11.11.11.1, SrcIP: 192,168.1,100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0016, seq: 0x1ccf
Route: WAN Tx (INTERNET1)
[IP-Router] 2010/12/20 17:11:06,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192,168.1,100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1ccf
Route: LAN-1 Tx (INTRANET1):
[IP-Router] 2010/12/20 17:11:06,430
IP-Router Rx (INTERNET3, RtgTag: 3):
DstIP: 192,168.3,100, SrcIP: 4.4.4.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0015, seq: 0x1cde
Route: LAN-1 Tx (INTRANET3):
[IP-Router] 2010/12/20 17:11:06,600
IP-Router Rx (LAN-1, INTRANET2, RtgTag: 2):
DstIP: 3.3.3.1, SrcIP: 192.168.2.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0014, seq: 0x1cea
Route: WAN Tx (INTERNET2)
[IP-Router] 2010/12/20 17:11:06,600
IP-Router Rx (INTERNET2, RtgTag: 2):
DstIP: 192,168.2,100, SrcIP: 33.31, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0014, seq: 0x1cea
Route: LAN-1 Tx (INTRANET2):
[IP-Router] 2010/12/20 17:11:07,430
IP-Router Rx (LAN-1, INTRANET1, RtgTag: 1):
DstIP: 11.11.11.1, SrcIP: 192.168.1.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0016, seq: 0x1cd0
```

```
Route: WAN Tx (INTERNET1)
[IP-Router] 2010/12/20 17:11:07,430
IP-Router Rx (LAN-1, INTRANET3, RtgTag: 3):
DstIP: 4.4.4.1, SrcIP: 192.168.3.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0015, seq: 0x1cdf
Route: WAN Tx (INTERNET3)
[IP-Router] 2010/12/20 17:11:07,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192,168.1,100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1cd0
Route: LAN-1 Tx (INTRANET1):
[IP-Router] 2010/12/20 5:11:07 PM,430
IP-Router Rx (INTERNET3, RtgTag: 3):
DstIP: 192,168.3,100, SrcIP: 44.41, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0015, seq: 0x1cdf
Route: LAN-1 Tx (INTRANET3):
[IP-Router] 2010/12/20 5:11:07 PM,600
IP-Router Rx (LAN-1, INTRANET2, RtgTag: 2):
DstIP: 3.3.3.1, SrcIP: 192.168.2.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0014, seq: 0x1ceb
Route: WAN Tx (INTERNET2)
[IP-Router] 2010/12/20 5:11:07 PM,600
IP-Router Rx (INTERNET2, RtgTag: 2):
DstIP: 192,168.2,100, SrcIP: 33.31, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0014, seq: 0x1ceb
Route: LAN-1 Tx (INTRANET2):
```

The output in just 2 seconds is enough to produce a large amount of data. For a better overview of the output, add a filter to the trace command. The filters start with the @ symbol and enter a search criterion. In this example, the filter reduces the output to that containing the search criterion "Internet1", in order to output only the packets from this remote site.

The filter is not case-sensitive.

```
root@MyDevice:/
> trace # ip-router @ INTERNET1
IP-Router ON @ INTERNET1
[IP-Router] 2010/12/20 17:11:50,430
IP-Router Rx (LAN-1, INTRANET1, RtgTag: 1):
DstIP: 11.11.11.1, SrcIP: 192.168.1.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0016, seq: 0x1cfb
Route: WAN Tx (INTERNET1)
[IP-Router] 2010/12/20 5:11:50 PM,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192,168.1,100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1cfb
Route: LAN-1 Tx (INTRANET1):
[IP-Router] 2010/12/20 5:11:51 PM,430
IP-Router Rx (LAN-1, INTRANET1, RtgTag: 1):
DstIP: 11.11.11.1, SrcIP: 192.168.1.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0016, seq: 0x1cfc
Route: WAN Tx (INTERNET1)
[IP-Router] 2010/12/20 5:11:51 PM,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192,168.1,100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1cfc
Route: LAN-1 Tx (INTRANET1):
```

Again, the time frame of the trace is about two seconds, but the amount of data has already been reduced significantly. The only data to be displayed is that relating to remote site "INTERNET1". However, further filter criteria can also be specified simply by placing a space between the first and second criteria. As well as a space symbol, the symbols "+" and "-" can also be used as operators. With a "+" both criteria must be met; with a "-" the criterion must not be fulfilled; a space means that one or the other of the associated criteria must be fulfilled. The option to use strings containing operators as a filter is implemented by quotation marks:

If you want to apply multiple search terms, you can separate the terms with the following operators:

- Space: A space before a search term is a logical OR operation. The trace output is only displayed if it contains one of the strings marked in this way.
- +: A plus sign before a search term is a logical AND operation. The trace output is only displayed if it contains all of the strings marked in this way.
- -: A minus sign before a search term is a logical NOT operation. The trace output is only displayed if it contains none of the strings marked in this way.

```
root@MyDevice:/
> trace # ip-router @ INTERNET1 -"echo request"
IP-Router ON @ INTERNET1 -"echo request"
[IP-Router] 2010/12/20 17:12:06,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192,168.1,100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1d0b
Route: LAN-1 Tx (INTRANET1):
[IP-Router] 2010/12/20 17:12:07,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192,168.1,100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1d0c
Route: LAN-1 Tx (INTRANET1):
```

The trace now shows only the entries that contain the remote site 'INTERNET1', but **not** the string 'echo request'. This displays only the responses to a ping as they return from the remote site.

You can use multiple traces simultaneously and filter by different criteria. In the following example, an Ethernet trace is run in addition to the IP router trace to see the packet associated with the ping on the Ethernet:

```
root@MyDevice:/
> trace # ip-router @ INTERNET1 +"echo reply"
IP-Router ON @ INTERNET1 +"echo reply"
root@MyDevice:/
> trace # eth @ ICMP +“echo reply”
Ethernet ON @ icmp +"echo reply"
[IP-Router] 2010/12/21 14:17:21,000
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192,168.1,100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0002, seq: 0x2654
Route: LAN-1 Tx (INTRANET1):
[Ethernet] 2010/12/21 14:17:21,000
Sent 98 byte Ethernet packet via LAN-1:
HW Switch Port : ETH-1
-->IEEE 802.3 Header
Dest : 00:a0:57:12:a9:21 (LANCOM 12:a9:21)
Source : 00:a0:57:12:f7:81 (LANCOM 12:f7:81)
Type : IPv4
-->IPv4 Header
Version : 4
Header Length : 20
Type of service : (0x00) Precedence 0
Total length : 84
ID : 18080
Fragment : Offset 0
TTL : 59
Protocol : ICMP
Checksum : 24817 (OK)
Src Address : 11.11.11.1
Dest Address : 192.168.1.100
-->ICMP Header
Msg : echo reply
Checksum : 18796 (OK)
Body : 00 00 00 02 00 00 26 54 ......
 7e c9 6d 8c 00 00 00 00 ~.m.....
 00 01 02 03 04 05 06 07 ........
 08 09 0a 0b 0c 0d 0e 0f ........
 10 11 12 13 14 15 16 17 ........
 18 19 1a 1b 1c 1d 1e 1f ........
 20 21 22 23 24 25 26 27 !"#$%
```

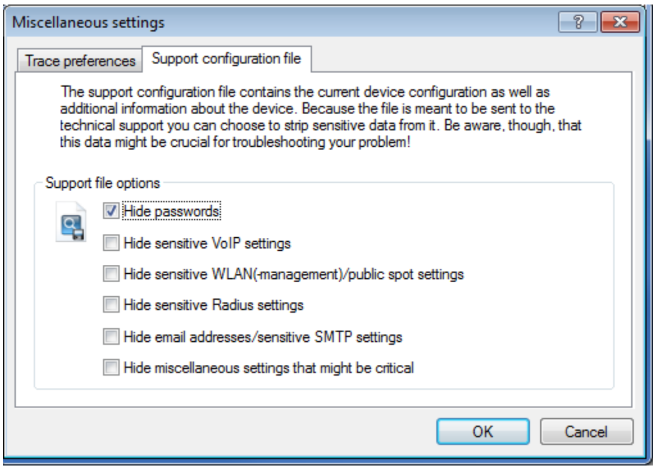
2.2.8 Saving a support file

A support file enables all information pertaining to support to be easily written to one file:

- Trace data as configured in the current settings (such as with function “Save trace data”)
- Current device configuration
- Bootlog
- Sysinfo

When saving the device configuration, security-related information of no relevance to support can be hidden. Use 'Extras > Other settings > Support file' in the trace window to select which information is not to be saved in the support file:

The support file created this way contains text-based information. The file can be opened using an editor or checked for any critical entries.



The support configuration file contains the current device configuration as well as additional information about the device. Because the file is meant to be sent to the technical support you can choose to strip sensitive data from it. Be aware, though, that this data might be crucial for troubleshooting your problem!

Support file options

☑ Hide passwords
□ Hide sensitive VoIP settings
□ Hide sensitive WLAN(-management)/public spot settings
□ Hide sensitive Radius settings
□ Hide email addresses/sensitive SMTP settings
□ Hide miscellaneous settings that might be critical

2.3 LANCOM Software Update for LCMS

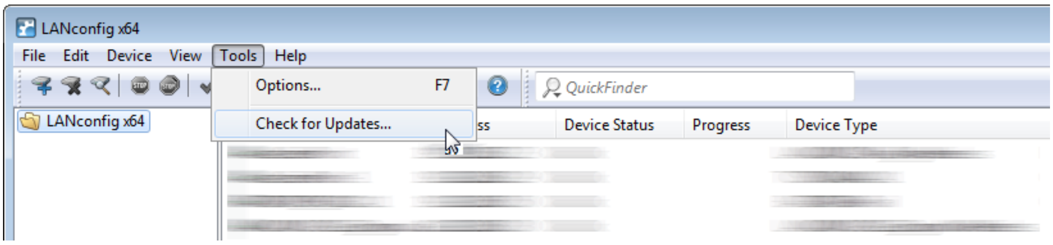
The software update for LCMS allows you to automatically download new versions of the LCMS and your device firmware.

New versions for LCMS (LANconfig, LANmonitor and WLANmonitor) are downloaded directly from the freely accessible download section of the LANCOM web server. Device-specific software such as new firmware versions require an account in the customer portal myLANCOM.

2.3.1 Manually starting the Software Update

To start the software update manually in LANconfig proceed as follows:

1. Start LANconfig.
2. Click on the Tools menu and select 'Check for updates...'.

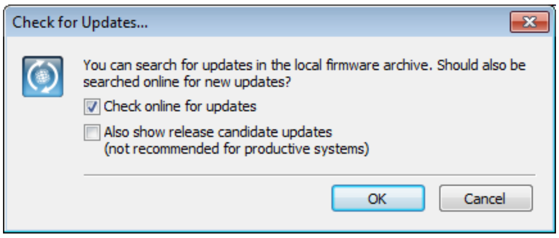


LANconfig searches the local firmware archive for updates. Optionally, you can extend the search with the following items:

- Find more updates online in the download area of the LANCOM web server.

- Include Release Candidates in the search. If you enable this option, the Software Update will not only offer to download the released software versions for use in productive environments, but also any available release candidates.

> Release candidates include the new features of upcoming software versions and have been thoroughly tested. Until the final release of version, the software may be further optimized—partly due to user feedback.



Check for Updates...

You can search for updates in the local firmware archive. Should also be searched online for new updates?

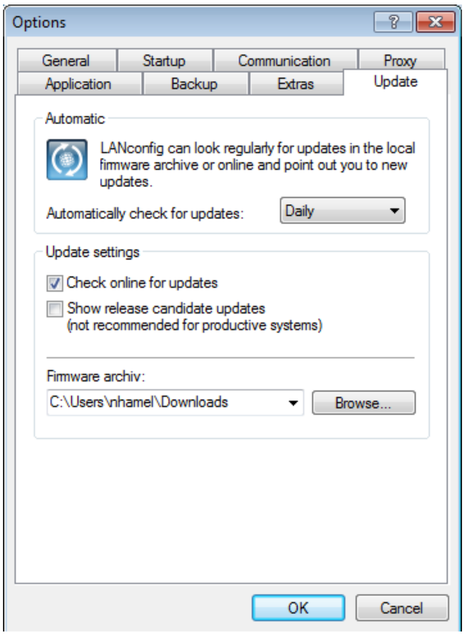
☑ Check online for updates

□ Also show release candidate updates (not recommended for productive systems)

2.3.2 Settings for the automatic search for new updates

Proceed as follows to start the software update automatically in LANconfig each time the application starts:

1. Start LANconfig.
2. Click on the Tools menu and select 'Options...'.
3. Go to the 'Update' tab.
4. Select the option 'Automatic software update check at startup'.



Options

Automatic

LANconfig can look regularly for updates in the local firmware archive or online and point out you to new updates.

Automatically check for updates: Daily

Update settings

☑ Check online for updates

□ Show release candidate updates (not recommended for productive systems)

Firmware archiv: C:\Users\nhamel\Downloads

Configure the following items for the automatic update:

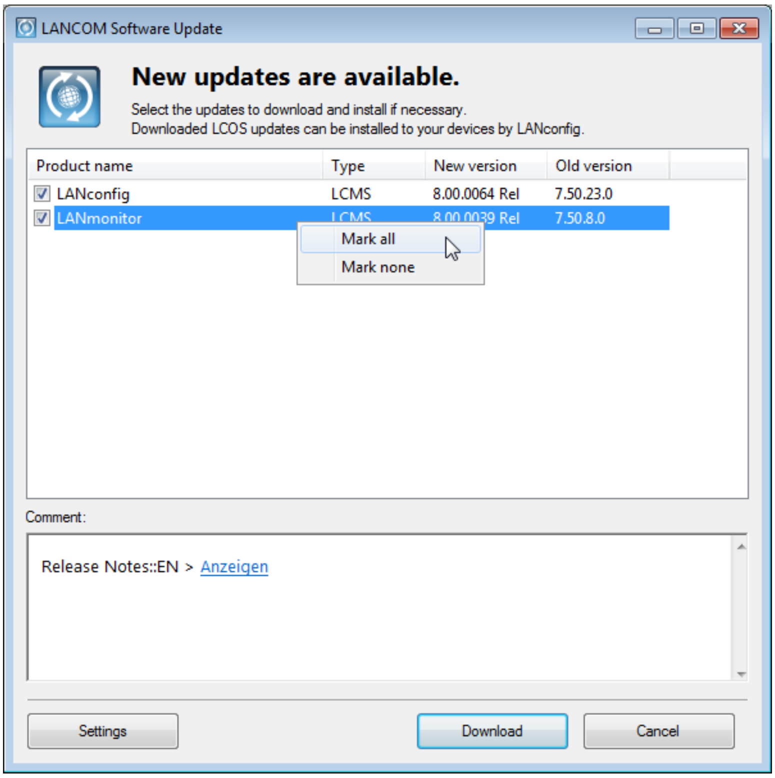
- Select the time interval for the automatic check for updates (daily, weekly or monthly). Alternatively, disable the automatic search with the setting 'Never'.
- Find more updates online in the download area of the LANCOM web server.
- Release candidates include the new features of upcoming software versions and have been thoroughly tested. Until the final release of version, the software may be further optimized—partly due to user feedback.
  Include Release Candidates in the search. If you enable this option, the Software Update will not only offer to download the released software versions for use in productive environments, but also any available release candidates.
- Select a suitable location for the firmware archive. The firmware archive has the following functions:

- When carrying out the automatic search for updates, LANconfig searches this location for new versions of the LCMS and the firmware.
- This is the location where LANCOM Software Update stores the updates from the download section of the LANCOM web server.

2.3.3 Selecting and installing the available updates

After successful connection to the update server, LANconfig displays the available updates.

Select the appropriate versions and click on 'Download'. As an alternative, you can click on the entries with the right-hand mouse key and select the entry 'Select all' or 'Select none' from the context menu.



LANCOM Software Update

New updates are available.

Select the updates to download and install if necessary.
Downloaded LCOS updates can be installed to your devices by LANconfig.

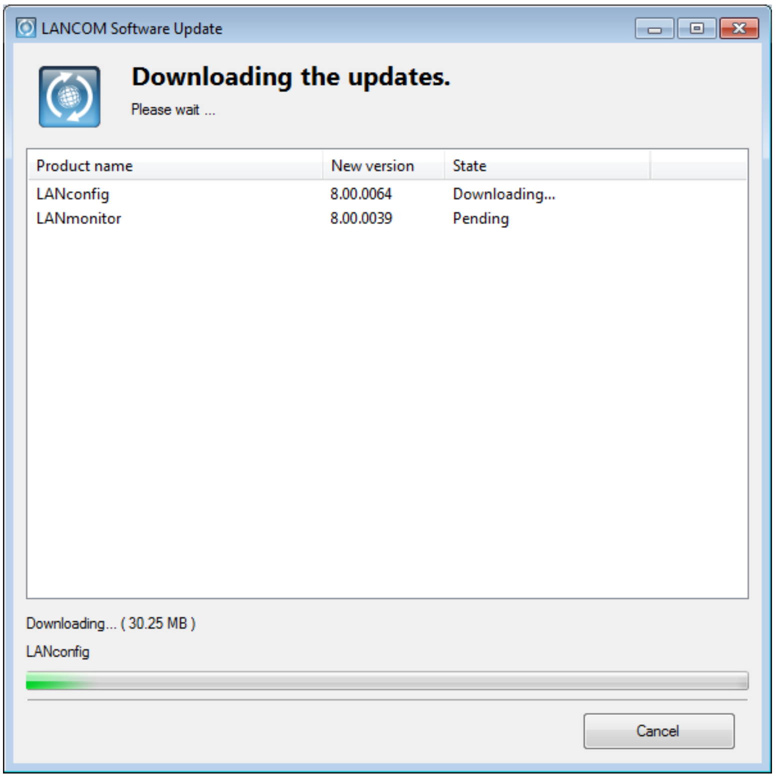
Product name	Type	New version	Old version
☑ LANconfig	LCMS	8.00.0064 Rel	7.50.23.0
☑ LANmonitor	LCMS	8.00.0039 Rel	7.50.8.0

Comment:

Release Notes::EN > Anzeigen

The first time you select firmware for download, the LANCOM Software Update requests you to enter your login data for myLANCOM.

LANCOM Software Update now downloads the selected software one after other and stores the files in the firmware archive.



LANCOM Software Update

Downloading the updates.

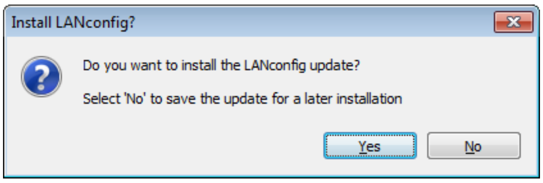
Please wait ...

Product name	New version	State
LANconfig	8.00.0064	Downloading...
LANmonitor	8.00.0039	Pending

Downloading... (30.25 MB)

LANconfig

After successfully downloading the software, LANCOM Software Update offers to install the downloaded software (LANconfig and LANmonitor only):

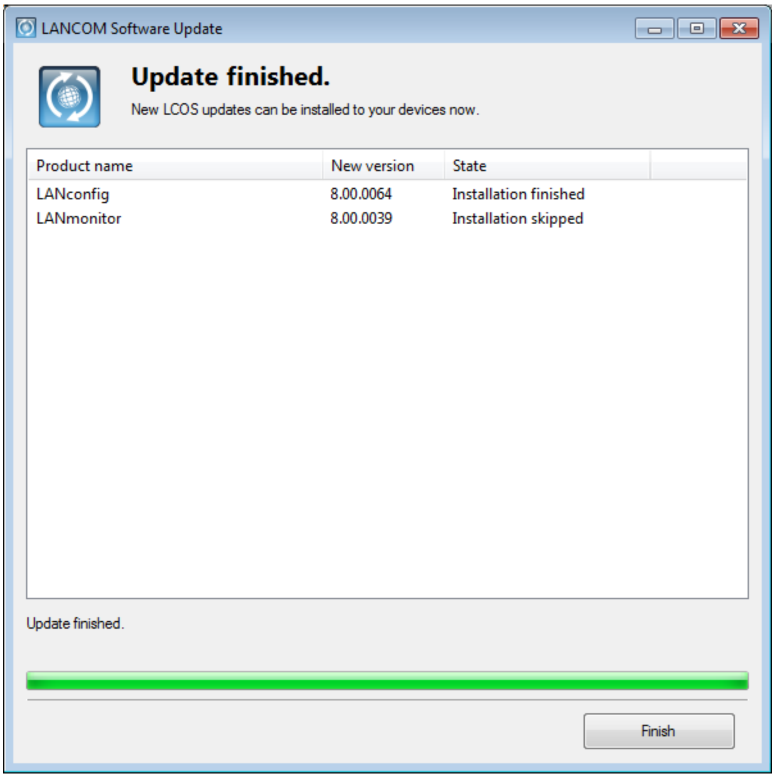


Install LANconfig?

Do you want to install the LANconfig update?

Select 'No' to save the update for a later installation

After installation, the LANCOM Software Update displays the results of the update procedure:



LANCOM Software Update

Update finished.

New LCOS updates can be installed to your devices now.

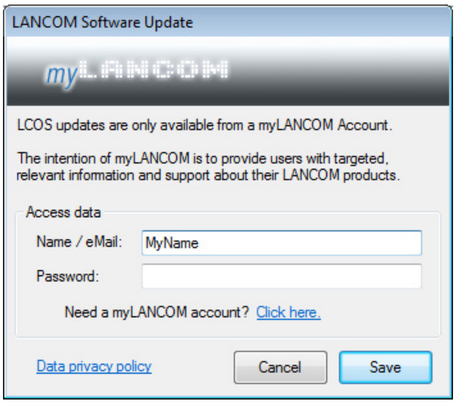
Product name	New version	State
LANconfig	8.00.0064	Installation finished
LANmonitor	8.00.0039	Installation skipped

Update finished.

2.3.4 Software Update Settings

For some functions, the LANCOM Software Update requires access to the customer portal myLANCOM. Proceed as follows to enter your myLANCOM credentials:

1. Start LANconfig.
2. Click on the Tools menu and select 'Check online for updates...'.
3. In the dialog with the results of the software updates, click on the 'Settings' button.
4. In the next dialog, enter the user name and password for access to myLANCOM.
5. If you wish, you can select the option 'Offer release candidate updates if available'. If you enable this option, the Software Update will not only offer to download the released software versions for use in productive environments, but also any available release candidates.



LCOS updates are only available from a myLANCOM Account.

The intention of myLANCOM is to provide users with targeted, relevant information and support about their LANCOM products.

Name / eMail: MyName

Password:

Need a myLANCOM account? Click here.

3 LAN

3.1 Bandwidth restriction of the LAN interfaces

3.1.1 Introduction

For a device with an integrated WLAN module, you can specify a bandwidth limit for individual LAN ports. The table of LAN interfaces contains the parameters necessary to configure bandwidth restrictions.

3.1.2 Additions to the menu system

2.23.21 LAN interfaces

This menu contains the settings for the LAN interfaces.

Telnet path: Setup/Interfaces/LAN-Interfaces

2.23.21.8 Tx limit

Enter the bandwidth limit (kbps) in the transmission direction. The value 0 means there is no limit.

Telnet path: Setup/Interfaces/LAN-Interfaces

Possible values:

- Maximum 10 numerical characters

Default: 0

ⓘ This setting is only available for devices with a WLAN module.

2.23.21.9 Rx limit

Enter the bandwidth limit (kbps) in the receive direction.The value 0 means there is no limit.

Telnet path: Setup/Interfaces/LAN-Interfaces

Possible values:

- Maximum 10 numerical characters

Default: 0

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

4 WLAN

4.1 WLAN layer-3 tunneling

4.1.1 Introduction

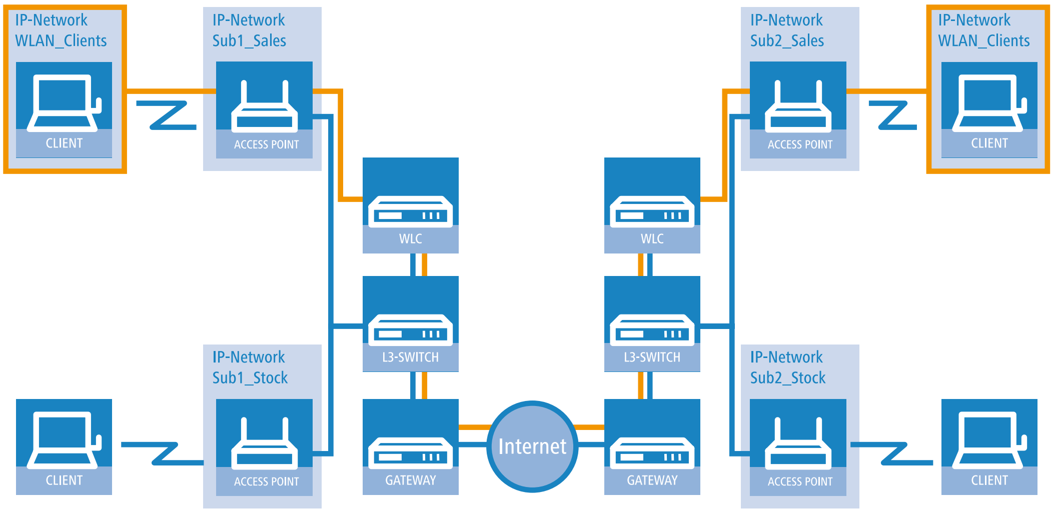
The CAPWAP standard for centralized WLAN management offers two different channels for transmissions:

- The obligatory control channel transports administrative data between the managed access point and the WLAN controller.
- The optional data channel transmits the payload data from the various WLAN networks (SSID) between the managed access point and the WLAN controller.

The decision whether to use of the optional data channel between the managed access point and the WLAN controller depends on the route to be taken by the payload data:

- If you deactivate the data channel, the access point forwards the payload data directly to the LAN. In this case, you control the allocation of WLAN clients to specific LAN segments, for example by assigning VLAN IDs. The advantage of this application lies in the low load on the controller and on the network as a whole, because the access point transmits only the management data via the CAPWAP tunnel and it transmits the payload data over the shortest available route.
- If you activate the data channel, the access point additionally forwards the payload data to the central WLAN controller. This approach has the following advantages:
  - □ The access points can provide access to networks that are only available on the WLAN controller, such as a central Internet access for a Public Spot.
  - □ The WLANs provided by the access points (SSIDs) can be separated from one another without the use of VLAN. Avoiding the use of VLAN reduces the effort required for the configuration of other network components such as switches, etc.
  - □ WLAN clients associated with the access points and in different IP networks can roam to other access points without interruption to their IP connections, because the connection is continually managed by the central controller and not by the access points (layer-3 roaming).

The use of data channels forms additional logical networks on the basis of the existing physical infrastructure. These logical networks are known as overlay networks.



Picture 2: “Overlay network across multiple IP networks”

Using the data channel even allows you to span logical overlay networks across multiple WLAN controllers.

Several WLCs within a single broadcast domain can support the same overlay network. Disable the WLC data channel between these controllers. Otherwise the multiple reception of the broadcast messages would give rise to loops. Since routers discard broadcast messages, you can activate the CAPWAP data channel for controllers in separate networks.

The access points use virtual WLC interfaces (WLC tunnels) to manage each SSID's data channels between access point and WLAN controller.Depending on the model, each WLAN controller provides 16 to 32 WLC tunnels that you can use when configuring the logical WLANs.

ⓘ Virtual WLC interfaces are available for selection in all dialogs used to select logical interfaces (LAN or WLAN), such as in the port table of the LAN and VLAN settings or for the definition of IP networks.

4.1.2 Additions to the menu system

2.37.1.14 Multicast networks

This table contains the settings for the transmission of CAPWAP multicast packets over the bridge interfaces.

When a WLAN controller receives a broadcast or multicast packet from a network belonging to a certain SSID, then it has to forward this packet to all access points that work with that SSID. The WLAN controller has two ways to reach all of these access points:

- The WLAN controller copies the packet and sends it as a unicast to the relevant access points. The replication of packets increases the CPU load on the controller and the necessary bandwidths, which negatively impacts performance especially in case of WAN connections.
- The WLAN controller sends the packet as a multicast. In this case, a single packet only has to be transmitted. However, multicast packets sent from a controller only reach those access points in its own broadcast domain. Access points at the other end of a routed WAN link are generally unable to receive multicast packets from the controller.

ⓘ The forwarding of multicast packets depends on the routers operated on the WAN route.

The WLAN controller regularly sends keep-alive multicast packets to the multicast group. If an access point responds to these packets, the controller is able to reach this access point with multicast packets. For all other access points, the controller copies the multicast packets it receives and sends them as a unicast to the appropriate access points.

If the transmission of CAPWAP multicast packets has been activated and a valid multicast IP address with port has been defined for the bridge interface, the device forwards the incoming broadcast and multicast packets as a multicast to this address.

Devices operating multicast also operate IGMP snooping for continuous updates to the information on multicast structure.

In applications featuring multiple WLAN controllers, multicast packets can lead to loops. In order to avoid loops due to multicasts when using the bridge, the WLAN controller applies the following measures:

- The WLAN controller does not support mutlicast packets in the WLC data tunnel. Instead the packets are sent as unicast.
- The WLAN controller does not forward packets that carry a CAPWAP multicast address as the recipient.
- The WLAN controller automatically enables IGMP snooping on all managed access points if CAPWAP works with multicast.

2.37.1.14.1 Bridge interface

This item allows you to select a bridge interface for the multicast settings.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Multicast-Networks

Possible values:

- Select one of the defined bridge interfaces

2.37.1.14.2 Operating

This option activates or disables the use of CAPWAP multicast packets for this bridge interface.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Multicast-Networks

Possible values:

- Yes
- No

Default: No

2.37.1.14.3 Multicast address

Use this item to select an IP address to which the device sends CAPWAP multicast packets for the selected bridge interface.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Multicast-Networks

Possible values:

- Maximum 15 characters to define a valid IP address

Default: 233.252.124.1 to 233.252.124.32 (IP addresses from the unassigned range)

2.37.1.14.4 Multicast port

This item allows you to select a port for transmitting CAPWAP multicast packets over the selected bridge interface.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Multicast-Networks

Possible values:

- Maximum 5 numbers to define a valid port number

Default: 20000 to 20031

2.37.1.14.5 Loopback address

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

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

Telnet path: /Setup/WLAN-Management/AP-Configuration/Multicast-Networks

Possible values:

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

Default: 00.0.0

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

2.37.34 WLC cluster

This menu contains the settings for the data connections and status connections between multiple WLAN controllers.

Telnet path: /Setup/WLAN-Management

2.37.34.2 WLC data tunnel active

This option activates or disables the use of data tunnels between multiple WLAN controllers.

Telnet path: /Setup/WLAN-Management

Possible values:

- Yes
- No

Default: No

2.37.34.4 WLC discovery

This table allows you to enable or disable the automatic search for further WLCs separately for each IP network.

Telnet path: /Setup/WLAN-Management/WLC-Cluster

2.37.34.4.1 Network

Select one of the IP networks defined in the device, in which you want to automatically search for additional WLAN controllers.

Telnet path: /Setup/WLAN-Management/WLC-Cluster/WLC-Discovery

Possible values:

- Select from the list of defined IP networks (maximum 16 characters).

- No

Default: INTRANET: no, DMZ: no

2.37.34.4.2 Operating

Use this option to enable or disable the automatic search for other WLAN controllers in the selected IP network.

Telnet path: /Setup/WLAN-Management/WLC-Cluster/WLC-Discovery

Possible values:

- Yes
- No

Default: INTRANET: yes, DMZ: no

The automatic search for other WLAN controllers is one way of establishing the connection between two WLCs. If you disable this option, the WLAN controller cannot automatically establish a data channel to another WLC over this network. As an alternative, you can define the remote sites in the static WLC list.

2.37.34.3 Static WLC list

This table is used to define additional WLAN controllers as remote sites to which a connection can be established. The controller initially establishes a control tunnel to this remote site. If you have activated the option for the data tunnel, the controller then automatically establishes a data tunnel to this remote site.

Telnet path: /Setup/WLAN-Management/WLC-Cluster

2.37.34.3.1 IP address

This item defines the IP address of another WLAN controller to which this controller can establish a data tunnel.

Telnet path: /Setup/WLAN-Management/WLC-Cluster/Static-WLC-List

The two WLAN controllers can only establish a connection when the devices meet the following requirements:

- For both devices you have defined the respective remote sites, either statically or using the automatic search.
- Both controllers have a certificate from the same CA.

2.37.34.3.2 Loopback address

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

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

Telnet path: /Setup/WLAN-Management/WLC-Cluster/Static-WLC-List

Possible values:

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

Default: 00.0.0

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

2.37.1.1 Network profiles

Here you define the logical WLAN networks for activation and operation via the associated access points (APs).

Telnet path: /Setup/WLAN-management/AP-configuration

2.37.1.1.34 VLAN ID

This item allows you to set the VLAN ID for this logical WLAN network. When the VLAN mode is set to 'tagged', the access point transmits the data from this WLAN network (SSID) with the VLAN ID set here.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- 2 to 4094

Default: 2

2.37.1.1.33 Inter-station traffic

Depending on the application, it may be required that the WLAN clients connected to an access point can—or expressly cannot—communicate with other clients. The setting that decides whether clients within an SSID can exchange data with one another has to be set separately for each logical WLAN.

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- Yes
- No

Default: Yes

2.37.1.1.32 Connect SSID to

Here you can select the logical interface used by the access point to transfer the payload data from this WLAN network (SSID).

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- LAN: The access point forwards payload data from this WLAN network via the bridge to its own local LAN interface. In this case, configure how the data packets are to be further processed by using appropriate routes directly on the access point, for example through a separate Internet connection.
- WLC-TUNNEL-1 to WLC-TUNNEL-x (model dependent): The access point forwards the payload data from this WLAN network via one of the virtual interfaces to the WLAN controller (WLC tunnel). In this case, configure how the data packets are to be further processed by using appropriate routes centrally on the WLAN controller, for example through a shared Internet connection.

Default: LAN

ⓘ Forwarding payload data from multiple SSIDs to the WLAN controller increases the CPU load and bandwidth demands of the central devices. Consider the performance requirements of central WLAN management that uses layer-3 tunneling.

ⓘ For each access point you can connect up to 7 SSIDs with a WLC tunnel. For each access point, the WLAN controller connects the WLC tunnel and its associated SSID to an available bridge group. Since one of the eight available bridge groups is reserved for other purposes, 7 bridge groups remain for assigning the WC-tunnel.

2.37.1.1.30 VLAN mode

This item allows you to select the VLAN mode for this WLAN network (SSID).

Telnet path: /Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- tagged: The access point marks the packets of this SSID with the ID configured under 2.37.1.1.34 VLAN ID.
- untagged: The access point forwards the packets of this SSID without any VLAN ID.

Default: untagged

The access point only uses the VLAN settings for the logical WLAN if you activate the VLAN module in the access point (in the physical WLAN parameters). The setting 'untagged' for a specific WLAN allows you to operate in a wireless LAN without VLAN, even if VLAN is otherwise activated.

2.37.1.2 Radio profiles

Here you define the physical WLAN parameters which apply to all of the logical WLAN networks that share a managed access point.

Telnet path: /Setup/WLAN-management/AP-configuration

2.37.1.2.17 Activate VLAN module of managed APs

Use this item to activate or deactivate the VLAN module in the managed access points. If VLAN is switched off, all VLAN settings in the logical network are ignored.

Telnet path: /Setup/WLAN management/AP-Configuration/Radioprofiles

Possible values:

- Yes
- No

Default: No

2.37.1.2.14 Management VLAN ID

VLAN ID for the management network. The management VLAN ID is used for tagging the management network which is used for communications between the WLAN controller and the access points. VLAN is only used if the VLAN module in the access point is enabled. The management network can be operated without tagging even if VLAN is enabled by selecting the corresponding setting for the management VLAN mode. The VLAN ID '1' is reserved internally for this.

Telnet path: /Setup/WLAN management/AP-Configuration/Radioprofiles

Possible values:

- 2 to 4094

Default: 2

2.37.1.2.18 Management VLAN mode

VLAN mode for the management network. VLAN is only used if the VLAN module in the access point is enabled. The management network can be operated untagged even if VLAN is activated.

Telnet path: /Setup/WLAN management/AP-Configuration/Radioprofiles

Possible values:

- untagged: The access point's management packets are not marked with a VLAN ID.
- tagged: The access point's management packets are marked with the VLAN ID that is configured in this radio profile as the management VLAN ID.

Default: untagged

2.37.1.12 DSCP for control packets

This item allows you to set the prioritization of control packets by DiffServ (Differentiated Services).

Telnet path: /Setup/WLAN-management/AP-configuration

Possible values:

- Best effort
- Assured-Forwarding-11
- Assured-Forwarding-12
- Assured-Forwarding-13
- Assured-Forwarding-21
- Assured-Forwarding-22
- Assured-Forwarding-23
- Assured-Forwarding-31
- Assured-Forwarding-32
- Assured-Forwarding-33

- Assured-Forwarding-41
- Assured-Forwarding-42
- Assured-Forwarding-43
- Expedited forwarding

Default: Best effort

2.37.1.13 DSCP for data packets

This item allows you to set the prioritization of data packets by DiffServ (Differentiated Services).

Telnet path: /Setup/WLAN-management/AP-configuration

Possible values:

- Best effort
- Assured-Forwarding-11
- Assured-Forwarding-12
- Assured-Forwarding-13
- Assured-Forwarding-21
- Assured-Forwarding-22
- Assured-Forwarding-23
- Assured-Forwarding-31
- Assured-Forwarding-32
- Assured-Forwarding-33
- Assured-Forwarding-41
- Assured-Forwarding-42
- Assured-Forwarding-43
- Expedited forwarding

Default: Best effort

4.1.3 Tutorials

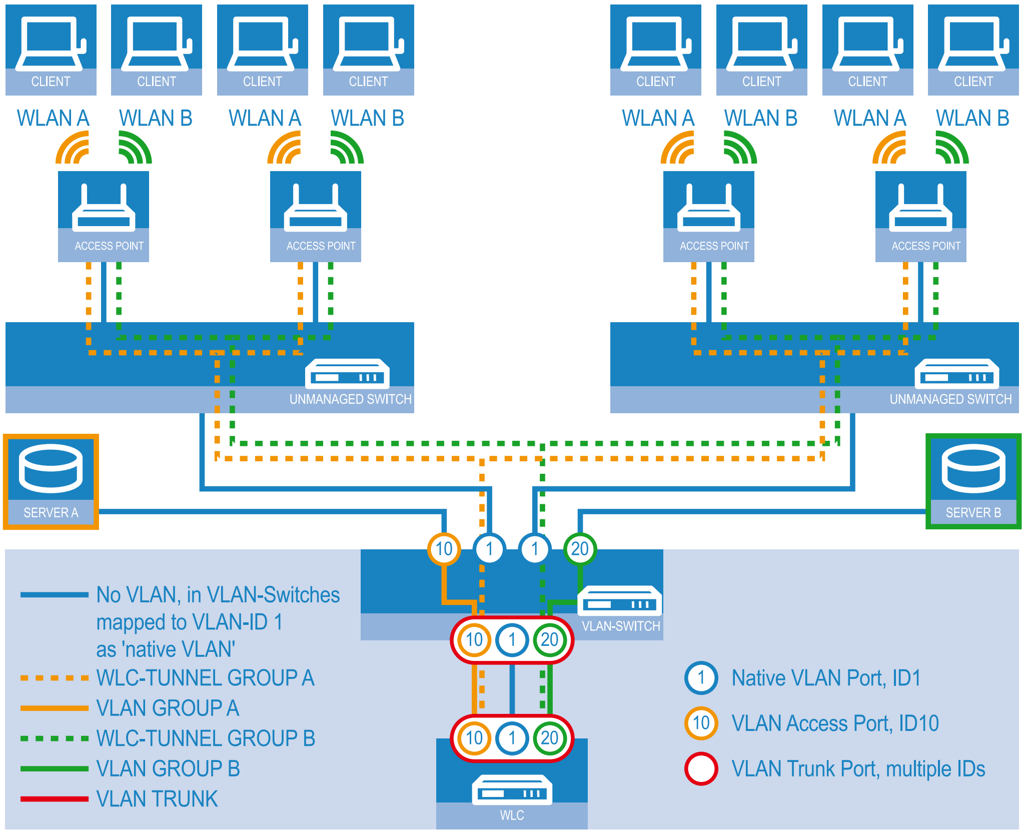
The following sections present specific scenarios with step-by-step instructions for a number of standard situations when operating WLAN controllers.

Overlay network: Separating networks for access points without using VLAN

In many cases, networks in a shared physical infrastructure are separated by using VLANs. However, this method assumes that the switches operated in the network are VLAN-capable and that these are configured for VLAN operations. Consequently, the administrator has to rollout the VLAN configuration for the whole network.

WLAN controllers enable you to separate the networks while minimizing the use of VLANs. The access points use a CAPWAP data tunnel to direct the payload from the WLAN clients straight to the controller, which then assigns the data to the corresponding VLANs. In this situation, VLAN configuration is only required for the controller and a single, central switch. All of the other switches in this example work without a VLAN configuration.

ⓘ With this configuration, you reduce the VLAN to the core of the network structure (illustrated with a blue background). What's more, only 3 of the switch ports in use require a VLAN configuration.



Picture 3: “Example application: Overlay network”

The diagram shows a sample application with the following components:

- The network consists of two segments, each with its own (not necessarily VLAN-capable) switch.
- Each segment contains several access points, each of which is connected to one of the switches.
- Each access point provides two SSIDs for the WLAN clients in two different user groups, shown in the diagram in green and orange.
- Each user group has access to its own dedicated server that is separated from other user group. The servers can only be accessed via the corresponding VLANs, i.e. through the access ports configured on the switch.
- A single WLAN controller manages all of the access points in the network.
- A central, VLAN-capable switch connects the switches in each segment, the servers for each group, and the WLAN controller.

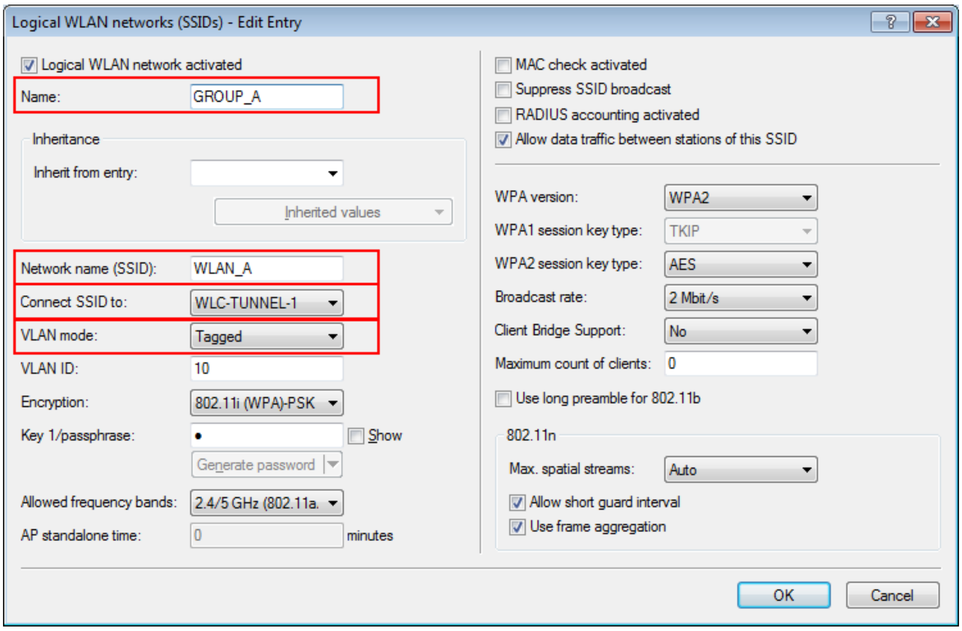
The aim of the configuration: A WLAN client that associates with an SSID is to have access to its "own" server, regardless of which access point is being used and regardless of the segment in which the client is located.

The following description assumes a working basic configuration of the WLAN controller. The configuration of the VLAN switch is not part of this description.

Configuring the WLAN settings

1. For each SSID, create an entry in the list of logical networks. This entry requires a suitable name and the corresponding SSID. Connect the SSID to a WLC tunnel, for example the first SSID to "WLC-TUNNEL-1" and the second to "WLC-TUNNEL-2 '. Set the VLAN mode to 'tagged', set the VLAN ID '10' for the first logical network and the VLAN ID '20' for the second logical network. In LANconfig

you find these settings under Configuration/WLAN Controller/Profiles/Logical WLAN networks (SSIDs).



Logical WLAN networks (SSIDs) - Edit Entry

☑ Logical WLAN network activated

Name: GROUP_A

Inheritance

Inherit from entry:

Inherited values

Network name (SSID): WLAN_A

Connect SSID to: WLC-TUNNEL-1

VLAN mode: Tagged

VLAN ID: 10

Encryption: 802.11i (WPA)-PSK

Key 1/passphrase: • □ Show

Generate password

Allowed frequency bands: 2.4/5 GHz (802.11a.

AP standalone time: 0 minutes

□ MAC check activated

□ Suppress SSID broadcast

□ RADIUS accounting activated

☑ Allow data traffic between stations of this SSID

WPA version: WPA2

WPA1 session key type: TKIP

WPA2 session key type: AES

Broadcast rate: 2 Mbit/s

Client Bridge Support: No

Maximum count of clients: 0

□ Use long preamble for 802.11b

802.11n

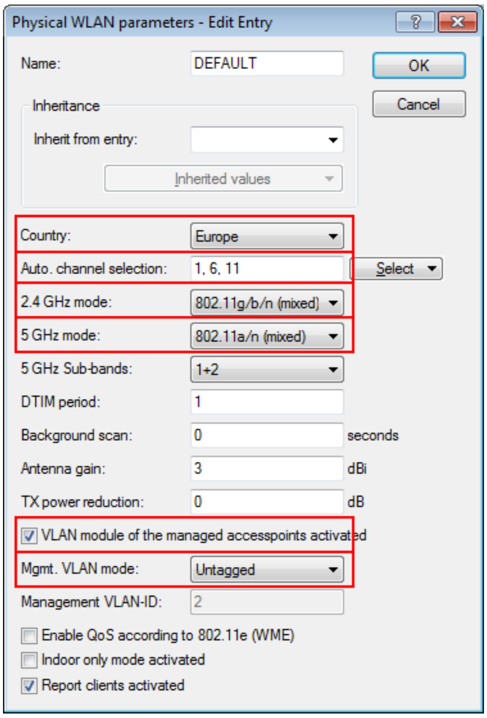
Max. spatial streams: Auto

☑ Allow short guard interval

☑ Use frame aggregation

Picture 4: “Logical WLAN networks for overlay networks”

2. Create an entry in the list of physical WLAN parameters with the appropriate settings for your access points, such as the country 'Europe' with the channels 1, 6 and 11 in 802.11b/g/n and 802.11a/n in mixed mode. For this profile in the physical WLAN parameters, enable the option to turn on the VLAN module on the access points. Set the operating mode for the management VLAN in the access points to 'Untagged'. In LANconfig you find these settings under Configuration/WLAN Controller/Profiles/Physical WLAN parameters.



Physical WLAN parameters - Edit Entry

Name: DEFAULT

Inheritance

Inherit from entry:

Inherited values

Country: Europe

Auto. channel selection: 1, 6, 11 Select

2.4 GHz mode: 802.11g/b/n (mixed)

5 GHz mode: 802.11a/n (mixed)

5 GHz Sub-bands: 1+2

DTIM period: 1

Background scan: 0 seconds

Antenna gain: 3 dBi

TX power reduction: 0 dB

☑ VLAN module of the managed accesspoints activated

Mgmt. VLAN mode: Untagged

Management VLAN-ID: 2

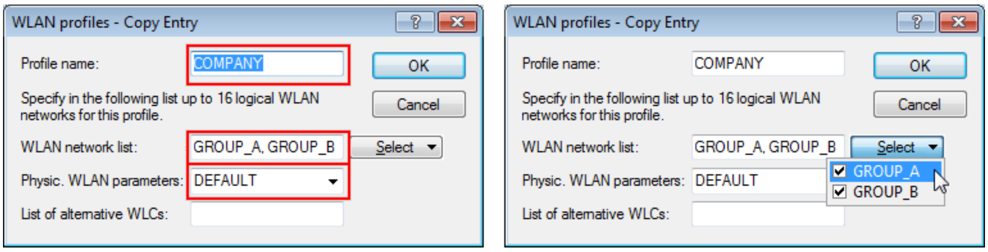
□ Enable QoS according to 802.11e (WME)

□ Indoor only mode activated

☑ Report clients activated

Picture 5: “Physical WLAN parameters for overlay networks”

3. Create a WLAN profile and give it a suitable name. Then assign the logical WLAN networks and the physical WLAN parameters created previously to this WLAN profile. In LANconfig you find these settings under Configuration/WLAN Controller/Profiles/WLAN profiles.



WLAN profiles - Copy Entry

Profile name: COMPANY

Specify in the following list up to 16 logical WLAN networks for this profile.

WLAN network list: GROUP_A, GROUP_B

Physic. WLAN parameters: DEFAULT

List of alternative WLCs:

WLAN profiles - Copy Entry

Profile name: COMPANY

Specify in the following list up to 16 logical WLAN networks for this profile.

WLAN network list: GROUP_A, GROUP_B

☑ GROUP_A

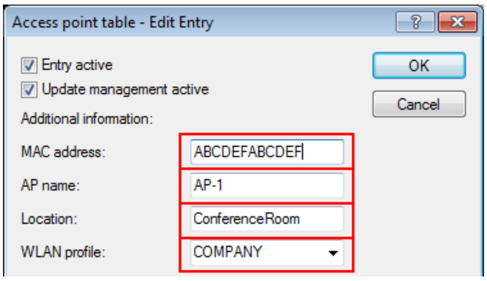
☑ GROUP_B

Physic. WLAN parameters: DEFAULT

List of alternative WLCs:

Picture 6: “WLAN profiles for overlay networks”

4. For each managed access point, create an entry in the access point table with a suitable name and the associated MAC address. Assign the WLAN profile created previously to this access point. In LANconfig you find these settings under Configuration/WLAN Controller/AP config./Access point table.



Access point table - Edit Entry

☑ Entry active

☑ Update management active

Additional information:

MAC address: ABCDEFABCDEF

AP name: AP-1

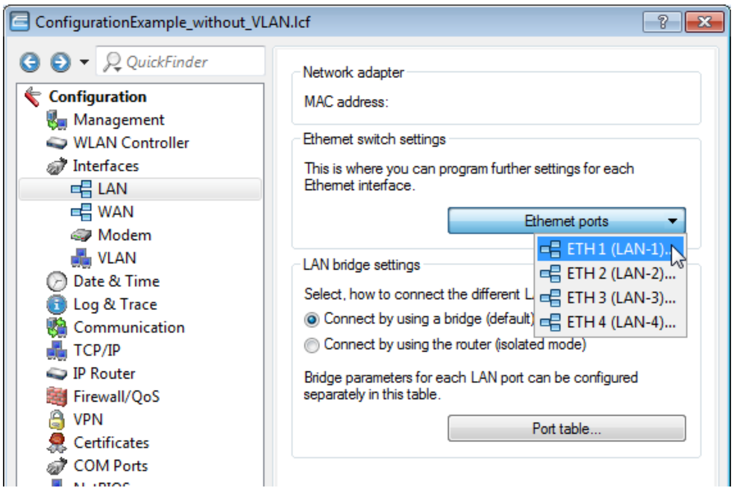
Location: ConferenceRoom

WLAN profile: COMPANY

Picture 7: “Access point table for overlay networks”

Configuring the interfaces on the WLC

5. Assign a separate logical LAN interface, e.g. 'LAN-1', to each physical Ethernet port. Make sure that the other Ethernet ports are not assigned to the same LAN interface. In LANconfig you find these settings under Configuration/Interfaces/LAN/Ethernet ports.



ConfigurationExample_without_VLAN.lcf

Network adapter

MAC address:

Ethernet switch settings

This is where you can program further settings for each Ethernet interface.

LAN bridge settings

Select, how to connect the different L

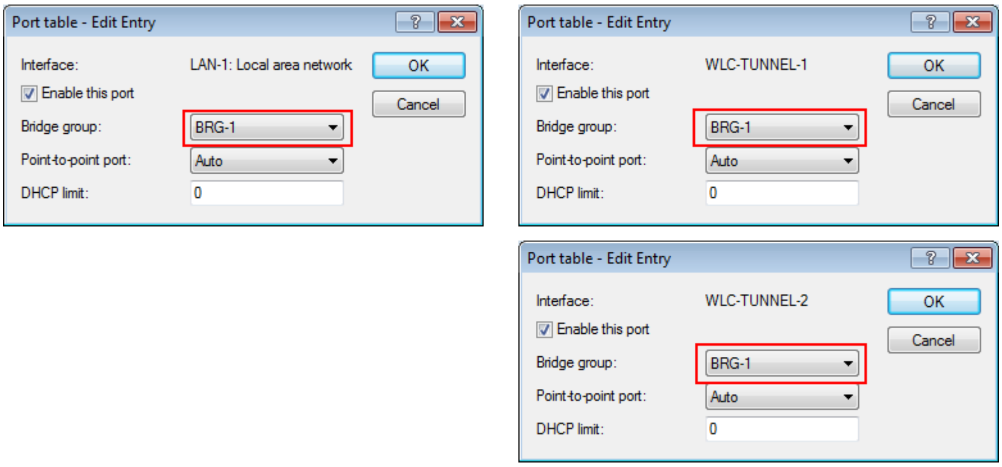
● Connect by using a bridge (default)

○ Connect by using the router (isolated mode)

Bridge parameters for each LAN port can be configured separately in this table.

Picture 8: “Ethernet setting for overlay networks”

6. Assign the logical LAN interface 'LAN-1' and the WLC tunnels 'WLC-tunnel-1' and 'WLC-tunnel-2' to the bridge-group 'BRG-1'. Make sure that the other LAN ports are not assigned to the same bridge group. In LANconfig you find these settings under Configuration/Interfaces/LAN/Port table.



Port table - Edit Entry

Interface: LAN-1: Local area network
☑ Enable this port
Bridge group: BRG-1
Point-to-point port: Auto
DHCP limit: 0

Port table - Edit Entry

Interface: WLC-TUNNEL-1
☑ Enable this port
Bridge group: BRG-1
Point-to-point port: Auto
DHCP limit: 0

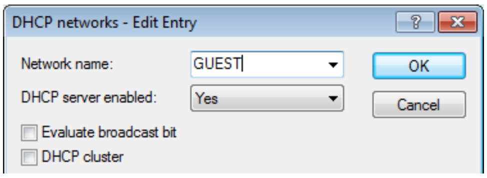
Port table - Edit Entry

Interface: WLC-TUNNEL-2
☑ Enable this port
Bridge group: BRG-1
Point-to-point port: Auto
DHCP limit: 0

Picture 9: “Port settings for overlay networks”

By default, the LAN interfaces and WLC tunnels do not belong to a bridge group. By assigning the LAN interface 'LAN-1' and the two WLC tunnels 'WLC-Tunnel-1' and 'WLC-Tunnel-2' to the bridge group 'BRG-1', the device transmits all data packets between LAN-1 and the WLC tunnels via the bridge.

7. The WLAN controller can optionally act as a DHCP server for the access points. To set this up, activate the DHCP server for the 'INTRANET'. In LANconfig you find these settings under Configuration/TCP/DHCP/DHCP networks.



DHCP networks - Edit Entry

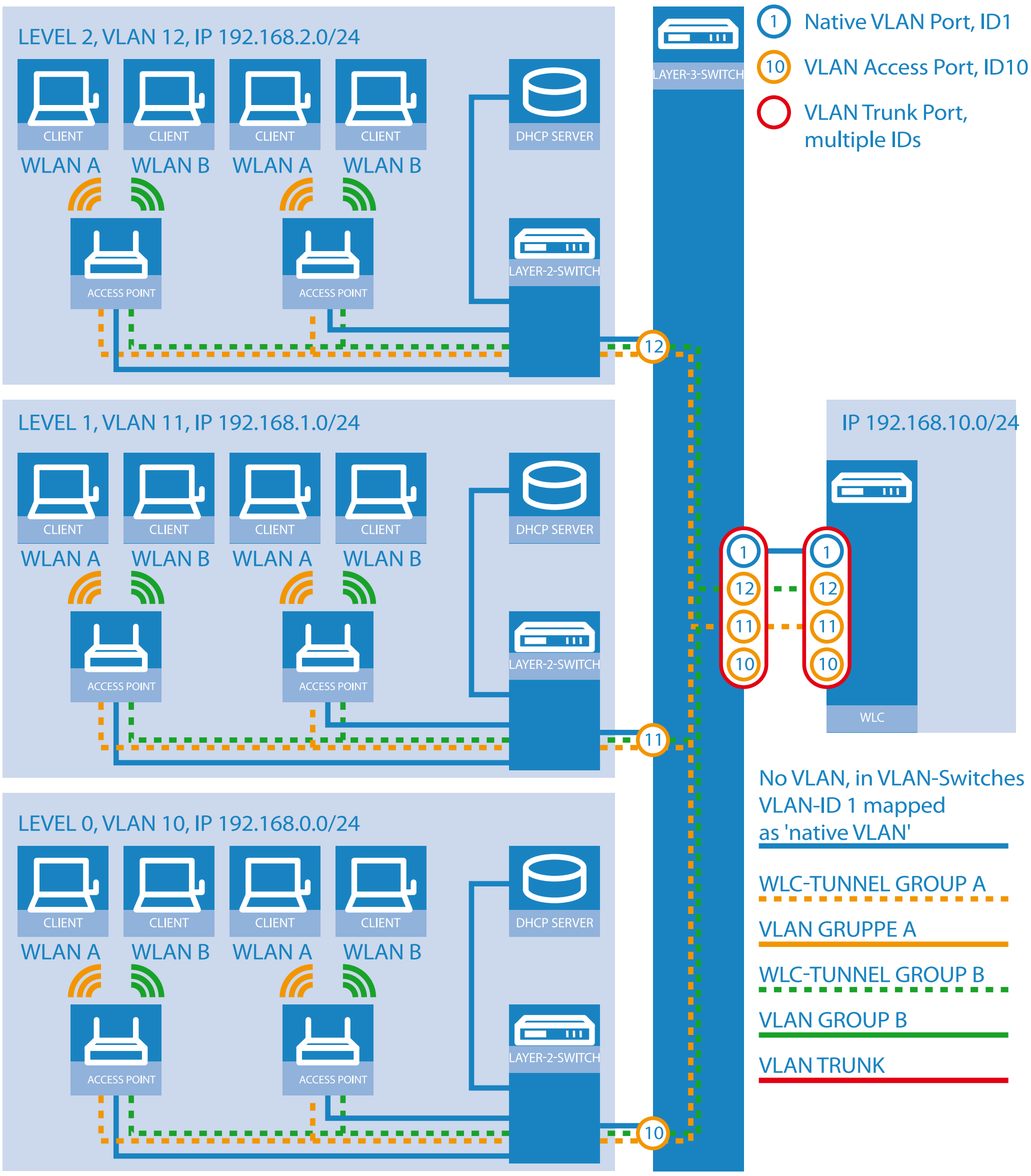
Network name: GUEST
DHCP server enabled: Yes
□ Evaluate broadcast bit
□ DHCP cluster

Picture 10: “DHCP settings for overlay networks”

Layer-3 roaming

Allowing payload data from the wireless LAN to pass-through the WLC tunnel to the controller enables roaming even beyond the limits of broadcast domains. In this example application, a layer-3 switch between the floors prevents the transmission of broadcasts, and thus separates the broadcast domains.

In this example, two user groups A and B each have access to their own WLAN (SSID). On all floors of the building, the access points provide two SSIDs, 'GROUP_A' and 'GROUP_B'.



Picture 11: "Example application: Layer-3 roaming"

The diagram shows a sample application with the following components:

- The network consists of three segments on separate floors of a building.
- A central layer-3 switch connects the segments and divides the network into three broadcast domains.
- Each segment uses its own IP address space and its own VLAN.
- Each segment operates a local DHCP server, which transmits the following information to the access points:
  - IP address of the gateway
  - IP address of the DNS server
  - Domain suffix

This information enables the access points to contact the WLC controller in another broadcast domain.

The aim of the configuration: When moving to another floor, a WLAN client that associates with a particular SSID is to retain access to its "own" WLAN, regardless of which access point is being used and regardless of the segment in which the client is located. Since the segments in this example use different IP address ranges, this scenario can only be implemented by managing the access points directly with the central WLAN controller via layer 3 and across the boundaries of the VLANs.

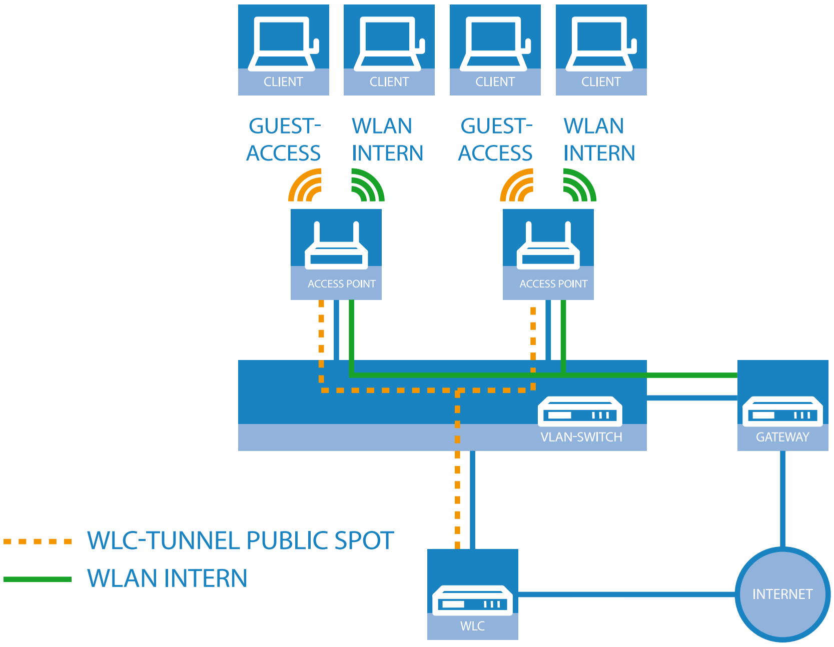
The configuration corresponds to the example Overlay network: Separating networks for access points without using VLAN.

WLAN controller with Public Spot

This scenario is based on the first scenario (overlay network) and enhances it to include specific settings for user authentication.

The configuration of a Public Spot can be greatly simplified if the payload data sent from the WLAN to the controller is routed through a WLC tunnel. A Public Spot can, for example, provide guests with Internet access in parallel with, but separated from, an internal wireless LAN.

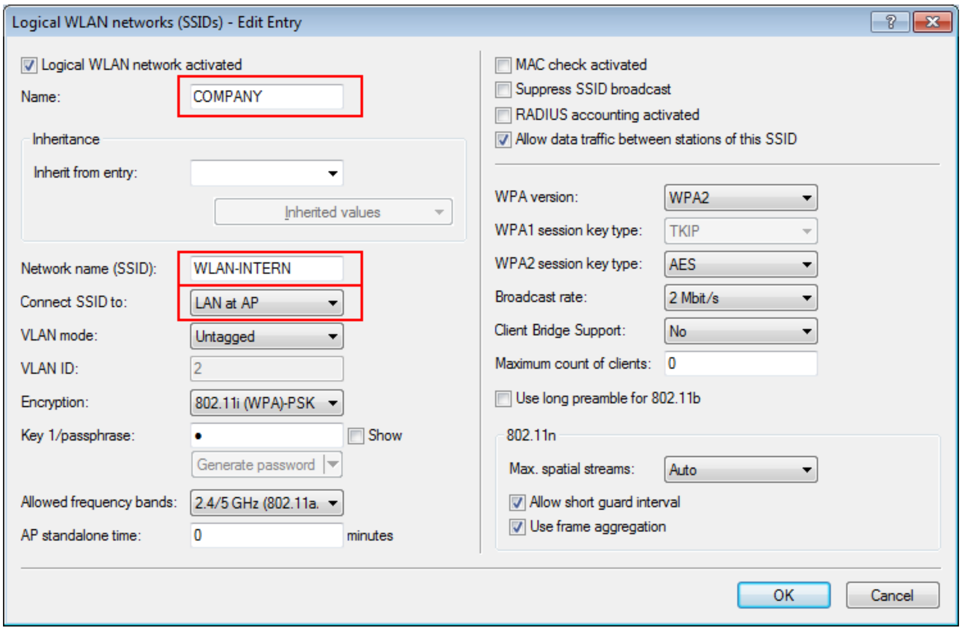
In this example, the employees of a company have access to a private WLAN (SSID), while the guests use a Public Spot to access the Internet. In all areas of the building, the access points provide two SSIDs, 'COMPANY' and 'GUESTS'.



Picture 12: “Example application: WLAN controller with Public Spot”

The aim of the configuration: A WLAN client that associates with the internal SSID should have access to all internal resources and the Internet via the central gateway. The access points break-out the payload data from the internal clients locally and pass it on directly to the LAN. The guests' WLAN clients associate with the Public Spot. The access points send the payload data from the guest clients through a WLC tunnel directly to the WLAN controller, which uses a separate WAN interface for Internet access.

1. The internal WLAN and the guest WLAN each require an entry to be created in the list of logical networks, each with a suitable name and the corresponding SSID. Link the SSID for internal use with the 'LAN at AP', and the SSID for guests with (for example) 'WLC-TUNNEL-1'. Disable encryption for the guest network SSID so that the guests' WLAN clients can associate with the Public Spot. You should also prevent inter-station traffic for this SSID. In LANconfig you find this setting under Configuration/WLAN Controller/Profiles/Logical WLAN networks (SSIDs).


Logical WLAN networks (SSIDs) - Edit Entry

☑ Logical WLAN network activated

Name: COMPANY

Inheritance

Inherit from entry:

Inherited values

Network name (SSID): WLAN-INTERN

Connect SSID to: LAN at AP

VLAN mode: Untagged

VLAN ID: 2

Encryption: 802.11i (WPA)-PSK

Key 1/passphrase: • □ Show

Generate password

Allowed frequency bands: 2.4/5 GHz (802.11a.

AP standalone time: 0 minutes

□ MAC check activated

□ Suppress SSID broadcast

□ RADIUS accounting activated

☑ Allow data traffic between stations of this SSID

WPA version: WPA2

WPA1 session key type: TKIP

WPA2 session key type: AES

Broadcast rate: 2 Mbit/s

Client Bridge Support: No

Maximum count of clients: 0

□ Use long preamble for 802.11b

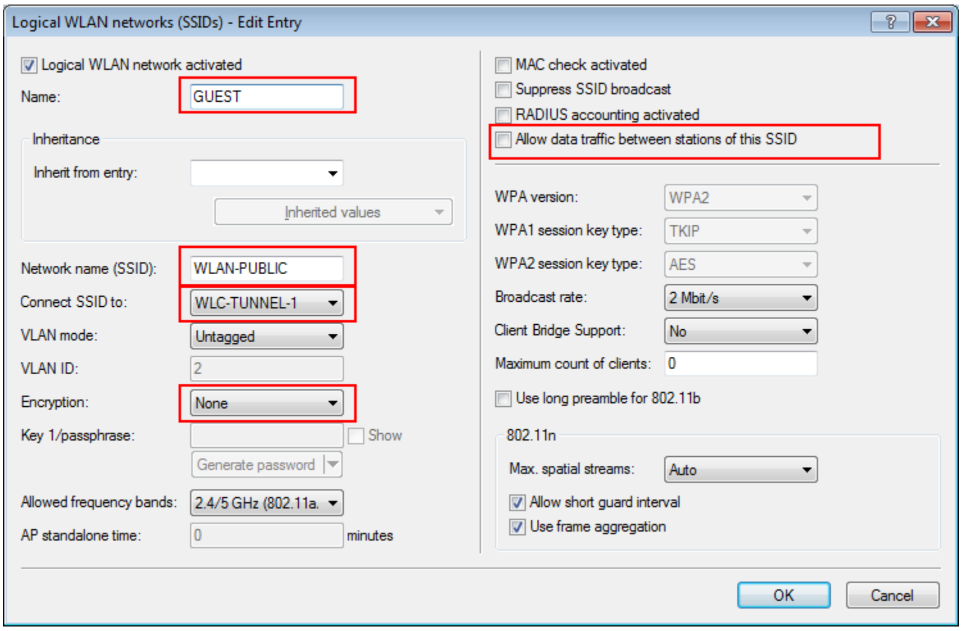
802.11n

Max. spatial streams: Auto

☑ Allow short guard interval

☑ Use frame aggregation

Picture 13: “Logical WLAN networks for internal use”


Logical WLAN networks (SSIDs) - Edit Entry

☑ Logical WLAN network activated

Name: GUEST

Inheritance

Inherit from entry:

Inherited values

Network name (SSID): WLAN-PUBLIC

Connect SSID to: WLC-TUNNEL-1

VLAN mode: Untagged

VLAN ID: 2

Encryption: None

Key 1/passphrase: □ Show

Generate password

Allowed frequency bands: 2.4/5 GHz (802.11a.

AP standalone time: 0 minutes

□ MAC check activated

□ Suppress SSID broadcast

□ RADIUS accounting activated

□ Allow data traffic between stations of this SSID

WPA version: WPA2

WPA1 session key type: TKIP

WPA2 session key type: AES

Broadcast rate: 2 Mbit/s

Client Bridge Support: No

Maximum count of clients: 0

□ Use long preamble for 802.11b

802.11n

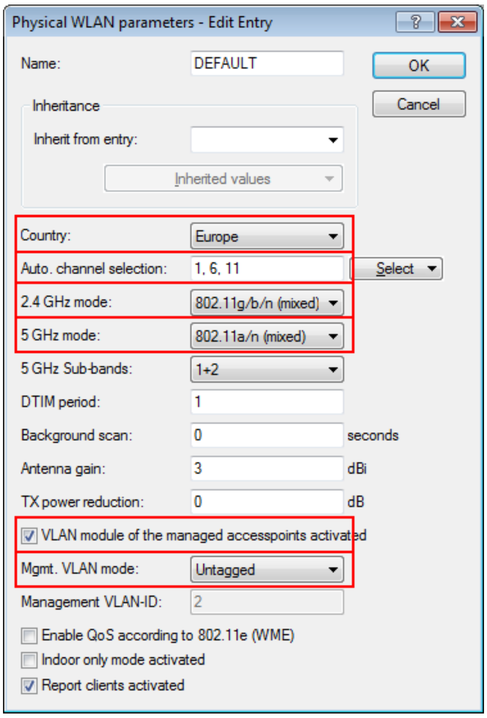
Max. spatial streams: Auto

☑ Allow short guard interval

☑ Use frame aggregation

Picture 14: “Logical WLAN networks for guest access accounts”

2. Create an entry in the list of physical WLAN parameters with the appropriate settings for your access points, such as the country 'Europe' with the channels 1, 6 and 11 in 802.11b/g/n and 802.11a/n in mixed mode. In LANconfig you find this setting under Configuration/WLAN Controller/Profiles/Physical WLAN parameters.



Physical WLAN parameters - Edit Entry

Name: DEFAULT

Inheritance

Inherit from entry:

Country: Europe

Auto. channel selection: 1, 6, 11

2.4 GHz mode: 802.11g/b/n (mixed)

5 GHz mode: 802.11a/n (mixed)

5 GHz Sub-bands: 1+2

DTIM period: 1

Background scan: 0 seconds

Antenna gain: 3 dBi

TX power reduction: 0 dB

☑ VLAN module of the managed accesspoints activated

Mgmt. VLAN mode: Untagged

Management VLAN-ID: 2

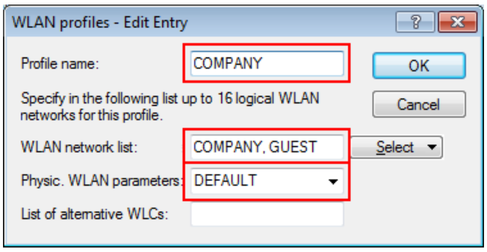
☐ Enable QoS according to 802.11e (WME)

☐ Indoor only mode activated

☑ Report clients activated

Picture 15: “Physical WLAN parameters for Public Spot APs”

3. Create a WLAN profile and give it a suitable name. Then assign the logical WLAN networks and the physical WLAN parameters created previously to this WLAN profile. In LANconfig you find this setting under Configuration/WLAN Controller/Profiles/WLAN profiles.



WLAN profiles - Edit Entry

Profile name: COMPANY

Specify in the following list up to 16 logical WLAN networks for this profile.

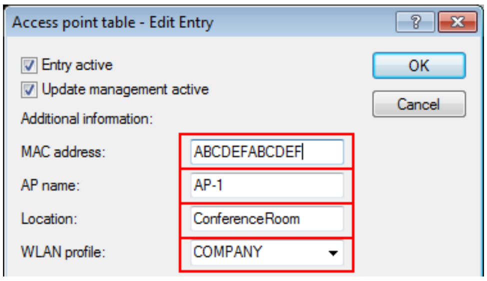
WLAN network list: COMPANY, GUEST

Physic. WLAN parameters: DEFAULT

List of alternative WLCs:

Picture 16: “WLAN profiles for Public Spot APs”

4. For each managed access point, create an entry in the access point table with a suitable name and the associated MAC address. Assign the WLAN profile created previously to this access point. In LANconfig you find this setting under Configuration/WLAN Controller/AP config./Access point table.



Access point table - Edit Entry

☑ Entry active

☑ Update management active

Additional information:

MAC address: ABCDEFABCDEF

AP name: AP-1

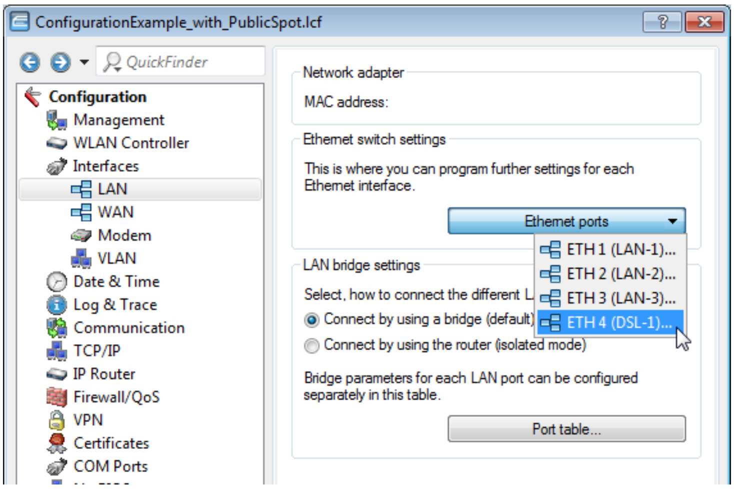
Location: ConferenceRoom

WLAN profile: COMPANY

Picture 17: “Access point table for Public Spot APs”

5. Assign a separate logical LAN interface, e.g. 'LAN-1', to each physical Ethernet port. Set the 4th Ethernet port to the logical interface 'DSL-1'. The WLAN controller will use this LAN interface for the

guest network Internet access. In LANconfig you find this setting under Configuration/Interfaces/LAN/Ethernet ports.



Network adapter

MAC address:

Ethernet switch settings

This is where you can program further settings for each Ethernet interface.

LAN bridge settings

Select, how to connect the different L

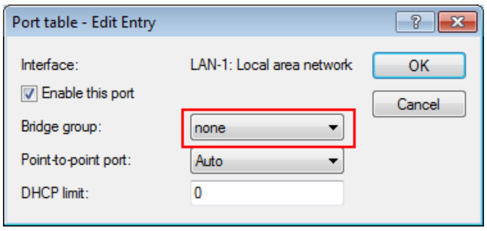
● Connect by using a bridge (default)

○ Connect by using the router (isolated mode)

Bridge parameters for each LAN port can be configured separately in this table.

Picture 18: “Ethernet settings for Public Spot APs”

6. Verify that the logical LAN interface 'WLC-tunnel-1' is not allocated to a bridge group. This ensures that the other LAN interfaces do not transmit any data to the Public Spot. In LANconfig you find this setting under Configuration/Interfaces/LAN/Port table.



Interface: LAN-1: Local area network

☑ Enable this port

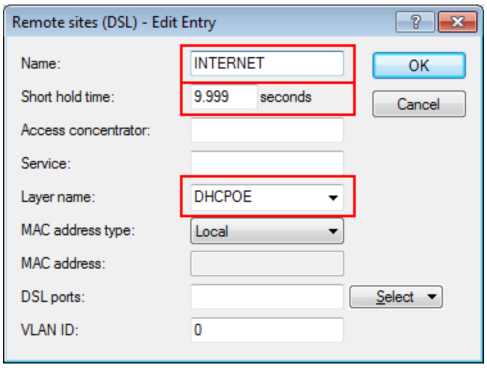
Bridge group: none

Point-to-point port: Auto

DHCP limit: 0

Picture 19: “Port settings for Public Spot APs”

7. For the guest Internet access, create an entry in the list of DSL remote sites with the hold time '9999' and the pre-defined layer 'DHCPOE '. This example assumes that Internet access is provided by a router with DHCP server. In LANconfig you find this setting under Configuration/Communications/Remote sites/Remote sites (DSL).



Name: INTERNET

Short hold time: 9.999 seconds

Access concentrator:

Service:

Layer name: DHCPOE

MAC address type: Local

MAC address:

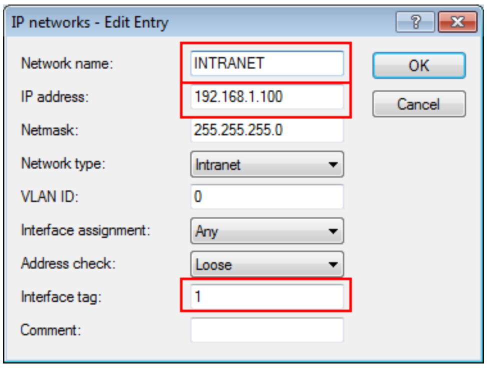
DSL ports:

VLAN ID: 0

Picture 20: “Remote site for Internet access”

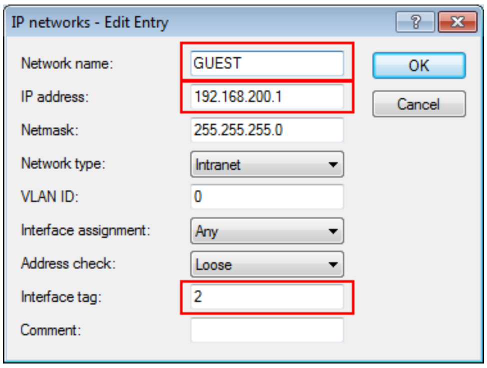
8. For internal users, create the IP network 'INTRANET' with (for example) the IP address '192.168.1.100' and the interface tag '1'. For the guest access, create the IP network 'GUEST-ACCESS' with (for example) the IP address of '192.168.200.1' and the interface tag '2'. The virtual

router in the WLAN controller uses the interface tags to separate the routes for the two networks. In LANconfig you find this setting under Configuration/TCP-IP/General/IP networks.



Network name: INTRANET
IP address: 192.168.1.100
Netmask: 255.255.255.0
Network type: Intranet
VLAN ID: 0
Interface assignment: Any
Address check: Loose
Interface tag: 1
Comment:

Picture 21: “IP network for internal use”

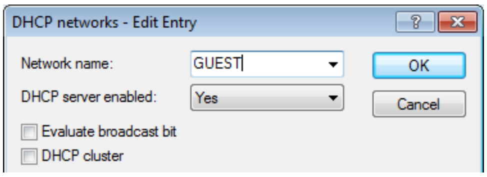


Network name: GUEST
IP address: 192.168.200.1
Netmask: 255.255.255.0
Network type: Intranet
VLAN ID: 0
Interface assignment: Any
Address check: Loose
Interface tag: 2
Comment:

Picture 22: “IP network for guest access”

9. The WLAN controller can act as a DHCP server for access points and the associated WLAN clients. To set this up, activate the DHCP server for the 'INTRANET' and the 'GUEST-ACCESS'. In LANconfig you find this setting under Configuration/TCP/DHCP/DHCP networks.

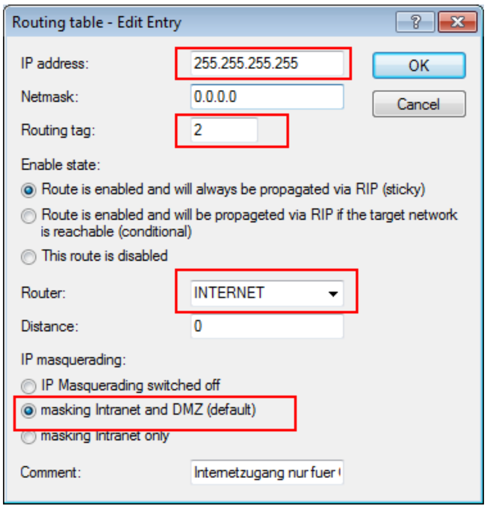
Activation of the DHCP server is obligatory for the guest network and optional for the internal network. There are other ways of realizing a DHCP server for the internal network.



Network name: GUEST
DHCP server enabled: Yes
□ Evaluate broadcast bit
□ DHCP cluster

Picture 23: “DHCP network for guest access”

10. Create a new default route in the routing table to direct the data from the guest network to the Internet connection used by the WLAN controller. Select the routing tag '2' and the router 'Internet'. Also activate the option 'Masking intranet and DMZ (default)'. In LANconfig you find this setting under Configuration/IP router/Routing/Routing table.



Routing table - Edit Entry

IP address: 255.255.255.255

Netmask: 0.0.0.0

Routing tag: 2

Enable state:

● Route is enabled and will always be propagated via RIP (sticky)

○ Route is enabled and will be propagated via RIP if the target network is reachable (conditional)

○ This route is disabled

Router: INTERNET

Distance: 0

IP masquerading:

○ IP Masquerading switched off

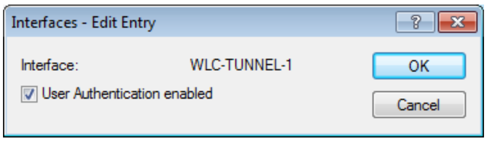
● masking Intranet and DMZ (default)

○ masking Intranet only

Comment: Internetzugang nur fuer (

Picture 24: “Routing entry for Internet access”

11. Activate the Public Spot user authentication for the logical LAN interface 'WLC-Tunnel-1'. In LANconfig you find this setting under Configuration/Public Spot/Public Spot.



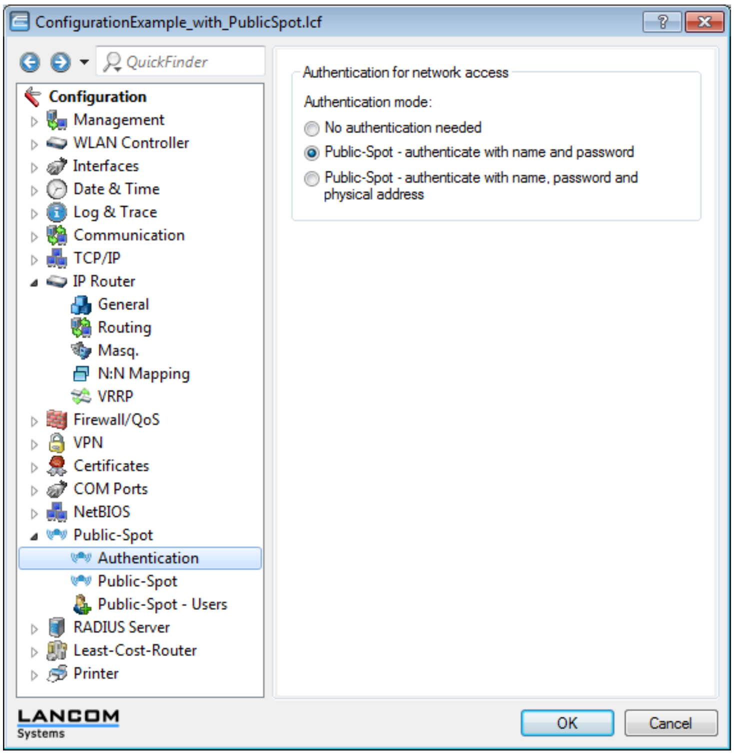
Interfaces - Edit Entry

Interface: WLC-TUNNEL-1

☑ User Authentication enabled

Picture 25: “Activation of user authentication for the WLC tunnel”

12. The final step is to enable authentication via the Public Spot for the WLAN controller. In LANconfig you find this setting under Configuration/Public Spot/Authentication.



ConfigurationExample_with_PublicSpot.lcf

Authentication for network access

Authentication mode:

○ No authentication needed

● Public-Spot - authenticate with name and password

○ Public-Spot - authenticate with name, password and physical address

Picture 26: “Activation of authentication via Public Spot”

In addition to configuring the WLAN controller, you must also configure the Public Spot either to use the internal user list or to use a RADIUS server, according to your needs.

4.2 Alarm limits for WLAN devices

Typical situations that cause problems in the wireless LAN environment include a decrease in signal strength below a certain threshold, the percentage of lost packets exceeding a certain threshold, or packets frequently having to be resent—all of which can greatly reduce the available bandwidth.

In order to recognize and react to these situations, LANCOM Wireless devices now feature alarms to provide information on the over- or undershooting of threshold values.

ⓘ A connection is not absolutely rated as poor. The assessment always depends on the parameters that are specified. It should be noted that threshold limits that are too high or too low can lead to incorrect evaluation, and that a very large number of false alarms could be the result. A certain amount of packet loss and fluctuating signal strengths are to be expected even for stable wireless connections.

Threshold limits can be set for each individual SSID and point-to-point link supported by an access point. These limits are used to evaluate a client's connection to the SSID and the connection to a P2P remote.

4.2.1 Additions to the menu system

2.23.20.13 Network alarm limits

This table contains the settings for the network alarm limits for the device's logical WLAN networks (SSIDs).

Telnet path: /Setup/Interfaces/WLAN

2.23.20.13.1 Interface

Select the logical WLAN network (SSID) for which you want to edit the network alarm limits.

Telnet path: /Setup/Interfaces/WLAN/Network-Alarm-Limits

Possible values:

- Choose from the SSIDs available in the device, e.g. WLAN-1, WLAN-2, etc.

2.23.20.13.2 Phy signal

The negative threshold value for the signal level of the corresponding SSID. If the value falls below this threshold, an alarm is issued. Setting this value to 0 deactivates the check.

Telnet path: /Setup/Interfaces/WLAN/Network-Alarm-Limits

Possible values:

- 3 numerical characters

Default: 0

2.23.20.13.3 Total retries

The threshold value for the total number of transmission retries for the corresponding SSID. Once the value is reached, an alarm is issued. Setting this value to 0 deactivates the check.

Telnet path: /Setup/Interfaces/WLAN/Network-Alarm-Limits

Possible values:

- 4 numeric characters to specify the repetitions in per mille

Default: 0 per mille

2.23.20.13.4 TX errors

The total number of lost packets for the corresponding SSID. Once the value is reached, an alarm is issued. Setting this value to 0 deactivates the check.

Telnet path: /Setup/Interfaces/WLAN/Network-Alarm-Limits

Possible values:

- 4 numeric characters to specify the repetitions in per mille

Default: 0 per mille

4.3 Interpoint alarm limits

4.3.1 Additions to the menu system

2.23.20.14 Interpoint alarm limits

This table contains the settings for the interpoint alarm limits for the device's P2P connections (SSIDs).

Telnet path: /Setup/Interfaces/WLAN

2.23.20.14.1 Interface

Select the P2P connection here for which you wish to set the interpoint alarm limits.

Telnet path: /Setup/Interfaces/WLAN/Interpoint-Alarm-Limits

Possible values:

- Choose from the P2P connections available in the device, e.g. P2P-1, P2P-2, etc.

2.23.20.14.2 Phy signal

The negative threshold value for the signal level of the corresponding P2P connection. If the value falls below this threshold, an alarm is issued. Setting this value to 0 deactivates the check.

Telnet path: /Setup/Interfaces/WLAN/Interpoint-Alarm-Limits

Possible values:

- 3 numerical characters

Default: 0

2.23.20.14.3 Total retries

The threshold value for the total number of transmission retries for the corresponding P2P connection. Once the value is reached, an alarm is issued. Setting this value to 0 deactivates the check.

Telnet path: /Setup/Interfaces/WLAN/Interpoint-Alarm-Limits

Possible values:

- 4 numeric characters to specify the repetitions in per mille

Default: 0 per mille

2.23.20.14.4 TX errors

The total number of lost packets for the corresponding P2P connection. Once the value is reached, an alarm is issued. Setting this value to 0 deactivates the check.

Telnet path: /Setup/Interfaces/WLAN/Interpoint-Alarm-Limits

Possible values:

- 4 numeric characters to specify the repetitions in per mille

Default: 0 per mille

5 UTM

5.1 Enhancements and changes to the content filter

5.1.1 Content filter for HTTPS pages

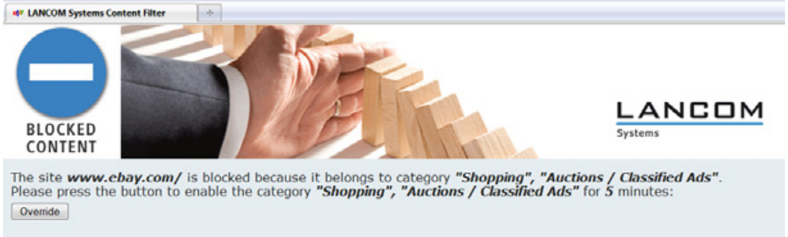
The first version content filter supported only HTTP pages, whereas LCOS 8.50 now also supports HTTPS pages.

By default the content filter uses the firewall rule 'CONTENT-FILTER'. When the content filter option is activated on a device with LCOS 8.50 or newer, the rule refers to the target 'WEB', which monitors outbound HTTP and HTTPS connections on ports 80 and 443.

ⓘ If you enabled the content filter option on a device with an LCOS version oder than 8.50, the firewall rule only uses HTTP port 80 as the target. If this is the case, then you can reset the target of the firewall rule to 'WEB' so that outgoing HTTPS connections are also checked with the content filter.

5.1.2 One-click override

The override function allows a website to be accessed even though it is classified as forbidden.With this feature enabled, the content filter informs the user why the page was blocked and also provides the option of unlocking the category for the set period of time.



The site ***www.ebay.com/*** is blocked because it belongs to category ***"Shopping", "Auctions / Classified Ads"***.
Please press the button to enable the category ***"Shopping", "Auctions / Classified Ads"*** for ***5*** minutes:

In case of an override, the content filter displays the relevant entry from the block-text table and directly below this, the text from the override-text table together with the 'Override' button. When the user clicks this button the content filter forwards the user to the requested page, if possible. If it is not possible to forward the user to the requested page, the content filter displays an error page.

In the LCOS versions earlier than version 8.50, the block texts, override texts and and error texts and associated attributes were used slightly differently than in the LCOS versions 8.50 and newer.

ⓘ When updating to LCOS 8.50, you should check the texts in the different tables and adjust them if necessary.

Depending on the application, the arguments relating to HTTP requests are transmitted in different ways according to the requested URL. In most cases, the browser sends a GET request with the arguments in the URL (e.g. a search term). In the case of an override, the content filter is able to forward GET requests as all the required information is included in the URL. However, in some cases the browser sends POST requests, for example for file uploads where the data to be transmitted is in the header of the request. In this case, the information that should be forwarded in case of an override is not contained in the URL. The content filter can only successfully forward post requests in case of an override if JavaScript has been enabled in the user's browser. Browsers based on the HTML rendering library 'WebKit' do not support the override of post requests with JavaScript.

ⓘ Content filters operating on a system without JavaScript activated or with WebKit browsers display an error page after clicking on the 'Override' button. These users can then click the button for reloading the web page and forwarding will then succeed.

The following sections show the changes made to the content filter menu system.

2.41.2.2.21 URL to show on error

This is where you can enter an alternative URL. In the event of an error, the URL entered here will be displayed instead of the usual web site. You can use this external HTML page to display your company's corporate design, for example, or to perform functions such as JavaScript routines, etc. You can also use the same tags here as used in the override text. If you do not make any entry here, the default page stored in the device will be displayed..

Telnet path: /Setup/UTM/Content-Filter/Global-Settings

Possible values:

- Valid URL address

Default: Blank

2.41.2.2.21 Loopback to use on error

This is where you can configure an optional sender address for the error URL to be used instead of the one that would normally be automatically selected for this target address. If you have configured loopback addresses, you can specify them here as sender address.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings

English description: Loopback-To-Use-On-Override

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ (Note: If there is an interface named "DMZ", its address will be taken).
- LB0 ... LBF for the 16 loopback addresses
- GUEST
- Any IP address in the form x.x.x.x

Default: Blank

The sender address specified here is used unmasked for every remote station.

2.41.2.2.10.2 Text

Enter the text that you wish to use as blocking text for this language.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/Block-Text

Possible values:

- 254 alphanumerical characters

Default:

Blank

Special values:

You can also use special tags for blocking text if you wish to display different pages depending on the reason why the web site was blocked (e.g. forbidden category or entry in the blacklist).

The following tags can be used as tag values:

- <CF-URL/> for the forbidden URL
- <CF-HOST/> or <CF-DOMAIN/> displays the host or the domain for the allowed URL. The tags are of equal value and their use is optional.
- <CF-CATEGORIES/> for the list of categories why the web site was blocked
- <CF-PROFILE/> for the profile name
- <CF-DURATION/> displays the override duration in minutes.
- <CF-OVERRIDEURL/> for the URL used to activate the URL (this can be integrated in a simple <a> tag or in a button)
- <CF-LINK/> adds a link for activating the override
- <CF-BUTTON/> for a button for activating the override

You can use a tag with attributes to display or hide parts of the HTML document: <CF-IF att1 att2> ... </CF-IF>.

Possible attributes are:

- BLACKLIST: If the site was blocked because it is in the profile blacklist
- FORBIDDEN: If the site was blocked due to one of its categories
- CATEGORY: When the override type is "Category" and the override was successful
- ERR: If an error has occurred.

Since there are separate text tables for the blocking page and the error page, this tag only makes sense if you have configured an alternative URL to show on blocking.

- OVERRIDEOK: If users have been allowed an override (in this case, the page should display an appropriate button)

If several attributes are defined in one tag, the section will be displayed if at least one of these conditions is met. All tags and attributes can be abbreviated to the first two letters (e.g. CF-CA or CF-IF BL). This is necessary as the blocking text may only contain a maximum of 254 characters.

Example:

- <CF-URL/> is blocked because it matches the categories <CF-CA/>.</p><p>Your content profile is <CF-PR/>.</p><p><CF-IF OVERRIDEOK></p><p><CF-BU/></CF-IF>

ⓘ The tags described here can also be used in external HTML pages (alternative URLs to show on blocking).

2.41.2.2.19.2 Text

Enter the text that you wish to use as error text for this language.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/Error-Text

Possible values:

254 alphanumerical characters

Default:

Blank

Special values:

You can also use HTML tags for the error text.

The following empty element tags can be used as tag values:

- <CF-URL/> for the forbidden URL
- <CF-HOST/> or <CF-DOMAIN/> displays the host or the domain for the forbidden URL. The tags are of equal value and their use is optional.
- <CF-DURATION/> displays the override duration in minutes.
- <CF-PROFILE/> for the profile name
- <CF-ERROR/> for the error message

You can use a tag with attributes to display or hide parts of the HTML document: <CF-IF att1 att2> ... </CF-IF>.

Possible attributes are:

- CHECKERROR: The error occurred while checking the URL
- OVERRIDEERROR: The error occurred while approving an override

Example:

<CF-URL/> is blocked because an error has occurred:</p><p><CF-ERROR/>

<CF-URL>: Blocked URL <CF-HOST> or <CF-DOMAIN>: Host part of the blocked URL <CF-PROFILE>: User content-filter profile <CF-DURATION>: Override time in minutes <CF-ERROR>: Error message <CF-IF> to </CF-IF>: Conditional evaluation of the following parameters with the logical OR: CHECKERROR: The error occurred while checking the URL (as earlier) OVERRIDE ERROR: The error occurred while approving an override

2.41.2.2.20.2 Text

Enter the text that you wish to use as override text for this language.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings/Override-Text

Possible values:

- 254 alphanumerical characters

Default:

Blank

Special values:

You can also use HTML tags for blocking text if you wish to display different pages depending on the reason why the web site was blocked (e.g. forbidden category or entry in the blacklist).

The following tags can be used as tag values:

- <CF-URL/> for the originally forbidden URL that is now allowed
- <CF-CATEGORIES/> for the list of categories that have now been allowed as a result of the override (except if domain override is specified).
- <CF-BUTTON/> displays an override button that forwards the browser to the original URL.
- <CF-BUTTON/> displays an override link that forwards the browser to the original URL.
- <CF-HOST/> or <CF-DOMAIN/> displays the host or the domain for the allowed URL. The tags are of equal value and their use is optional.
- <CF-ERROR/> generates an error message in the event that the override fails.
- <CF-DURATION/> displays the override duration in minutes.

You can use a tag with attributes to display or hide parts of the HTML document: <CF-IF att1 att2> ... </CF-IF>.

Attributes can be:

- BLACKLIST: If the site was blocked because it is in the profile blacklist
- FORBIDDEN: If the site was blocked due to one of its categories
- CATEGORY: When the override type is "Category" and the override was successful
- DOMAIN: When the override type is "Domain" and the override was successful
- BOTH: When the override type is "Category-and-Domain" and the override was successful
- ERROR: When the override fails
- OK: When either CATEGORY or DOMAIN or BOTH are applicable

If several attributes are defined in one tag, the section should be displayed if at least one of these conditions is met. All tags and attributes can be abbreviated to the first two letters (e.g. CF-CA or CF-IF BL). This is necessary as the blocking text may only contain a maximum of 254 characters.

Example:

<CF-IF CA BO>The categories <CF-CAT/> are</CF-IF><CF-IF BO> in the domain <CF-DO/></CF-IF><CF-IF DO>The domain <CF-DO/> is</CF-IF><CF-IF OK> released for <CF-DU/> minutes.</p><p><CF-LI/></CF-IF><CF-IF ERR>Override error:</p><p><CF-ERR/></CF-IF>

6 Project management

6.1 Custom Rollout Wizard

6.1.1 Introduction

In large-scale networking projects, administrators often have to install many devices of the same or similar type at different locations. To reduce or avoid the need to be personally present at the various locations, administrators often prepare the equipment at the central office for rollout. On location, an employee or a customer then runs a special wizard that sets the site-related parts of the configuration and puts the device into operation.

With a special instruction language, LCOS gives administrators the ability to define highly complex wizards. Custom wizards support the following functions:

- Definition of any internal variables
- Conditional branches
- Conditional goto instructions to any URL
- Conditional display of notices
- Runs all (non-interactive) actions that are available with the LCOS command line interface
- Read-out current values from the configuration in the devices
- Write new values to the configuration in the devices
- Status checks such as checking the time in the device
- Connection checks, e.g. the successful VPN connection to a specific remote site

In compliance with the rules of the instruction language, the administrator compiles a new Wizard in the form of a text file, which is then loaded into the device.The user on-site can run the custom wizard from WEBconfig by using the appropriate name.

ⓘ You can restrict certain administrator accounts to be available specifically under the Rollout Wizard only, allowing even inexperienced users to configure certain functions without allowing access to the complete configuration.

ⓘ At the time of the release of LCOS 8.50, users of the following devices can use the instruction language to customize wizards:

- LANCOM 1681V
- LANCOM 1711+ VPN
- LANCOM 1721+ VPN
- LANCOM 1821n Wireless
- LANCOM 1811n Wireless
- LANCOM 1751 UMTS

6.1.2 Structure of the custom wizard

The instructions that describe a custom wizard consist of the following sections:

- String tables with the necessary texts in English and German.
- A definition of the wizard.
- Any number of sections describing the HTML pages that the wizard is to display.
- An initialization section, which defines the actions when you start the wizard.
- A concluding section, which defines the actions when you stop the wizard.

Note the following conventions for the instructions that describe the wizard:

- The elements of the instructions exactly follow the structure given above.
- The text file with the instructions is encoded in ISO 8859-1.
- Comments start with a semicolon and serve only to improve the readability of the instructions.

- Internal variables begin with the key word `wizard.` (Including the dot) and store information for the internal processing of the wizard.
- Configuration variables begin with the keyword `config.` (including the dot) and read out information from the current device configuration, or they write them to the current configuration. Enter the configuration variables in one of the following forms:
  - Dedicated parameters in the configuration are referenced via `config.1.<SNMP-ID>`, for example `config.1.2.1` to access the device name (to be found in the menu under /setup/name)

One way to find the SNMP-ID for a parameter in the configuration is to enter the command `ls -a` at the command line in the corresponding submenu.

  - You can reference the values in a table with:

    `config.^.<SNMP-ID>.<Line>.ID:<Column>`

    Example for finding the value in the first line and the column with ID '2' in the routing table '1.2.8.2':

    `config.1.2.8.2.1.ID:2`

  - If you do not know the ID of the column, an alternative for you to reference the values in a table is to enter:

    `config.1.<SNMP-ID>.<Line>.<Column>`

    Example for finding the value in the first line and second column:

    `config.1.2.8.2.1.2`

  - If you do not know which line in the table you need, you can reference the values in a table via a known value in the first column:

    `config.<SNMP-ID>."<Known-Value>".ID:<Column>`

    Example for finding the value in the column with ID '2' on the line with the value of the default route in its first column:

    `config.1.2.8.2."255.255.255.0".ID:2`

    If the table contains multiple rows with the same value in the first column, then the configuration variable references the first of these lines.

  - If the required line in the table is only defined after the user has entered input into the wizard, you can reference the value in the table by using a variable with:

    `config.<SNMP-ID>.\"<Internal-Variable>\".ID:<Column>`

    Example for finding the line whose first column contains a value that agrees with the current value of the internal variable wizard.target_network:

    `config.1.2.8.2."\wizard.target_network"\.ID:2`

- Device-property variables begin with the key word `device.` (including the dot) and are used to read-out specific properties from the device. For more information about the device variables, see the Using device properties as variables.

6.1.3 String tables

The instructions for the custom wizard basically define the texts that are to be displayed in German and English.

The line `stringtable "English"` delivers the English text, the line `stringtable "German"` delivers the German texts. Each string definition consists of the keyword `string`, followed by the name of the string and the value enclosed by double inverted commas.

The following example shows the string tables with just one entry:

```
; -String tables start-----------------------------------------------
   stringtable "English"
   string title_test, "Test wizard"
   stringtable "Deutsch"
   string title_test, "Test-Assistent"
; -String tables end------------------------------------------------
```

The interpreter of the instructions that describe the custom wizard in LCOS requires all texts to contain a German and an English definition. LCOS will not execute the wizard if an entry in the English string table is not accompanied by an entry of the same name in the German string table (or vice versa).

6.1.4 Definition of the wizard

The definition specifies the name of the wizard. The keyword `wizard` precedes the internal name in double inverted commas followed by the reference to an entry in the string table (String tables). The wizard displays the external name defined by this string when the HTML page is executed:

```
; -Wizard Definition Start---------------------------
   wizard "My_Test-Wizard", title_test
; -Wizard Definition End----------------------------
```

6.1.5 Sections

The sections represent the actual HTML pages that are displayed when the wizard is executed in the user's browser.

Each section begins with the keyword `section` and ends with the beginning of the next section. The last section ends at the beginning of the 'on-init' area, i.e. there is no explicit keyword for the end.

The sections include the following elements in any order and quantity:

- Conditions
- Optional freely definable name of the section, starting with the keyword `label`, followed by a string of upper- and lowercase letters and underscores '_':

  ```
  Label My_RolloutAssistent
  ```

The instruction set for the wizard can use the freely definable name as a goto target.

- Static text starting with the keyword `static_text` followed by a reference to an entry in the string table (String tables):

  ```
  static_text str.conf_general
  ```

- Fields for different data types such as text or IP address, check boxes, radio buttons, selection lists, etc.

Information on the various fields can be found in the "Fields" section.

- Actions performed by the wizard in different situations depending on the keyword at the beginning of the block:
  - on_show: The wizard performs the actions in this block before a section (HTML page) is displayed.
  - on_skip: The wizard performs the actions in this block if a section (HTML page) is not to be displayed due to conditions contained within it.
  - on_next: The wizard performs the actions in this block if the user clicks on 'Next' in the section (HTML page).
  - on_back: The wizard performs the actions in this block if the user clicks on 'Back' in the section (HTML page).

Notes on the structure of the blocks with the actions and the elements in them are to be found in the Actions section.

6.1.6 Conditions

You can specify any number of conditions for an element. Conditions in different lines are AND operators; conditions in one line are OR operators.

The instructions for the wizard can add conditions to any element in a section. Conditions always refer to the previous element. They consist of a class specifier and one or more condition patterns. A pattern consists of two operands and one operator.

If a condition contains multiple condition patterns in one line, the wizard evaluates this expression as an OR operator.

If the instructions contains multiple conditions relating to a parent element on separate lines, the wizard assesses the expression to be an AND operation.

The instructions can include the following classes:

- `only-if`: The preceding element is only executed or displayed when at least one of the following condition patterns is fulfilled.
- `skip-if`: The preceding element is not executed or displayed when all of the following condition patterns are fulfilled.

The condition pattern can contain the following operands:

- Static text
- Internal variables of the wizard
- Variables for referencing values from the current configuration of the device (configuration variables)
- The character '*' as a wildcard

The condition pattern can contain the following operators:

- `equal`: Checks if the two operands are equal.
- `exists`: Checks if the specified configuration variable is set, i.e. that the value of the parameter in the configuration is not empty.
- `empty`: Checks if the first operand is empty. The second operand is specified as a wildcard '*'.
- `contains`: Checks if the first operand contains the second operand.
- `!`: Negates the condition.

Examples:

The following condition only displays the section if the internal variable 'wizard.test_select' is equal to '0'.

```
section
only_if wizard.test_select, "0", equal
```

The following condition sets the internal variable 'wizard.intranet_name' to the value 'INTRANET' if this variable is empty.

```
set wizard.intranet_name, "INTRANET" only_if wizard.intranet_name, *,
empty
```

The following condition sets the internal variable 'wizard.target_1' to the value 'TARGET_1' if the internal variable 'wizard.select_target' is set either to '1' or '5'.

```
set wizard.target_1, "TARGET_1" only_if wizard.select_target, "1",
equal, wizard.select_target, "5", equal
```

6.1.7 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.

`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 (see LCOS).

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

6.1.8 Variables

In some attributes of the fields you can use variables to replace the value of the attribute with another string or supplement it with an additional string.

to insert an internal variable into the value of an attribute, use the syntax `$(VariableName)`. To insert the user name from the internal variable `wizard.username` into a URL, add the following attribute:

```
http://host/directory?param=$(username)
```

To insert a predefined variable into the value of an attribute, use the syntax `%VariableName`. You can use the following predefined variables in the attributes:

- `%` inserts a percent sign.
- `f` inserts the version and the date of the firmware currently active in the device.
- `r` inserts the hardware release of the device.
- `v` inserts the version of the loader currently active in the device.
- `m` inserts the MAC address of the device.
- `s` inserts the serial number of the device.
- `n` inserts the name of the device.
- `l` inserts the location of the device.
- `d` inserts the type of the device.

6.1.9 Actions

The wizard uses actions to change values in the device configuration.

One or more conditions can be defined for any action. If these conditions are met, the wizard performs the action.

set

Syntax:

- `set $target, $sourcelist`
- `set $target, $number, add`
- `set $target, $number, sub`

This action replaces the content of the target variable with the specified source. The source contains a comma-separated list of variables or text strings.

If the target variable is a single configuration parameter, specify only one value as the source. Other values are ignored.

If the target variable is a table, you should first specify the value in the source from the line that the wizard should change. The wizard searches the first index column for this value and it changes the first line in which it finds this value. If the wizard does not find a line with the matching value, it adds a new line to the table.

If the target variable is a numeric value, you can use the `add` or `sub` action to add or subtract the amount defined as `$number`.

Examples

The following action sets the default route to the desired values:

```
set config.1.2.8.2, "255.255.255.255", "0.0.0.0", "0", "INTERNET", "0",
"on", "Yes", ""
```

The following action increases the value of the ARP aging minutes to '5':

```
set config.1.2.7.11, "5", add
```

The following action reduces the value of the ARP aging minutes by '5':

```
set config.1.2.7.11, "5", sub
```

del

This action clears the contents of the target variable. If this variable is a table, enter the value from the first index column in the line that is to be deleted.

Example

The following action deletes the default route from the routing table:

```
del config.1.2.8.2, "255.255.255.0"
```

cat

This action lists the content of the source variables after the target variable.

Example

The following action adds the content of the variables `wizard.user` and the variable `wizard.name`:

```
cat wizard.name, wizard.user
```

cut

This action removes a certain number of characters from the target variables. Enter as a parameter the position of the character to be deleted counting from the left and, optionally, the number of characters to be deleted.

Examples

The following action will delete all characters in the variable `wizard.name` after the 2nd character.

```
cut wizard.name, 2
```

The following action will delete all characters in the variable `wizard.name` exactly 4 characters after the 2nd character.

```
cut wizard.name, 2, 4
```

trigger_config_change

Depending on the part of the firmware that is affected, changes by the wizard to the configuration do not take immediate effect, as some modules use internal structures for the configuration.

The action `trigger_config_change` triggers an update to these internal structures. You should insert this action into a section if you want to make sure that the configuration has been updated when you change a page in the Rollout Wizard.

When you exit, the wizard automatically executes this action.

exec

The string that follows this is executed as a command on the console. In this case variables can be used in the string, for example to start a LoadScript.

6.1.10 Trace for rollout wizards

The HTML pages of the wizard only display the results of internal processing. While the wizard is being built, the trace can provide additional information to the administrator which could be used for further optimization, for example about the analysis of the various conditions.

Start trace from the command line using the command `trace + rollout-wizard`.

6.1.11 Using user-defined HTML templates

An an option, the appearance of the wizard can be adapted to your company's design guidelines by uploading a customized HTML template into the device. The template can specify the basic structure of HTML pages and the design of colors, fonts, etc. by means of CSS rules.

Two fixed tags in the HTML template are used to insert the contents from the wizard into the respective HTML pages:

- `<WIZARD_LOGO>`: The wizard inserts the logo (GIF, JPEG or PNG format) as saved to the device under 'WEBconfig/File management/Upload certificate or file'.
- `<WIZARD_CONTENT>`: This tag marks the point where the wizard inserts the contents of the sections in the form of a two-column table with the corresponding buttons.

A very simple example of an HTML template looks like this:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/
html4/strict.dtd">
```

```
   <html>
     <head>
       <title>Titel des Assistenten</title>
       <meta http-equiv="Content-Type" content="text/html; charset=iso-
8859-1">
     </head>
     <body>
       <div>
         <WIZARD_LOGO>
       </div>
         <WIZARD_CONTENT>
       </body>
   </html>
```

The wizard a selection of predefined CSS classes that you can easily customize by specifying appropriate values in your HTML template, including:

- `class="header"`: The CSS class for the header with the logo.
- `class="wizardName"`: The CSS class paragraph with the name of the wizard at the head of the page.
- `class="headerLogo"`: The CSS class for the area for the logo in the header.
- `class="wizardTable"`: The CSS class for tables with the displayed fields.
- `class="footer"`: The CSS class for the footer with the buttons.

Using device properties as variables

In some situations, a wizard has to make decisions based on the device properties. For instance, the wizard should only write certain values to the configuration if the device has a particular type of WAN interface. The wizard has access to certain variables of the device properties. These variables begin with the key word `device.` (including the dot), followed by the name of the relevant property. The wizard can use the following variables for read-access to the device properties:

`device.flags.dhcp_addr`: This variable indicates whether a DHCP server has assigned an IP address to the device (in which case the variable is set to '128 ') or not ('0').

`device.hasADSL`: This variable indicates whether the device has an ADSL interface ('1') or not ('0').

`device.hasISDN`: This variable indicates whether the device has an ISDN interface ('1') or not ('0').

`device.hasUMTS`: This variable indicates whether the device has an UMTS interface ('1') or not ('0').

`device.hasDSL`: This variable indicates whether the device has an DSL interface ('1') or not ('0').

`device.FirmwareVersion`: This variable indicates the current firmware version of the device.

`device.HardwareRelease`: This variable indicates the hardware release of the device.

`device.LoaderVersion`: This variable indicates the loader version of the device.

`device.MacAddress`: This variable indicates the MAC address of the device in hexadecimal notation without any separators.

`device.SerialNumber`: This variable indicates the serial number of the device.

`device.Location`: This variable indicates the location of the device as specified under `/setup/snmp`.

`device.DeviceString`: This variable indicates the type of the device.

`device.Name`: This variable indicates the name of the device as specified under `/setup`.

6.1.12 Uploading files for the wizard

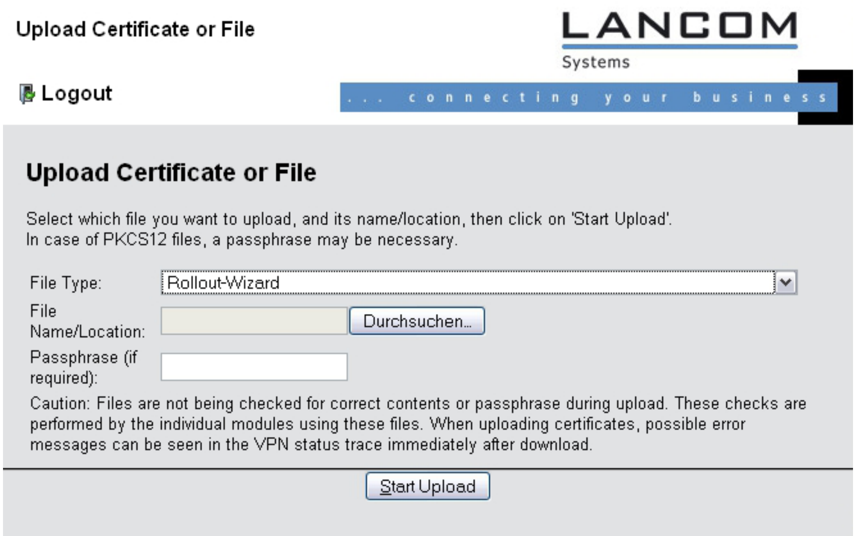
To make the wizard available, upload the following files to the device:

`Rollout-Assistent`: The instructions for compiling the wizard (required). This ISO-8859-1 encoded text file is required for operating the wizard. There is no limit on its size.

`Template-fuer-Rollout-Assistent(*.html,*.htm)`: An HTML template for the wizard (optional). This template controls the way that the sections appear in the HTML pages when the user's browser displays the wizard. The template allows you to use your own CSS information to define the layout. If you do not load a custom HTML template into the device, the wizard uses a predefined template. The template must not exceed a size of 64KB.

`Logo-fuer-Rollout-Assistent(*.gif,*.png.*.jpeg)`: Your company logo (optional). The wizard places this image file at the location of the `<WIZARD_LOGO>` marker in the template. If you do not load a logo into the device, the wizard uses a predefined logo.

Go to 'WEBconfig/File management/Upload certificate or file' to upload these files.



Upload Certificate or File

Select which file you want to upload, and its name/location, then click on 'Start Upload'.
In case of PKCS12 files, a passphrase may be necessary.

File Type:	Rollout-Wizard
File Name/Location:	
Passphrase (if required):	

Caution: Files are not being checked for correct contents or passphrase during upload. These checks are performed by the individual modules using these files. When uploading certificates, possible error messages can be seen in the VPN status trace immediately after download.

6.1.13 Deleting wizard files from the device

To delete wizard files from the device, use the `remove` command. Certain parameters allow you to define which files are to be deleted:

```
rollout <action> [file]
```

Available actions:

- `-r`
- `-remove`

Available files:

- `all`: Deletes the wizard, the template and the logo
- `wizard`: Deletes the wizard
- `template`: Deletes the template
- `logo`: Deletes the logo

6.1.14 The Rollout Wizard in the LCOS menu

The following parameters control the behavior of the Rollout Wizard.

2.21.20.1 Operating

Switches the Rollout Wizard on or off. After being switched on the Wizard appears as an option on the WEBconfig start page.

Telnet path: /Setup/HTTP/Rollout-Wizard

Possible values:

- On
- Off

Default: Off

2.21.20.2 Title

The name for the Rollout Wizard as displayed on the start page of WEBconfig.

Telnet path: /Setup/HTTP/Rollout-Wizard

Possible values:

- Max. 50 characters

Default: Rollout

2.21.20.8 Use extra checks

This option enables consistency tests that check some internal aspects of the wizard.

Executing these additional tests is very time consuming. Activate this option only during development of the wizard and deactivate this option for normal operation.

Telnet path: /Setup/HTTP/Rollout-Wizard

Possible values:

- On
- Off

Default: Off

6.1.15 Starting the Rollout Wizard

To make the wizard available, upload the following files to the device:

Go to 'WEBconfig/File management/Upload certificate or file' to upload these files.

6.1.16 Example of a Rollout Wizard:

This section presents an example of a Rollout Wizard. The wizard is used for setting up an Internet connection.

In the first section, the wizard defines the text that the device provides for display on the various HTML pages.

```
stringtable "German"
 string title_MyCompany, "MyCompany Rollout"
 string txt_Welcome, "Welcome to the MyCompany Rollout Wizard"
 string dev_serial_number, "Serial number"
 string dev_type, "Device type"
 ;---Page: What type of connection string inet_Selection, "Internet
connection type" string inet_PPPoE, "PPPoE" string inet_IPoE, "IPoE" ;-
--Page: IPoE
 string inet_ipoe, "Please enter the details for the connection."
 string con_ipaddress,      "IP address"
 string con_subnet,         "Net mask"
 string con_gateway,        "Gateway"
 string con_dns,            "DNS"
 ;---Page: PPPoE
 string inet_pppoe, "Please enter your username and password."
 con_username string,       "username"
 string con_password,       "password"
 --- Page: End
 string end,               "The configuration is now complete."
```

The wizard starts the first line of the next section with the name 'MyCompany Rollout'. The device displays the text string `str.title_MyCompany` as the title of the HTML page.

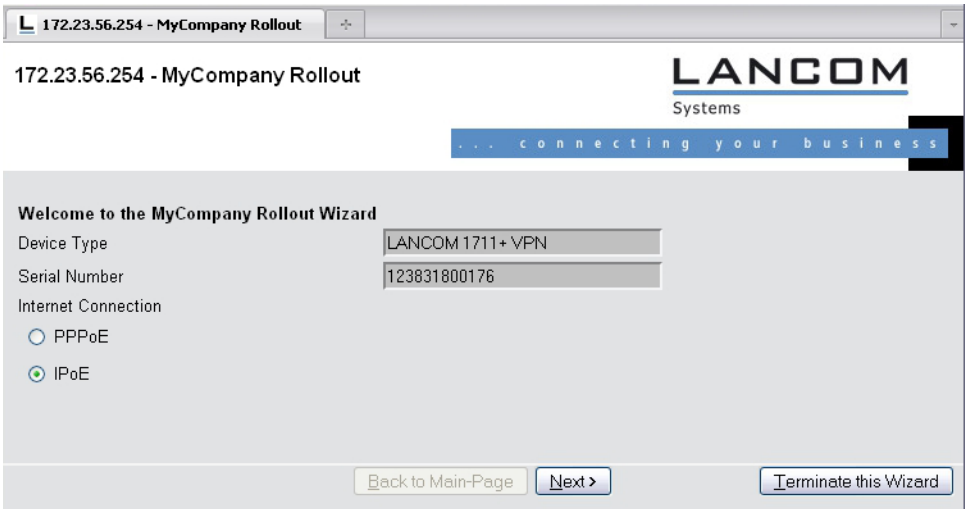
The wizard then defines the sections, which correspond to the required HTML pages.

The 'Start' section first shows a static greeting text. Below that, the Wizard has two read-only fields that display the device type and serial number. The wizard reads out these two values from the device using the field `on_show` when it opens the page. The wizard offers the user a selection of options for the Internet connection, either 'PPPoE' or 'IPoE'. Since no values are defined for the option fields, the wizard sets the variable `select_inet` according to the user's selection, e.g. PPPoE to '0' and IPoE to '1'.

```
wizard "MyCompany Rollout", str.title_MyCompany
section ;---Start---
 static_text    str.txt_Welcome
 readonly_text device_string
  description   str.dev_type
 readonly_text device_serial_number
  description   str.dev_serial_number

 selection_buttons select_inet
  description   str.inet_Selection
  button_text   str.inet_PPPoE, str.inet_IPoE
 on_show
  set wizard.device_string, device.DeviceString
  set wizard.device_serial_number, device.SerialNumber

 on_next
```


172.23.56.254 - MyCompany Rollout

Welcome to the MyCompany Rollout Wizard

Device Type: LANCOM 1711+ VPN

Serial Number: 123831800176

Internet Connection

○ PPPoE

● IPoE

172.23.56.254 - MyCompany Rollout
LANCOM
Systems
... connecting your business
Back to Main-Page
Next >
Terminate this Wizard

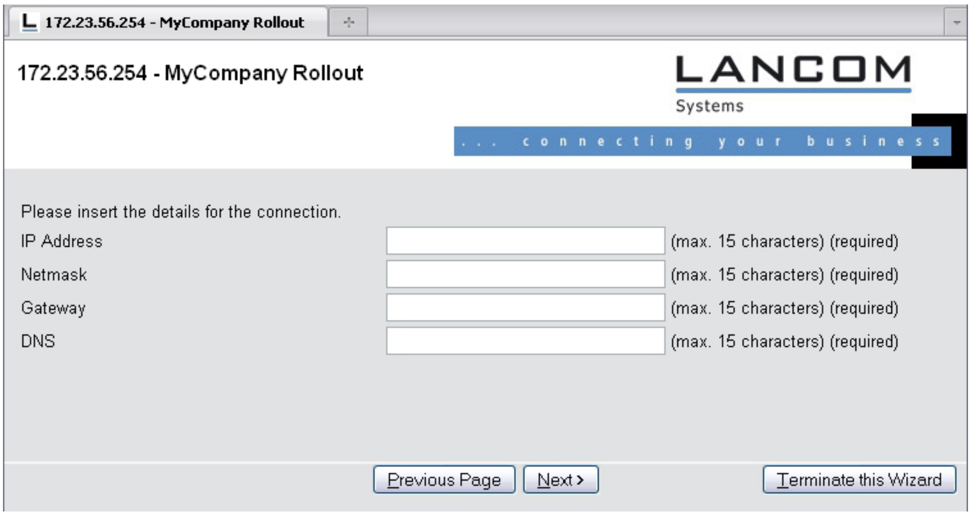
The wizard only displays the IPoE section if the variable select_inet is set to the value '1'.

On this page, the wizard asks the user to provide values for the IP address, netmask, gateway and DNS server. All fields are required to run the wizard.

```
section ;---IPoE---
 only_if wizard.select_inet, "1", equal

 static_text   str.inet_ipoe

 entryfield_ipaddress inet_ipaddress
  description  str.con_ipaddress
  never_empty  1
 entryfield_ipaddress inet_subnet
  description  str.con_subnet
  never_empty  1
 entryfield_ipaddress inet_gateway
  description  str.con_gateway
  never_empty  1
 entryfield_ipaddress inet_dns
  description  str.con_dns
  never_empty  1
```



172.23.56.254 - MyCompany Rollout

Please insert the details for the connection.

IP Address (max. 15 characters) (required)

Netmask (max. 15 characters) (required)

Gateway (max. 15 characters) (required)

DNS (max. 15 characters) (required)

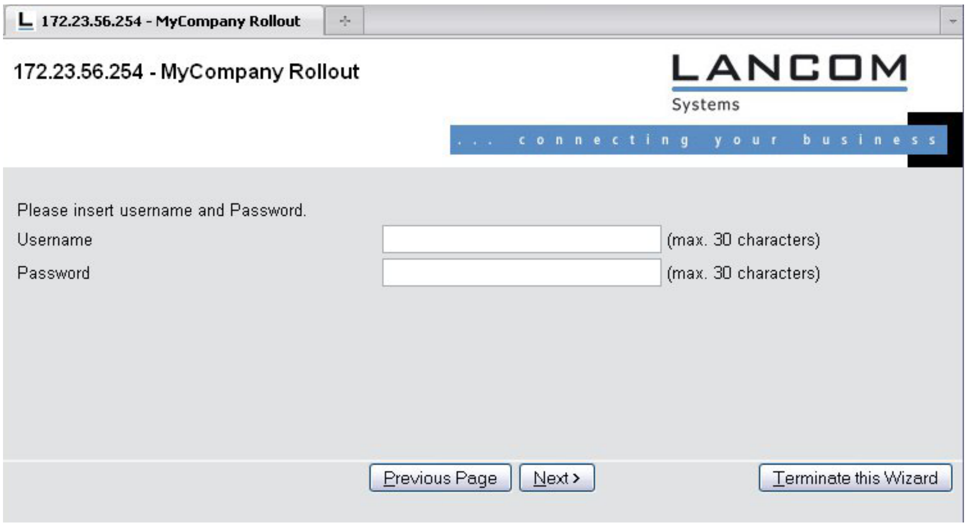
172.23.56.254 - MyCompany Rollout
LANCOM
Systems
... connecting your business
Previous Page
Next >
Terminate this Wizard

The wizard only displays the PPPoE section if the variable select_inet is set to the value '0'.

On this page of the wizard prompts the user for the user name and password, each with a maximum length of 30 characters.

```
section ;---PPPoE---
 only_if wizard.select_inet, "0", equal
 static_text   str.inet_pppoe

 entryfield_text inet_username
  description  str.con_username
  max_len   30
 entryfield_text inet_password
  description  str.con_password
  max_len   30
```



172.23.56.254 - MyCompany Rollout

Please insert username and Password.

Username (max. 30 characters)

Password (max. 30 characters)

172.23.56.254 - MyCompany Rollout
LANCOM
Systems
... connecting your business
Previous Page
Next >
Terminate this Wizard

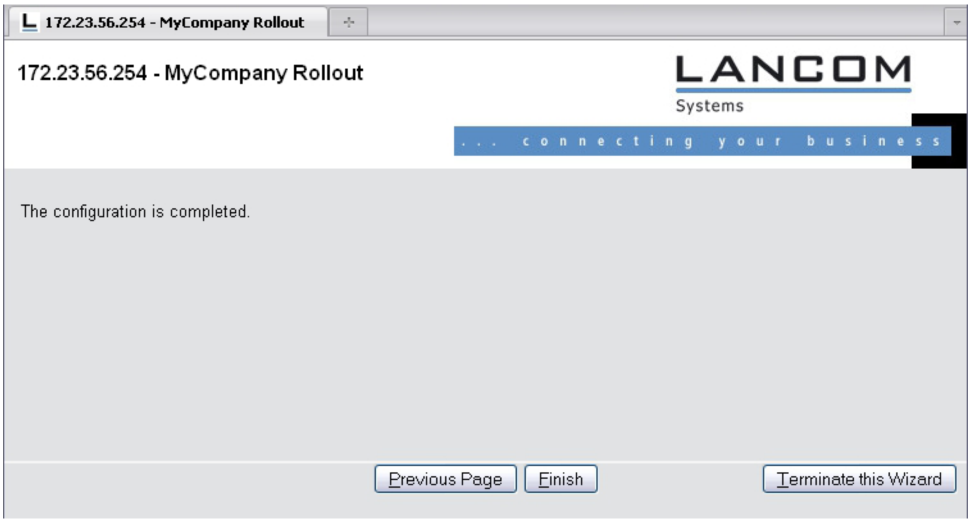
The last page of the wizard initially displays a summary in static text. Follow-up actions are carried out when the wizard is finished:

- If the user has selected IPoE, the wizard creates a corresponding remote site and an entry in the list of IP parameters.
- If the user has selected PPPoE, the wizard creates a corresponding remote site and an entry in the PPP list.
- Whichever option is selected, the Wizard creates a default route 'INTERNET in the router.

```
section ;---ende---
 static_text   str.ende

on_init  ;---Befehle, die bei der Initialisierung des Wizards
durchgeführt werden.---
on_apply ;---Befehle, die bei der Fertigstellung des Wizards
durchgeführt werden.---
```

```
 ;---Wenn IPoE ausgewählt wurde, werden die entsprechenden Daten nun
eingetragen.
 ;---Remote site
 set config.1.2.2.19, "INTERNET", "9999", "", "", "IPOE", "0",
"000000000000"
 only_if wizard.select_inet, "1", equal
 ;---IP-Parameter
 set config.1.2.2.20, "INTERNET", wizard.inet_ipaddress,
wizard.inet_subnet, "0.0.0.0", wizard.inet_gateway, wizard.inet_dns,
"0.0.0.0", "0.0.0.0", "0.0.0.0"
 only_if wizard.select_inet, "1", equal
 ;---If PPPoE was selected, the corresponding data is entered.
 ;---Remote site
 set config.1.2.2.19, "INTERNET", "9999", "", "", "PPPOE", "0",
"000000000000"
 only_if wizard.select_inet, "0", equal
 ;---PPP list
 set config.1.2.2.5, "INTERNET", "none", "60", wizard.inet_password,
"5", "5", "10", "5", "2", wizard.inet_username, "1"
  only_if wizard.select_inet, "0", equal
 ;---Set the default route.
 set config.1.2.8.2, "255.255.255.255", "0.0.0.0", "0", "INTERNET", "0",
"on", "Yes", ""
```


172.23.56.254 - MyCompany Rollout
172.23.56.254 - MyCompany Rollout
LANCOM
Systems
... connecting your business

The configuration is completed.

Previous Page
Finish
Terminate this Wizard

7 Certificates

7.1 OCSP client for certificate validation

7.1.1 Introduction

The Online Certificate Status Protocol (OCSP) provides a way to verify the status of certificates, for example when establishing VPN connections. The devices use this protocol to investigate whether the issuer has revoked the certificate before its expiry, so marking it as invalid.

Certificate issuers update the status of all issued certificates on a special server, the OCSP responder. The OCSP client (e.g. a VPN router that wants to establish a connection) uses the HTTP protocol to send an OCSP request to the responder to verify the certificate. The responder answers with a signed response, which the OCSP client uses to verify its validity. The message from the OCSP responder describes one of the following conditions:

- Good: The verified certificate has not been revoked.
- Revoked: The verified certificate has been revoked and may not be used to establish VPN connections.
- Unknown: The OCSP responder cannot determine the status of the certificate. This may be because the OCSP responder does not recognize the certificate issuer because the certificate has been faked and therefore has not been entered into the database of the OCSP responder.

You can use the OCSP to complement or substitute certificate verification by certificate revocation lists (CRL). OCSP offers the following advantages when compared to CRLs:

- The issuers generate the CRLs at specific time intervals and, in the ideal case, distribute the CRLs to the devices which use the certificates for establishing VPN connections. The reliability of this check thus depends on the speed with which CRLs in the devices are updated. However, certificate verification through an OCSP responder is always "online", i.e. it is automatically updated. The operator of the OCSP responder can automatically synchronize their data with that of the CA or CAs, thus ensuring that they are up to date at all times.
- Using certificate revocation lists for certificate verification takes up a considerable amount of device memory, especially if the CRLs are large. Querying certificate status from an OCSP responder, on the other hand, is independent of the number of CAs and certificates being used, and is therefore more scalable.
- As the CRL method does not allow for unknown certificates, this method cannot detect fake certificates. The OCSP responder, depending on its configuration, responds to a request about an unknown certificate with a negative evaluation.

7.1.2 Additions to the menu system

2.39.6.2 Responder profile table

This table contains information on the Certificate Authorities (CAs), whose certificates are evaluated by the OCSP client by sending a request to an OCSP responder.

Telnet path: /Setup/Certificates/OCSP-Client

2.39.6.2.1 Profile name

Enter here the name of an OCSP-responder profile to be referenced by the OCSP client in the CA profile table.

Telnet path: /Setup/Certificates/OCSP-Client/Ca-Profile-Table

Possible values:

- Maximum 32 alphanumerical characters

Default: Blank

2.39.6.2.2 URL

Enter the URL for the OCSP client to access the OCSP responder.

Telnet path: /Setup/Certificates/OCSP-Client/Ca-Profile-Table

Possible values:

- Valid URL with a maximum of 251 alphanumeric characters

Default: Blank

2.39.6.1 CA profile table

This table contains information on the Certificate Authorities (CAs), whose certificates are evaluated by the OCSP client by sending a request to an OCSP responder.

Telnet path: /Setup/Certificates/OCSP-Client

2.39.6.1.1 Profile name

Enter here the name of a CA profile to be used by the OCSP client for a particular CA.

Telnet path: /Setup/Certificates/OCSP-Client/Ca-Profile-Table

Possible values:

- Maximum 32 alphanumerical characters

Default: Blank

2.39.6.1.2 CA distinguished name

Enter the distinguished name of the CA, whose certificates are evaluated by the OCSP client with this profile name.

Telnet path: /Setup/Certificates/OCSP-Client/Ca-Profile-Table

Possible values:

- Maximum 251 alphanumerical characters

Default: Blank

2.39.6.1.3 Prefer AIA

Certificates used for establishing VPN connections optionally include the URL of the relevant OCSP responder in the field Authority Info Access (AIA). This item defines whether the OCSP client prefers to use the URL from this entry in the CA profile table or the URL from the AIA field, if available.

Telnet path: /Setup/Certificates/OCSP-Client/Ca-Profile-Table

Possible values:

- No: The OCSP client always uses the URL from this CA-profile table entry and ignores the URL in the AIA field.
- Yes: The OCSP client uses the URL from the AIA field (if specified) and ignores the URL from this CA profile table entry.

Default: No

2.39.6.1.4 Responder profile name

This item selects the responder profile used by the OCSP client to evaluate certificates from this CA.

Telnet path: /Setup/Certificates/OCSP-Client/Ca-Profile-Table

Possible values:

- Select from the list of profile names in the table 2.39.6.2 Responder profile table, maximum 32 alphanumeric characters.

Default: Blank

ⓘ If the field for the responder profile name is left empty, the machine evaluates the certificates from the CA defined here not with OCSP, but with the help of a CRL.

2.39.6.1.5 Source interface

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

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

Telnet path: /Setup/Certificates/OCSP-Client/Ca-Profile-Table

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet

- "DMZ" for the address of the first DMZ
- LB0 to LBF for the 16 loopback addresses
- Any valid IP address

Default: 00.0.0

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

2.39.6.1.6 Certificate evaluation

This item defines how the device behaves if certificate evaluation fails. During connection establishment, the OCSP client first queries the OCSP responder about the validity of the certificate.If the certificate is about to expire, the OCSP client automatically repeats the query about the validity before the certificate expires.

Telnet path: /Setup/Certificates/OCSP-Client/Ca-Profile-Table

Possible values:

- Strict: The device will block connection establishment if the OCSP responder answers requests for the certificate used during connection establishment in one of the following ways:
  - The OSCP responder does not answer
  - The OSCP responder responds that the certificate is unknown
  - The OSCP responder recognizes the certificate and marks it as revoked
- Loose: The device will block connection establishment if the OCSP responder answers requests for the certificate used during connection establishment in one of the following ways:
  - The OSCP responder does not answer
  - The OSCP responder responds that the certificate is unknown

Default: Strict

ⓘ If necessary, you can log and review the results of certificate evaluation by the OCSP responder with SYSLOG, SNMP traps and relevant traces.

2.39.6.1.7 Syslog events

The OCSP client can optionally generate SYSLOG messages with information on the results of certificate checks by the OCSP responder.

Telnet path: /Setup/Certificates/OCSP-Client/Ca-Profile-Table

Possible values:

- Yes: The OCSP client generates SYSLOG messages
- No: The OCSP client does not generate SYSLOG messages

Default: Yes