LANCOM Systems

Information regarding
LCOS Software Release 8.00 RU4

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

Internet: http://www.lancom.eu

07.04.2011, CBuersch

Table of Contents

LANCOM Systems

1. Preface

LCOS („LANCOM Operating System“) is the operating system for all LANCOM routers, wireless LAN access points and WLAN controllers. In the context of the hardware given by the products the at a time latest LCOS version is available for all LANCOM products and is available free of charge for dowload from LANCOM Systems.

This document describes the innovations within LCOS software release 8.00 RU4, as well as the changes since release 7.82

Warning hints – Backing up the current configuration

Before upgrading your device to a new LCOS version it is essential to backup the configuration of your router. Due to extensive features it is not possible to downgrade to a previous firmware without using the backup configuration.
Please see the reference manual for instructions on how to backup the router configuration.

If you want to upgrade devices which are only accessible via router connections or WLAN bridges, please keep in mind to upgrade the remote device first and the local device afterwards.

Note – Upgrading central site components

We strongly recommend updating productive systems only after internal tests in client environment. Despite intense internal and external quality assurance procedures possibly not all risks can be eliminated by LANCOM Systems.

Note – Using managed access points

Prior to managing a LANCOM accesspoint using a WLAN controller, you have to upgrade your access point with the latest converter. The corresponding converter file can be found in your device’s download directory on the LANCOM homepage. The converter upload is similar to a firmware upgrade.

Note – Using certificates

Prior to loading certificates into the LANCOM you must install the current converter. The appropriate converter file can be found in your device’s download directory on the LANCOM homepage. Flashing the converter file works similar to a firmware upgrade.

Note – Using converter firmwares

You will need enough free memory to use a firmware 6.0 and newer in your LANCOM 15x1, 1611+, 821+ and DSL/I-10+.
Due to the implementation of several new features within the current build of the firmware, it is no longer possible to store two main firmware versions side by side. To gain more free space for the current version, it is now necessary to upload a converter firmware into your device. The converter-firmware has a much smaller size, so that it is now possible to store the main release of the firmware besides the converter-firmware.
This setup is only necessary once for a single device and is done with the so-called converter-firmware (see readme.pdf of the affected devices).
After having flashed the converter-firmware the firmsave function of the LANCOM device is available only on a limited scale. The update to a newer firmware is furthermore possible. However, in case of an update failure the LANCOM will only work with a minimal-firmware which allows just local access to the device. Any extended functionality, in particular remote administration, is not possible when running the minimal-firmware.

Note – Dynamic VPN registration

By reason of patent you have to register the functionality „Dynamic VPN“ with IP address transmission over ISDN. This operating mode is usually required when you configure a VPN tunnel with dynamic IP addresses on both sides without dynamic DNS services.
Any other Dynamic VPN operation mode (e.g. transmitting the IP address via ICMP, provoking a callback etc.) does not require registration.
The registration process is fully anonymous - no personal or company data will be transmitted.

The registration of the Dynamic VPN option requires administrator rights on the LANCOM device.

Registration with LANconfig
When scanning the device (e.g. right after program start) LANconfig automatically recognizes devices which have to be activated. After confirming the arising hint LANconfig automatically transmits solely the device's serial number to the LANCOM Systems registration server. The registration code is automatically transmitted back, thus the option will be activated. The state of this procedure is visible in LANconfig.

Registration with WEBconfig
For the registration with WEBconfig the serial number of the device is required. You can find this information on the bottom of your device.

Using WEBconfig you will find a link on the first page which leads you to the LANCOM Systems registration server. Here you must enter your device's serial number and -optional- your e-mail address. After transmitting the data you will receive a registration code for the option.
To load this code into your device, please proceed as follows:
Log in to the device with administrator rights. Select “Enable Software Option”, which is placed on the entry page. On the following page enter the registration code and confirm by selecting “Apply”.

Note – Using VoIP options

VoIP options for LANCOM 1821 Wireless ADSL are discontinued with LCOS 7.20. The final version containing the VoIP Call Manager is LCOS 6.32.
As from LCOS 7.5x support for VoIP options for the devices LANCOM 1511 Wireless DSL and 1521 Wireless ADSL is discontinued. The final version containing the VoIP Call Manager is LCOS 7.30.
For the „VoIP ready“ routers LANCOM 1711 VPN, 1721 VPN and 1811 Wireless DSL support for the subsequently installed VoIP option will be discontinued with LCOS version 7.56. If you want to continue using your VoIP option, please do only use LCOS versions up to and including 7.54.
For T-Systems Business LAN R800+ VoIP functionality is discontinued in LCOS 7.60
LCOS 7.70 is the final version supporting VoIP options for the remaining „VoIP ready“ devices.

2. Known Issues

Latest support notes and known issues regarding the current LCOS version can be found in the download area of our website http://www.lancom-systems.eu/Common-Support-Hints.64.0.html

3. New Features, Changes and History

LCOS changes 8.00.0255 RU3 ► 8.00.0269 RU4

Bugfixes / Changes:

WLAN:

- Error correction for WLAN module noise value detection
- Fixed beacon transmit failures for devices LANCOM 1780EW-3G and LANCOM L-32x
- Fix to avoid double authentication in Public Spot
- Improved recognition of corrupted WLAN and EAPOL info elements

Network Connectivity:

- Fixed problems with action table variable %t
- Fixed possible loop when parsing TCP options
- Updated index parser for central firmware management via WLC
- Modified syslog behaviour for message aggregation
- Fixed sending default routes via RIP
- Modified DHCP automode behaviour for client requests
- Modified DHCP cluster mode
- Improvements in ARP handling
- Fixed syslog messages for traps

LCOS changes 8.00.0221 RU2 ► 8.00.0255 RU3

Bugfixes / Changes:

WLAN:

- Plainly reduced amount of beacon transmit failures, particularly when operating in 40 MHz mode
- Radio field optimization of the WLC can be used again
- If a WLAN client refuses packet aggregation, no more aggregates are sent to the client

Network Connectivity:

- Improvements for internal certificate search
- A „Destination unreachable“ is no longer seen as an ICMP polling answer
- The RADIUS server user table can be filled without errors by script again
- If a draft method negotiation starts after NAT-T is negotiated in RFC mode, the LANCOM device will accept this
- An already configured SIP line can be edited via WEBconfig
- The message „Content Filter is starting“ is only displayed on initial start
- The backup chain is passed through on main connection loss even if a backup connection was cancelled due to an error
- SNMP traps are sent again for dial-up connections
- When using N:N NAT active FTP connections can be used error-free again
- ISDN ports of the LANCOM 1724 are configurable via WEBconfig2 to DSS1 NT reverse

LCOS changes 8.00.0173 RU1 (only for WLC) ► 8.00.0221 RU2

Bugfixes / Changes

WLAN:

- Polling packets from WLAN clients in powersave mode are no longer filtered
- A WLAN accesspoint in client mode can use the „ANY“ SSID again
- A WLAN Nokia mobile phone can send data packets via LANCOM accesspoint with activated APSD
- VoIP usage improvements for WLAN point-to-point connections
- If encryption changes from WPA to WEP the WLAN client can connect without restarting the accesspoint
- The WAN IP address is no longer set as NAS address in active accounting sessions on public spot devices
- After the CA has renewed its certificates in the WLC, the access point’s SCEP client can do its update successfully
- Fixed an error when resetting the configuration of a WLC 4006 or WLC 4025
- Authentication via EAP/TLS can be used with Intel 2200bg clients
- A LANCOM access point can be used as LAN sided EAP supplicant against a LANCOM switch

Network Connectivity:

- A PKCS#12 container for SSL can be decompressed and the embedded certificate can be used
- LCP-, VPN- and ICMP polling is only executed if no data is received on the connection
- Fixed a bug when writing back a configuration file via outband interface
- SIP packets are sent completely if the registrar requests proxy authentication
- SSH access can be used with additionally configured users
- Fixed a bug in the WEBconfig wizard „Connect two local networks (VPN)“
- The private key of a PKCS#12 container is decompressed correctly
- Fixed an LCOS watchdog in task “SF” which could occur when updating to LCOS 8.0
- If the SCEP client uses auto approve, the challenge password is no longer sent within the request if a valid device certificate is available
- Re-registration of DNS leads to a DNS table update. So the client remains resolvable via DNS even after TTL expiration
- All flags of the DHCP request are sent back in the reply packet
- The requested DHCP client lease time is no longer reported extended by one minute
- Connection establishments are retried if previously failed due to no modem sync
- The connection time is reported in the correct line within the connection table
- If too many HTTP tunnels were created via WEBconfig, the website for deleting those can be accessed
- The “show cf” command doesn’t cause an LCOS-Watchdog on an device with disabled content filter
- Modified hardware failure handling, so a damaged UMTS module of a LANCOM 1751 does not prevent ADSL operation
- Outdated menue entries can no longer be read via SNMP
- The station access table is not used for admin ISDN dial-in, as there are random local IP addresses used for dial-in
- Corrected WEBconfig DynDNS wizard for DynAccess ‘.de’ accounts
- On incoming calls the B channel is displayed correctly in the call info table
- If the IP addres of a remote media endpoint changes during SIP connection establishment, data may be sent through a different interface
- A script which was read from the device with default values can be uploaded to the device without error

LCOS changes 8.00.0162 Release ► 8.00.0173 RU1 (only for WLC)

Bugfixes / Changes:

- Fixed an LCOS watchdog when finishing the Public-Spot wizard
- Fixed an LCOS watchdog when using background scan
- Fixed an LCOS watchdog when activating Public Spot user authentication for the interfaces
- Fixed an LCOS watchdog when using Public Spot on the LAN-1 interface
- Fixed an LCOS watchdog in the automatic ISDN protocol recognition
- Corrected allocation to the ISDN lines for outgoing ISDN calls
- VDSL access can be selected in the WEBconfig internet wizard
- ARF networks can be propagated locally via RIP
- No filtering of data packets from RAS clients which got an IP address from the configured WAN pool
- The content filter of the HTTP proxy reports adequate status codes to the http client for block- and errorpages
- Improved configuration of contentfilter whitelists in WEBconfig
- On portscans, port 0 is no longer reported as open
- On ADSL- and ISDN line errors the error display is deleted not until the connection could be re-established. Unnecessary condition changes are avoided (e.g. in LANmonitor)

LCOS changes 8.00.0149 RC2 ► 8.00.0162 Release

Bugfixes / Changes:

WLAN:

- WLAN channel selection is no longer set to „automatic“ in WEBconfig
- WLAN data LED showing data traffic on L-32x
- Authenticating to a Public Spot can be used with external authentication sites again
- WEBconfig’s Public Spot wizard opens the voucher popup window without HTTP error message
- In a VLAN environment a new access point regains its controller after having received a new LCOS version from it

Network Connectivity:

- Corrected spreading of outgoing ISDN calls to the ISDN lines
- Partitioned data storage mediums connected to the USB port do not hinder LCOS boot
- Aborted outgoing calls before establishment do no longer prevent further calls
- RIP learned routes are processed faster and need less CPU resources
- The „show script“ command shows the last handled script even repeatedly
- A configuration can be uploaded via TFTP, even with active VLANs
- Netmasks of host addresses can be configured with the IP network table again
- With activated IPsec over HTTPS* port 443 is always open, even if configuration via HTTPS is disabled
- Corrected routing tag assignment for internal TCP services
- TCP connections are no longer cut when modifying firewall rules

* based on NCP VPN Path Finder technology

LANCOM Systems

LCOS changes 8.00.0124 RC1 ► 8.00.0149 RC2

Bugfixes / Changes:

WLAN:

- New access points can be assigned to a profile in the WLC using a wizard
- Support for DFS (ETSI 301 893 v1.5) for radar pulse detection

Network Connectivity:

- Manual rule creation was customized for the case the remote station gets an IP address from the network which is configured as target network in the firewall
- A monitoring job checks the UMTS module of the LANCOM 1751 UMTS and resets it if it does not report all necessary COM ports
- Correct masquerading of VPN packets, if the LANCOM was configured as config mode client
- A configuration can be uploaded to a password-free LANCOM without errors even if a password is still set in LANconfig
- If the VPN gateway is part of the remote network, the VPN tunnel can be established without configuring a particular host route for the VPN gateway
- Corrected detection of the index column of an SNMP table
- LCOS can be uploaded to devices which are not registered for VPN
- Telnet/SSH client can be used with TACACS+
- SNMPwalk does no longer skip columns
- Necessary firewall rules are created when updating the content filter
- The USB interface supports partitioned data storage mediums (FAT) for automatic loading of LCOS files, configuration data, scripts and for the HTTP fileserver
- Accelerated configuration upload via USB
- Reworked performance statistics output for the content filter

LANCOM Systems

LCOS changes 7.82.0020 Release ► 8.00.0124 RC1

New Features:

WLAN:

- Loadbalancing functionality for WLAN controllers, too
- Accesspoint channel load can be monitored via WLC
- New consistent MIB for LANCOM L-32x series and Wireless LAN controllers, which can be obtained via LANCOM
- RADIUS accounting per WLAN-SSID and configuration of the SSID assignment per WLAN controller

Network Connectivity:

- With IPsec over HTTPS* VPN packets are encapsulated in SSL
- Implementation of the Content Filter (optional for appropriate router models)
- The LANCOM device sends an early message before a license expires
- Alternative boot configurations can be stored in the LANCOM
- Implementation of telnet- and SSH clients with new function right in the admin table
- Support for USB memory devices for USB setup, Public Spot- and Content Filter option (lodging of HTML documents)
- Automatic LCOS- and configuration upload from USB memory devices (USB setup)
- Files on a LANCOM-mounted USB stick can be used by the internal http server
- The bootlog is saved compressed to memory
- An alternative DHCP server can be specified for DHCP forwarding

Bugfixes / Changes:

WLAN:

- WLC-communicated fixed IP addresses and VLAN settings are completely adopted, even if the management VLAN is not 1

Network Connectivity:

- IP addresses are shown correctly in firewall logs
- An appropriate timeserver can be added in WEBconfig
- No ARP requests are sent for non-configured gateways (IP: 0.0.0.0) in the IP parameter list
- A cancelled telnet session does no longer deny access
- Checksums are displayed correctly in the VPN packet trace
- Incoming PPTP connections can be established using DNS names
- A RADIUS authentication can happen through a PPTP tunnel
- Incoming PPTP connections are logged to PPTP statistics only after successful connection establishment
- The PublicSpot Wizard does no longer lead to an LCOS watchdog.
- Simplified Dial-In using certificates can be used with tagged default routes, too
- The Public Spot Wizard can be set as function right in the administrator table

* based on NCP VPN Path Finder technology

4. Comments

If you want to upgrade the firmware of your device to a new version, please install the latest LANtools first. **Before running the firmware-upload you should save the router configuration to a file**. After that you can use LANconfig to load the latest LCOS-version into the device.

In principle, we suggest upgrading the firmware of your device only if you are in need of the latest features.

Please note that different firmware files might be available for your device. Further information can be found in the file README.PDF in the download area of our homepage.

