

LANCOM Release Notes

LCOS

8.84 SU11

Copyright (c) 2002-2019 LANCOM Systems GmbH, Wuerselen (Germany)

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

Internet: <http://www.lancom-systems.com>

November 5th, 2019, CBuersch

Table of Contents

1. Preface	2
2. Device-specific compatibility to LCOS 8.84	2
3. History LCOS 8.84	4
LCOS improvements 8.84.0309 SU11	4
LCOS improvements 8.84.0308 SU10	5
LCOS improvements 8.84.0289 SU9	6
LCOS improvements 8.84.0267 RU8	6
LCOS improvements 8.84.0262 RU7	6
LCOS improvements 8.84.0244 RU6	7
LCOS improvements 8.84.0231 RU5	7
LCOS improvements 8.84.0193 RU3	8
LCOS improvements 8.84.0177 RU2	8
LCOS improvements 8.84.0142 RU1	10
LCOS improvements 8.84.0132 Rel	10
LCOS improvements 8.84.0103 RC1	11
LCOS improvements 8.82.0123 RU2	12
LCOS improvements 8.82.0100 RU1	13
LCOS improvements 8.82.0089 Rel	13
LCOS improvements 8.82.0067 RC2	14
LCOS improvements 8.82.0051 RC1	14
LCOS improvements 8.80.0159 RU1	15
LCOS improvements 8.80.0157 RU1	16

4. General advice	17
Disclaimer	17
Backing up the current configuration	17
Using converter firmwares to free up memory	17

1. Preface

LCOS („LANCOM Operating System“) is the established LANCOM operating system for 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 download from LANCOM Systems.

This document describes the innovations within LCOS software release 8.84 SU11, as well as the improvements since the previous version.

Before upgrading the firmware, please pay close attention to chapter 4 “General advice” of this document.

Latest support notes and known issues regarding the current LCOS version can be found in the support area of our website <https://www.lancom-systems.com/service-support/instant-help/common-support-tips/>

2. Device-specific compatibility to LCOS 8.84

LANCOM products regularly receive major firmware releases throughout their lifetime which provide new features and bugfixes.

LCOS release updates including bugfixes and general improvements are available on a regular basis for devices which do not support the latest LCOS version. You can find an overview of the latest supported LCOS version for your device under <https://www.lancom-systems.com/products/firmware/lifecycle-management/product-tables/>

As from LCOS 8.50 support for the following devices is discontinued

- > LANCOM 1811 Wireless
- > LANCOM 1721 VPN

For the following devices the additional, LANconfig-like WEBconfig view is removed as from LCOS 8.60

- > LANCOM L-310
- > LANCOM L-305
- > LANCOM L-54 dual Wireless
- > T-Systems Business LAN R800+

Please use instead either LANconfig or use the configuration view “LCOS Menu Tree” in WEBconfig

As from LCOS 8.80 support for the following devices is discontinued

- > LANCOM L-54 Wireless (Hardware release <E)
- > LANCOM L-54 dual Wireless (Hardware release <G)
- > LANCOM OAP-54-1 Wireless

As from LCOS 8.82 support for the following devices is discontinued

- > LANCOM XAP Wireless
- > LANCOM L-305 / L-310 Wireless
- > LANCOM L-54 dual Wireless

As from LCOS 8.84 support for the following devices is discontinued

- > Telekom R800+
- > LANCOM 821+
- > LANCOM 1611+
- > LANCOM 1711
- > LANCOM 1821n

3. History LCOS 8.84

LCOS improvements 8.84.0309 SU11

Bugfixes / improvements

- > A potentially security-relevant issue has been fixed on LANCOM routers in conjunction with IPv6. This issue can occur when IPv6 networks are connected via IPsec (IKEv1 or IKEv2), and an IPv6 Internet connection is used simultaneously. In this case, an update to the current LCOS version is strictly recommended. This issue has been fixed in the following LCOS versions:
 - > LCOS 10.32 SU3
 - > LCOS 10.20 SU9
 - > LCOS 10.12 SU14
 - > LCOS 9.24 SU12
 - > LCOS 9.00 SU8
 - > LCOS 8.84 SU11
- > In rare cases, SSL/TLS handshake packets can become so big that they have to be split over multiple records. An SSL/TLS reassembler has now been implemented which reassembles these packets.
- > No LANCOM devices could be found using the LL2M broadcast command "ll2mdetect - b" from the CLI.

LCOS improvements 8.84.0308 SU10

Bugfixes / improvements

- > A security issue within WPA2 authentication (KRACK attack) using P2P connections with 802.11a/b/g/n Wi-Fi modules has been fixed.

CVE-2017-13077: reinstallation of the pair-wise key in the Four-way handshake

CVE-2017-13080: reinstallation of the group key in the Group Key handshake

The WLAN client mode / WLAN station mode with 802.11a/b/g/n Wi-Fi modules is not affected.

Note

- > LCOS is **NOT** affected by the following WPA2 security issues (KRACK attack)

CVE-2017-13084: reinstallation of the STK key in the PeerKey handshake

CVE-2017-13086: reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake

CVE-2017-13087: reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame

CVE-2017-13088: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame

CVE-2017-13078: reinstallation of the group key in the Four-way handshake

CVE-2017-13079: reinstallation of the integrity group key in the Four-way handshake

CVE-2017-13081: reinstallation of the integrity group key in the Group Key handshake

- > LCOS would only be affected by the following WPA2 security issues (KRACK attack) when using 802.11r (fast roaming), but this is not supported by this LCOS version.

CVE-2017-13082: accepting a retransmitted Fast BSS Transition Reassociation Request and reinstalling the pair-wise key while processing it.

LCOS improvements 8.84.0289 SU9

Bugfixes / improvements

Network connectivity

- › If the device does not offer individual SSL-/SSH keys, they will be generated once
- › Support for SHA-256 within WEBconfig's SSL device certificate
- › TLS Handshake uses 2048 Bit Diffie-Hellman

LCOS improvements 8.84.0267 RU8

New features

Network connectivity

- › The mobile network can now be selected based on signal strength.

LCOS improvements 8.84.0262 RU7

Bugfixes / improvements

Network connectivity

- › If overlapping networks are configured, reply packets are forwarded to the correct network
- › An address assigned by the DHCP server is only checked against the requesting network
- › Fixed a bug which caused a voice transmission abort when calling from an ISDN phone via All-IP line
- › The Telekom voicebox can be retrieved again
- › For ISDN users, the number type of the Called Party Number is now set according to the transmitted number
- › Fixed a problem which caused the ADSL up- and downstream not to be displayed
- › A LANCOM now responds with its IP address while a DNS lookup to its name
- › Fixed a problem which led to not being able to establish a new VPN phase 2 SA after a phase 2 soft timeout
- › The monitoring interval for SIP trunks is handled correctly
- › SIP trunks register even if SIP-ALG is enabled
- › A PPTP connection works even if the target is an IPSec backup connection
- › Naming of the ADSL interface was adjusted within the MIB

Wi-Fi

- › Stability improvements for scenarios with many WLAN clients
- › Fixed a problem where WLAN clients were registered, but no data transmission was possible
- › Prevention of duplicate MAC address entries in the station table
- › Fixed a problem with AR93xx based WLAN modules in TKIP encrypted networks

LCOS improvements 8.84.0244 RU6**Bugfixes / improvements****Network connectivity**

- › Improved VoIP router support for double challenge authentication
- › ADSL sub interfaces are shown again in the 1781A-3G's MIB
- › Fixed a problem with the VPN Load Balancer
- › Fixed a problem with the bandwidth reservation
- › It is no longer possible to create multiple DNS entries for the same name on the CLI

Wi-Fi

- › Optimized transmit power for wireless abg modules

LCOS improvements 8.84.0231 RU5**Bugfixes / improvements****Network connectivity**

- › If there is a failure during a PPP negotiation, a backup connection is always established when the remote site is configured with a hold time of 9999
- › Improved propagation of additional routes via RIP
- › Fixed a problem with an SNMP query
- › The CLI command „who“ now shows the correct time
- › Fixed a problem with offline created LANconfig configuration files, which could not be uploaded by WEBconfig
- › Fixed a problem when sending SMS
- › The RTP timestamp is set correctly when RTP events are used within the callmanager
- › If the WWAN module is disabled in the LCOS, the connection is cut, too

Wi-Fi

- > The expiration types are used correctly when E-Mail2SMS is used
- > Block-Ack handling problem solved for different WLAN clients
- > Improved WLAN transmission power in the 2.4 Ghz band

LCOS improvements 8.84.0193 RU3**New features****Network connectivity**

- > While updating the firmware, LCOSCap and RCap are automatically terminated
- > Support for 1781VA-4G

Bugfixes / improvements**Wi-Fi**

- > If RCap is used, authentication and association frames are recorded, too
- > Public Spot improvements

Network connectivity

- > The DHCP Server ignores packets with invalid or wrong checksum
- > Fixed a bug which led to a not working DNS forwarding
- > SIP-ALG improvements
- > If the volume budget is used, the month change is taken into account

LCOS improvements 8.84.0177 RU2**New features****Network connectivity**

- > Configurable RIP Output Delay
- > RIP responses as an answer to a RIP request are sent to the sourceport of the RIP request (RFC 2453)
- > It is now possible to change the SIM PIN
- > The FQDN of a HTTPS connected site is taken from the server certificate within the content filter
- > VDSL vectoring support for ‚overISDN‘ LANCOM devices

Bugfixes / improvements

Wi-Fi

- › No access point restart when searching for printers from within the android app „Page Scope Mobile“
- › No more errors when logging in to a Public Spot with the browser set to italian or spanish language
- › No more loops when finishing Spectral Scan
- › Bugfix in RADIUS protocol handling
- › Corrected PMS trace display
- › Reworked PMS Accounting Plus option
- › Reworked Public Spot login
- › New Public Spot login text for the LANCOM 1823
- › Changed XML interface for Public Spot Re-login

Network connectivity

- › The backup connection for the event „volume budget exceeded“ is established even if no keepalive is set for this connection
- › A manually set alternative SMTP port is allowed again
- › Hardware NAT is disabled for PPPoE remote stations
- › Improvements in IKE memory management
- › Reworked loadbalancer channel selection
- › CLI: Reworked status display for the VPN menu
- › Improved SIM card recognition
- › Corrected MTU handling for Ipv6
- › Padding bytes are allowed within MLPP
- › Modified Link End record handling for the FIAS interface
- › Improvements for the DH precalculation
- › LANCAPI: better DDI support
- › LANCAPI: Reworked LANCAPI-MSN handling
- › LANCAPI: LANCAPI rejects an incoming call if it knows that it won't be answered

LCOS improvements 8.84.0142 RU1

New features

Network connectivity

- › Added a limitation to 2 SMS transmission attempts
- › Syslog message is sent for an unsuccessful SMS delivery

Bugfixes / improvements

- › It is now possible to set the SSH Keepalive parameter on the CLI

LCOS improvements 8.84.0132 Rel

New features

Network connectivity

- › Implementation of an X.25 bridge
- › Configuration of further SNMP communities

Bugfixes / improvements

Wi-Fi

- › If the Accesspoint IP management is done statically by the WLC, the DHCP server is reactivated when deleting an IP address
- › RADIUS accounting data is transmitted completely when using the XML interface

VoIP

- › The WAN address which is used by SIP-ALG is displayed correctly on the status page

Network connectivity

- › If TACACS+ authentication is used, no readonly access is displayed for an SSH connection, since the TACACS+ server adopts the command rights management
- › Read SMS messages can be marked unread
- › Accounting data is collected completely
- › Access rights which are reported by the RADIUS server are evaluated correctly
- › OCSP is available for a LANCOM 1681V

LCOS improvements 8.84.0103 RC1

New features

Wi-Fi

- › RADIUS requests to the MAC address check provider are cached to avoid unessential queries
- › 802.11u (Hotspot 2.0) can be configured via WLAN controller
- › Improved WLAN throughput due to Adaptive Noise Immunity
- › User accounts can be de/activated individually in the RADIUS table
- › The LANCOM device recognizes a querier within the network and, if necessary, activates IMGP snooping automatically
- › Multi-/Broadcasts can be sent within the WLAN with the lowest used data rate of all authenticated WLAN clients
- › Accelerated WLAN roaming when using WPA2 Enterprise with OKC
- › A PublicSpot error page can be displayed if the WAN connection is faulty
- › A terms & conditions confirmation can be activated during a PublicSpot authentication via voucher
- › Smart Ticket web pages can be individualized
- › Further languages added to the PublicSpot pages
- › A PublicSpot user can open a session information page later
- › After a failed PublicSpot authentication the field „username“ is no longer cleared
- › When using Smart Ticket the user can enter the mobile number in any format
- › Smart Ticket can send an SMS directly via the LANCOM mobile radio module
- › WLAN DHCP answers can be converted from broad- to unicasts
- › User specific HTML code can be used in a PublicSpot template. This code will be shown user-dependent on the voucher
- › For PublicSpot authentication the LAN MAC address, the LANCOM IP address and the client IP address can be handed over within the URL

Network connectivity

- › Data volume display for WAN connections
- › DSL sync information is logged to SYSLOG
- › Detailed information for mobile radio connections is written to SYSLOG
- › A /64 prefix can be forwarded to LAN unchanged with IPv6 WAN connections
- › Support for the UMTS stick Web'n'Walk Fusion III
- › The used LTE frequency bands can be set fix
- › ARF networks with identical IP address ranges can be connected via Proxy ARP
- › Sending and receiving SMS via LANCOM mobile radio module
- › Implementation of a rollout wizard
- › IPv6 addresses can be handled in the action table
- › The LANCOM SMTP client supports encrypted connections (TLS/STARTTLS)
- › A RADIUS authentication can be used for device login

- › The LANCOM device automatically creates an SSH key after system reset
- › Information for WAN connections which were established via IPoE/DHCPoE are written to SYSLOG
- › Device information is no longer transferred within the HTTP header
- › Enhanced the action table by the routing tag
- › Sending SMS can be done with an appropriate HTTP call with mobile number and text as parameters

Bugfixes / improvements

Wi-Fi

- › Access points in routed subnets connect to the WLC after a device restart
- › A traceroute via a tagged connection is answered from the correct ARF network
- › New Public Spot users can be created easily in a row using the setup wizard
- › Authentication of a Public Spot user without browser (WISPr) does work in v1.0 and 2.0
- › No further use of the previously retrieved website after logging out of the Public Spot

VoIP

- › If an external ISDN user connects a call to a further remote station, this connection works in both directions now
- › SIP ALG handles shortforms within the SIP header correctly

Network connectivity

- › No unneeded certificate errors are shown in the SYSLOG
- › The VPN load limit for simultaneous tunnel establishments works for aggressive mode connections, too
- › IPv6 prefix changes on a WAN interface are considered within the LAN accordingly
- › With active DNS forwarders and disabled DNS server the LANCOM device answers DNS requests via masked default route with a „Port unreachable“.
- › The CLI command „show vpn“ returns always the complete VPN rule listing
- › NAT-T is included in the IPv6 firewall default configuration
- › The CLI command „sshkeygen“ can be used in scripts using the parameter „-q“

LCOS improvements 8.82.0123 RU2

Bugfixes / improvements

Network connectivity

- › Improved initialization of the internal 3G/4G mobile modem after first start

LCOS improvements 8.82.0100 RU1

Bugfixes / improvements

Wi-Fi

- › No router restart when configuring Public Spot Email/SMS country codes
- › If a not registered Public Spot Client accesses an HTTPS page, the generated SSL certificate is removed afterwards. Thus, a router restart due to memory shortage is avoided
- › Browserless registration of a Public Spot user (WISPr) is now possible using the Windows 8 client, too
- › If multi- or broadcasts are suppressed on a WLAN SSID, a client can still get an IP address via DHCP

VoIP

- › Improved support for non T.38 capable fax devices to a T.38 supported SIP line

Network connectivity

- › During an ISDN-RAS dial-in the windows client is registered faster within the network
- › Improved packet runtimes for data transmission with small packet sizes (e.g. VoIP) via IPsec-over-HTTPS
- › Firewall rule conditions are evaluated for multicast packets, too
- › If a RADIUS server is accessed via VPN tunnel, the NAS IP is communicated correctly
- › No more device restart if there is a %s committed to the SYSLOG module (e.g. as variable within a URL)
- › A LANCOMs configuration can be read via HTTPS using the current Chrome browser for Android devices

LCOS improvements 8.82.0089 Rel

Bugfixes / improvements

Wi-Fi

- › Default text for the Public Spot administration portal SmartTicket is now language dependent
- › The default value for the Public Spot login page protocol is set to HTTP
- › An individual fallback template can be used within the Public Spot module
- › The default Public Spot login page can be personalized by a description field
- › Further optimization of the Public Spot templates
- › For the smartphone-/tablet-display a second picture for the authentication mask can be uploaded

VoIP

- › After having finished a VoIP phone call, further incoming RTP packets in SIP-ALG are not discarded.
- › SIP-ALG exchanges the external IP address with the IP address of the internal subscriber for REGISTER answer packets correctly

Network connectivity

- The ARF network type can be set correctly via CLI
- The IPv6 firewall value „Destination Cache Limit“ can be set via CLI
- Fixed a masking table overflow
- If a PPTP connection is closed by one site, e.g. by internet connection loss, further data can be transmitted on a new connection, even if the old connection is closed logically due to a failed polling

LCOS improvements 8.82.0067 RC2

Bugfixes / improvements

Wi-Fi

- When logging in to a LANCOM Public Spot network, the default browser is invoked automatically on IOS devices, showing the login screen
- New Public Spot display available for the LANCOM L-321, too
- Corrected website title for failed SmartTicket Login
- SmartTicket calling number forwarding included in the new templates

Network connectivity

- If the LANCOM device refuses an ISDN call for dynamic VPN, there is no error display anymore
- VPN connections with an extranet address can be re-established even if configured without keep-alive

LCOS improvements 8.82.0051 RC1

New features

Wi-Fi

- For LANCOM devices with Public Spot option the source VLAN and NAS port ID (interface) of the requesting WLAN client can be handed over within the URL
- Dynamic VLAN assignment for public spot users allows different profile properties (e.g. bandwidth)
- Broadcast and multicast transmission can be disabled per WLAN radio cell
- Support for 802.11u (Hotspot 2.0)
- Support for Public Spot login without using a browser (WISPr)
- The MAC address can be used to identify a Public Spot client to allow automatic re-login at a later time
- For the LANCOM 1781 devices the WLC option can be extended to 12 managed devices

- › Public Spot users can be created automatically
- › Improved display of the Public Spot configuration pages on tablets and smartphones

Network connectivity

- › Adjustment of the syslog validity margin
- › Support for the DHCPv6 server ‚Reconfigure‘ option
- › Extension of the internal syslog table
- › DNS forwarding can be configured for each ARF network
- › The firewall identifies and prevents source address flooding

Bugfixes / improvements

Wi-Fi

- › Multiple PMS (Property Management System) account data usage by the same user is subsumed in the accounting list.

Network connectivity

- › Improved USB device recognition after reboot
- › A LANCOM device does no longer answer LAN ARP requests unintentionally
- › The USB port is reactivated after a USB overcurrent case

LCOS improvements 8.80.0159 RU1

Bugfixes / improvements

Network connectivity

- › Improved initial recognition of the device’s mobile access card on device boot

LCOS improvements 8.80.0157 RU1

Bugfixes / improvements

Wi-Fi

- › The configuration of a LANCOM 3850 without external WLAN card can be stored to the device without errors
- › The automatic MAC address authentication within the Public Spot module can be used again
- › URL forwarding works again after login when using Public Spot SmartTicket
- › Radio-field optimization does no longer affect RADIUS configuration

VoIP

- › SIP-ALG can be used with LAN-LAN routing, too
- › SIP-ALG can handle multiple accounts of a Telekom Call&Surf IP connection
- › SIP-ALG allows for SIP update requests.

Network connectivity

- › A RADIUS server can assign IPv4 addresses to the LANCOM again
- › If a dynamic IPv6 prefix is used in conjunction with fixed address assignment, the assigned address is released when the current prefix is discontinued
- › The masking address of the WAN IP table is no longer used for answering ARP requests
- › Dynamic VPN over D channel can be used again
- › An entry in the DNS forwarding table is operative without restart
- › If a server sends a TCP ACK to an expired session, the LANCOM answers with an RST
- › If no DNS server was assigned to an internet remote station, the DNS server under TCP/IP->Addresses is used.

4. General advice

Disclaimer

LANCOM Systems GmbH does not take any guarantee and liability for software not developed, manufactured or distributed by LANCOM Systems GmbH, especially not for shareware and other extraneous software.

Backing up the current configuration

Before upgrading your LANCOM devices to a new LCOS version it is essential to backup the configuration data!

Due to extensive features it is **not possible to downgrade** to a previous firmware without using the backup configuration.

If you want to upgrade devices which are only accessible via router connections or Wi-Fi bridges, please keep in mind to upgrade the remote device first and the local device afterwards. Please see the [LCOS reference manual](#) for instructions on how to upgrade the firmware.

We strongly recommend updating productive systems in client environment only after internal tests.

Despite intense internal and external quality assurance procedures possibly not all risks can be eliminated by LANCOM Systems.

Using converter firmwares to free up memory

Due to numerous new functions within the LCOS firmware it may not be possible in some circumstances for older devices to keep two fully-featured firmware versions at the same time in the device. To gain more free memory, a smaller firmware with less functionality has to be uploaded to the device first. As a result, significantly more memory will be available for a second firmware.

This installation has to be done only once by using a "converter firmware".

After having installed the converter firmware, the firmsafe function of the LANCOM device is only available on a limited scale. The update to a new firmware is furthermore possible without any problems.

However, after a failed update the LANCOM device works with the converter firmware which only allows local device access. Any advanced functionality, particularly the remote administration, is not available as long as the converter firmware is active.