SECURE. **NETWORKS.**

LANCOM Release Notes

LCOS

9.00 SU8

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

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

November 5th, 2019, 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 Wi-Fi 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 9.00 SU8, as well as the improvements since the previous version.

Before upgrading the firmware, please pay close attention to chapter 3 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. New features, improvements, and history

LCOS improvements 9.00.0328 RU7 > 9.00.0329 SU8

Bugfixes / improvements

General

- 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

LCOS improvements 9.00.0327 SU6 > 9.00.0328 RU7

Bugfixes / improvements

VoIP

- Incoming UDP packets can now be selectively limited to the interfaces LAN, WAN, or VPN in the SIP provider- and SIP-PBX line configuration.
  Further information is available under this KnowledgeBase article.

LCOS improvements 9.00.0316 SU5 > 9.00.0327 SU6

Bugfixes / improvements

Wi-Fi

A security issue within WPA2 authentication (KRACK attack) using 802.11r (Fast-Roaming) while in AP mode (base station) has been fixed:

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

Please check with the manufacturer of your Wi-Fi client for the availability of updates. These devices need to be updated, too.

A security issue within WPA2 authentication (KRACK attack) using WLAN client mode / WLAN station mode with 802.11ac-Wi-Fi modules as well as while using P2P connections with 802.11ac- and 802.11a/b/g/n Wi-Fi modules has been fixed:

- CVE-2017-13077: reinstallation of the pairwise 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

Please install LCOS version 9.24 SU7, 10.12 SU1, or newer when using access points with 802.11ac Wi-Fi module

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 improvements 9.00.0275 RU4 > 9.00.0316 SU5

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 9.00.0258 / 9.02.0258 RU3 > 9.00.0275 RU4

Bugfixes / Improvements

Network Connectivity

- Improved VoIP router support for double challenge authentification
- Fixed a problem with the bandwidth reservation
- ADSL sub interfaces are shown again in the 1781A-3G's MIB
- In an EAP trace the RADIUS server address is displayed again.
- A problem with the COM port server was solved.
- A problem with the volume budget was solved.
- Fixed a problem with the VPN Load Balancer
- It is no longer possible to create multiple DNS entries for the same name on the CLI

Wi-Fi

- After expiration of the Public Spot ticket, the access expires even if the re-login timer has a longer duration than the Public Spot ticket.
- The same user cannot log into the Public Spot if the multiple log-in is deactivated and upper/lower case is not observed.

LCOS improvements 9.00.0237 / 9.02.0237 RU2 > 9.00.0258 / 9.02.0258 RU3

Bugfixes / Improvements

Network Connectivity

- Fixed a problem with LL2M
- The firewall IDS and DOS packet action is set correctly within WEBconfig
- WLAN clients get the correct VLAN ID from an assigned WLC if the WLC is the RADIUS proxy
- Fixed a problem with radio field optimization

Wi-Fi

- Block-Ack handling problem solved for different WLAN clients
- Improved WLAN transmission power in the 2.4 Ghz band

LCOS improvements 9.00.0212 RU1 > 9.00.0237 / 9.02.0237 RU2

Hint

LCOS 9.00 RU2 and LCOS 9.02 RU2 correspond to the same firmware version. For the following devices LCOS is released as version 9.02:

- LANCOM IAP-321
- LANCOM IAP-321-3G
- LANCOM IAP-322
- LANCOM IAP-3G
- LANCOM L-1302acn dual Wireless
- LANCOM L-1310acn dual Wireless
- LANCOM OAP-320
- LANCOM OAP-321
- LANCOM OAP-321-3G
- LANCOM OAP-322
- LANCOM OAP-3G

Bugfixes / Improvements

Network Connectivity

- Fixed a VPN problem with unknown payloads
- The RTP timestamp is set correctly when RTP events are used within the callmanager
- Fixed a problem with the Content Filter
- LC-1781VA(-4G), LC-1781VAW: VDSL (over POTS) modem vectoring support

Wi-Fi

- The expiration types are used correctly when E-Mail2SMS is used
- Improved performance of the Public Spot user management with WEBconfig

LCOS improvements 9.00.0197 Rel > 9.00.0212 RU1

New Features

Network Connectivity

- The content filter only sends one e-mail per day. In this message all errors are listed which occured since the last mail

Bugfixes / Improvements

Network Connectivity

- Client Steering timers are stopped if Client Steering is disabled
- The LANtracer does not stall when the console status tree is learned
- Offline created configurations can be uploaded to the device via WEBconfig again

LCOS improvements 9.00.0186 RC2 > 9.00.0197 Rel

New Features

Network Connectivity

- The mail client supports IPv6

Bugfixes / Improvements:

Network Connectivity

- Improvements for L2TP

LCOS improvements 9.00.0154 RC1 > 9.00.0186 RC2

New Features

Network Connectivity

- An AC name can be configured for the PPPoE server
- Firewall sessions are deleted if the DHCP relay agent overwrites the allocated IP address
- If the LCOSCap feature is enabled in LCOS, this feature will be disabled once during a firmware update.

Bugfixes / Improvements

Network Connectivity:

- No line cut off when using SIP ALG
- The DHCP server ignores packets with invalid or wrong checksum
- Improvements in L2TP

LCOS improvements 8.84.0177 RU2 > 9.00.0154 RC1

New Features

Wi-Fi

- Support for PRP (Parallel Redundancy Protocol) acc. to IEC 62439-3
- WLAN keys cannot be read via SNMP without device password
- CAPWAP can be disabled on a WLC
- RADIUS servers can be specified via DNS hostname
- One particular RADIUS accounting server can be configured per SSID
- Improvements in Band Steering (delayed authentication to the 2,4GHz band)
- Client bridge mode and bandwidth limit are configurable per profile on a WLC
- Support for Fast Roaming acc. to 802.11r
- Support for AutoWDS
- Name length for Point to Point connections extended to 24 characters
- Extended capture format for 802.11n features (Wireshark compatible)
- A LANCOM in client mode extends successively the retention time on a channel if it does not find an access point
- Configuration of point-to-point connections is now independent from the first WLAN SSID
- Additional WLC setting to restart a managed access point after an LCOS upload
- Simplified WLC CA backup
- A WPT redistribution can be initialized by a WLC
- WLAN key fields are treated as password fields and no longer readable in clear text
- Support for Router Advertisement Snooping
- Support for Client Steering
- The settings for double bandwidth can be configured separately for each radio module
- A WLC can rollout a profile automatically depending on the IP address assignment/site
- Improved radio field optimization in consideration of site information
- Support for WLAN Protected Management Frames according to 802.11w
- AP deauthentication switchable in client mode
- If an AP loses the WLC connection it starts a new WLC search automatically
- An automatic AP reallocation occurs if a WLC is restored within a WLC cluster after a breakdown
- U-APSD is switchable per SSID on a WLC
- If the firmware of a managed AP is upgraded via WEBconfig, the AP can be restarted automatically after the firmware upload
- Support for 802.11h
- Support for a dynamic change of user sessions within Public Spot using the XML interface
- A WLAN data trace can be limited to single WLAN management frame classes
- Multiple IPv6 loopback addresses can be configured for a LANCOM device

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
- Within the content filter the FQDN of a site which is connected by HTTPS is taken from the server certificate
- Support for VDSL vectoring
- The LANCOM RADIUS server can be addressed via IPv6
- Support for DS-Lite (IPv4 in IPv6-tunnel)
- IPv6 support for RAS services
- Configuration for (asymmetric) flow control
- The menu tree can be displayed sorted
- Flash memory state can be displayed
- The GPS service on LANCOMs with integrated mobile radio modules (LANCOM 178x-XX) can be used without SIM
- The VPN RAS wizard is available from within WEBconfig
- Configurable SNMP port
- If a LANCOM is used in multiple ARF networks, in which VRRP is only partially used, VRRP packets are only considered within these ARFs
- Bootlog only available with admin rights on the CLI
- Support for DHCP Option 82 (Agent Information Option)
- The internal SSL Certificate has a keylength of 2048 bit
- Die SSL/TLS algorithms are configurable
- The SIM PIN can be changed
- Support for L2TP
- 4G devices support GSM and UMTS Only modes
- Removed support for IPX/SPX
- The RADIUS client supports hostnames
- Support for RADIUS server shell privilege levels
- LANCOM device login can be secured via RADIUS server and Shell privilege level
- PFS and DH groups 15 and 16 can be used in VPN
- The XML interface supports dynamic user session chages
- Support for Lightweight DHCPv6 relay agent
- When authenticating to a Public Spot via SMS, the specified call number is checked for invalid characters
- Advertisements can be shown to Public Spot users in configurable time intervals
- RADIUS supports RADIUS IPv6 attributes acc. to RFC 6911
- SHA2-384 and SHA2-512 can be configured for VPN tunnel establishment

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
- If China is set in the country selection, the country code is communicated properly within the WLAN beacons
- While doing a spectral scan the radio band and its subbands cannot be reconfigured
- Packets to unknown MAC addresses are no longer mirrored back to the client bridge they have been sent from
- The WEBconfig WLAN wizard properly sets the search bands for client mode operation
- If a Spectral Scan is started for both frequency ranges, no error message is displayed afterwards
- SSIDs containing blank characters can be configured via WEBconfig
- The frequency band can be successfully configured within the WLAN wizard

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 the call if it knows that it won't be answered
- Stability improvements with faulty SNMP set commands
- Hex values are saved properly to the MIB
- Usage of the basic setup wizard does not lead to a device restart
- A configuration upload via CLI does not lead to a device restart
- The interface speed is reported properly via SNMP
- Script adjustments for devices with default settings
- Improved SNMP trap descriptions within the MIB
- The WEBconfig basic setup wizard sets the network mask properly
- A firewall rule generated by the VPN RAS wizard is used for generating VPN rules, too
- Hostnames including blank characters can not be added to the BOOTP table via WEBconfig
- WEBconfig is accessible via IPv6 addresses
- If users are authenticated by RADIUS servers in conjunction with an XML interface, accounting data is transmitted properly
- The table „VLAN Group Key Assignment“ can be configured via WEBconfig
- The WEBconfig basic setup wizard does not preallocate fields with „::“
- Syslog server settings can be configured properly via SNMP
- Serial autoconfiguration can be configured via WEBconfig
- The intranet IP address can be configured via WEBconfig
- WEBconfig's Dynamic DNS wizard writes the configuration accurately

3. Important 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.

General notes

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/lcos/lifecycle-management/product-tables/

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 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.

Device-specific advice

LANCOM 178x 4G:

To avoid delayed connection establishments within mobile radio (eg in case of backup) it is recommended to use the **latest firmware version 3.5.24 for the LTE mobile modem** (Sierra MC-7710). Please refer also to the following Knowledgebase article: Link

Using converter firmwares

To use any firmware from version 8.8 in your LANCOM 1722 1723, 1724 and in the L-320agn, L-321agn and L-322agn (less than hardware release E), enough space must be available in the memory of your device.

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 firmsafe 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.