Information regarding

LCOS Software Release 10.00 RU3

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

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

14.06.2017, CBuersch

Table of Contents

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 10.00 RU3, as well as the improvements since release 9.24.

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

Devices delivered with LCOS 10.00 or higher automatically connect to the LANCOM Management Cloud (LMC). This functionality provides zero-touch installation for new devices. In case you do not want to use the LMC, this feature can be disabled while running the default setup wizard for the initial configuration, or at any time from within LANconfig under Management > LMC.
You can manually re-enable the usage of the LMC whenever you want.

LCOS improvements 10.00.0170 RU2 ► 10.00.0171/0238 RU3

Build 0171 for all devices

Bug fixes / improvements

General

- The WEBconfig setup wizard "Configure Internet access" configured a downstream and upstream rate of 2176 kbps for the selected Ethernet interface under "Setup/Interfaces/DSL", and an external overhead of 12 bytes, although these values had never been defined.

Build 0238 for the LANCOM 730-4G

New Features

General

- Support for the LANCOM 730-4G

LCOS improvements 10.00.0165 RU1 ▶ 10.00.0170 RU2

Bug fixes / improvements

General

- A LANCOM LSR script rollout can no longer lead to a sudden restart of the LANCOM device.
- The power LED of a LANCOM access point does not show the status of the LANCOM Management Cloud if the device is managed by a LANCOM WLAN Controller.
- The table /Status/VPN/LMC will not get empty while the configured VPN connections are still active.
- The LANCOM Management Cloud client is available for the LANCOM WLAN Controllers WLC-4006+, WLC-4025+, and WLC-4100.

VPN

- If a disconnection request for an IKEv2 VPN connection is initiated by one station (e.g. after a configuration change), the phase-2 SA disconnect is done at both stations.
- After a configuration change, a CRL check is done in the IKE part of a VPN connection

Wi-Fi

- After having received a profile from the LANCOM WLAN controller, managed LANCOM access points are permanently accessible under the IP address which is saved within that profile.

VoIP

- Establishing a Telekom SIP trunk line can no longer cause a sudden restart of the LANCOM VoIP router due to DSL problems or faulty encryption settings.

LCOS improvements 10.00.0107 Rel ▶ 10.00.0165 RU1

New features

General

- The automatic VLAN detection was extended with provider 1&1 (VLAN 7).
- LANCAPI connections can only be established from the WAN side via VPN.
- For a more subtle categorization, new categories have been added to the Content Filter and existing categories with comprehensive topics have been divided into single categories.
- **Note:** The IP router service statistics under "/Status/IP-Router/Service-Table" is no longer supported in further LCOS versions. It is recommended to use the new Layer 7 application detection instead.

Bug fixes / improvements

General

- Performance improvements for PPPoE- and IPoE WAN connections when using logical WAN connections over a physical WAN interface.
- The SNMP port 161 is no longer shown as closed in the services overview, although SNMPv3 is allowed for WAN. For clarity reasons, a separate item for SNMPv3 was added to the services overview.
- The router password of a user with admin rights can now consist of more than 15 characters.
- IPv4 fragment forwarding (/setup/ip-router/1-N-NAT/fragments/) with simultaneous QoS limitation is no longer classified as an attack, communication is further possible.
- Dynamically learned routes via eBGP, iBGP or RIP are added only to their corresponding routing context (routing tag), see LANCOM Knowledgebase).
- If an IP route is changed to a different remote site using WEBconfig or the command line, these changes apply immediately.
- Three useless dialogs for configuring EoGRE tunnels have been removed from the configuration of LANCOM routers without LAN bridge.
- The combined usage of N:N NAT and the integrated DNS server does no longer lead to unexpected router restarts in particular cases.
- If WAN tag generation is set to "automatic" and the first route for the remote site is set to a tag different from 0 in the routing table, this route is no longer added to the forwarding information base with tag 0 (see LANCOM Knowledgebase).

VPN

- If a LANCOM router has accepted an IKEv2 connection on the LAN, this connection is established even if the source address does not contain routing tag 0.
- No more sudden router restart if a GRE tunnel is put into an IPSec tunnel and both remote sites are named identically.
- If a CHAP response is received during an L2TP negotiation, the connection is not relevant for counting VPN licenses.

Wi-Fi

- An accurate text is shown on the English login page of a Public Spot scenario with PMS accessibility.
- After a device reset, the following default values change as follows:
- Wi-Fi idle timeout is 900 seconds (15 minutes)
- Band Steering is enabled by default
- Adaptive RF Optimization is enabled by default

VoIP

- RTP events are recognized accurately within the RTP Stream with DTMF signaling as per RFC 2833.
- With disabled Voice Call Manager the configured SIP provider lines are no longer established.
- A change of the valid registrar IP address via DNS resolution is now applied, even if a SIP trunk line is already established in static mode.

LCOS improvements 10.00.0063 RC1 ▶ 10.00.0107 Rel

New features

Network Connectivity

- Bonjour Proxy
- Added a status table for recent admin logins
- Switchable WAN access for the RADIUS server
- Telnet is now disabled by default

Wi-Fi

- Public Spot with PMS supports now Rx- and Tx bandwidths for charges
- Configurable headline for the Public Spot login page
- PMS login now supports the function “accept terms of service“

Bug fixes / improvements

Network Connectivity

- Fixed a re-keying issue during an IKEv2 VPN connection
- SIP lines are reconnected with configured load balancer
- SIP calls are no longer disconnected after 15 minutes
- IKEv2 VPN connections with CFG server mode are re-established
- After a factory reset the cloud certificate is deleted, too
- The sender address is set correctly with L2TP tunnels
- Needless information is deleted from the bootlog
- Improvements in Layer 7 application detection
- Fixed a SIPS issue
- Revised link on the login page for the WEBconfig IPv6 HTTPS connection to the LANCOM device

Wi-Fi

- Script rollout via WLC works again as provided
- The status page is displayed correctly after a Public Spot login

LCOS improvements 9.24.0153 RU3 ▶ 10.00.0063 RC1

New features

Network Connectivity

- Support for the LANCOM Management Cloud
- IPv6 support within the Voice Call Manager
- Support for SIPS and SRTP on the client's side in the Voice Call Manager
- Support for tunnel password- and LCS routing tag attribute by the internal RADIUS server
- Support for layer 7 application detection
- SIP line extension for the VoIP+10 option by additional 10
- The number of default SIP lines is increased from 20 to 25 lines
- New status table for recent admin logins
- SIP trunk support within the LAN
- Incoming requests for SIP-PBX lines can be restricted

Wi-Fi

- Support for RADIUS CoA within the Wi-Fi

Bug fixes / improvements

Network Connectivity

- RADIUS authentication via VPN works again if WAN access is configured to „only via VPN"
- End marker for unencrypted LCF/LCS files
- The Outbound proxy parameter was removed and is set automatically now

Wi-Fi

- The firmware version can be optionally used within the WLC script management
- The first comment entry in the LANCOM device can be set from a WLC

3. Important advice

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 support of the current LCOS version

As from LCOS 10.00 support for the following devices is discontinued:

- LANCOM L-320agn Wireless (less than Hardware Release G)
- LANCOM L-320agn Wireless (white) (less than Hardware Release G)
- LANCOM L-321agn Wireless (less than Hardware Release G)
- LANCOM L-322agn dual Wireless (less than Hardware Release G)
- LANCOM 1681V
- LANCOM 1781EF
- LANCOM 1781EW
- LANCOM 1780EW-3G
- LANCOM 7100
- LANCOM 9100
- LANCOM OAP-382

- The LANCOM access points of the L-32x series with the name addition R2 (LANCOM L-32x R2 or equal or above Hardware Release G) are not affected by this and continue to receive current LCOS versions.
- 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/

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.

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.