Release Notes

LCOS
10.94 RU2

Table of contents

1. Preface

The LANCOM family of operating systems—LCOS, LCOS SX, LCOS LX, and LCOS FX—forms the trusted basis for the entire LANCOM range of products. Within the scope of the hardware specified by the products, the latest firmware version is available for all LANCOM products and is offered by LANCOM Systems for download free of charge.

This document describes the innovations within LCOS software release 10.94 RU2, as well as the improvements since the previous version.

Before upgrading the firmware, please pay close attention to chapter 7 “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
www.lancom-systems.com/service-support/instant-help/common-support-tips

2. The release tag in the software name

Release Candidate (RC)
A Release Candidate has been extensively tested by LANCOM and includes new LCOS featurses. It is suitable for testing and is not recommended for use in productive environments.

Release Version (REL)
The release version has been extensively and successfully tested in practice. It contains new features and improvements over previous LANCOM operating system versions and is therefore recommended for use in productive environments.

Release Update (RU)
A release update is a further development of an initial release version in productive environments and contains minor improvements, security fixes, bug fixes and smaller features.

Security Update (SU)
Contains important security fixes for the respective LANCOM operating system version and ensures that your security level remains very high on an ongoing basis in your productive environment.

3. Device-specific compatibility to LCOS 10.94

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 www.lancom-systems.com/products/firmware/lifecycle-management/product-tables

LANCOM devices without support as of LCOS 10.94

→ 1790-4G
→ 1790VA-4G
→ 1793VA-4G
→ ISG-1000
→ ISG-4000
→ 883 VoIP
→ 730VA
→ L-321agn (R2)
→ OAP-1702B
→ LN-830U
→ 1906VA
→ 1781EW+
→ LN-830E
→ LN-830E+
→ 1790EF
→ 884 VoIP
→ R883+

4. Advices regarding LCOS 10.94

General notes on the update

As of LCOS 10.90, the CLI menu for VRRP has been moved from '/Setup/IP-Router/VRRP/' to '/Setup/VRRP/'. The table structure and the associated OID path have also changed due to the support for VRRPv3 and IPv6.

Please note that add-ins for the LMC and any existing scripts for VRRP must be adapted for LCOS 10.90 and higher. Existing scripts for VRRP are not compatible with LCOS 10.90 and higher.

Information on default settings

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.

Support for eSIM

The following products and hardware releases support eSIM functionality as of LCOS 10.94:

- → LANCOM 1930EF-5G
- → LANCOM 1936VAG-5G
- → LANCOM OAP-5G
- → LANCOM 1800EF-4G (from hardware release D)
- → LANCOM 1800EF-5G (from hardware release D)
- → LANCOM 1800EFW-5G
- → LANCOM 1803VAW-5G
- → LANCOM 180xVA-4G (from hardware release D)
- → LANCOM 180xVA-5G (from hardware release D)

The above cellular routers (equipped with the Quectel EM060K 4G module and Quectel RM520N-GL 5G module) must be updated to the latest WWAN firmware before using eSIM functionality.

The latest WWAN firmware is available for download in the respective product's download section.

The following minimum firmware versions are required for eSIM operation:

- → For 4G cellular routers with Quectel EM060K:
  EM060KEAAAR01A05M2G_A0.300.A0.300-RU1
- → For 5G cellular routers with Quectel RM520N-GL:
  RM520NGLAAR03A03M4G_A0.301.A0.301-RU1

IPv4 WAN Access Switch for Internal DNS Services

Starting with LCOS 10.94, access to the DNS forwarder and DNS server for IPv4 WAN access can be globally enabled or disabled. After updating to LCOS 10.94, the configuration is set to “VPN” by default, meaning that the DNS service is only accessible via LAN and VPN. VPN access includes the protocols IKE/IKEv2/IPSec and WireGuard.

As a result, access to the DNS services on interfaces where the router acts as a PPTP, L2TP, or PPPoE server is no longer permitted. In such cases, a manual adjustment of the configuration after the update is required. This does not apply when clients use an external DNS server — it only affects setups where the router itself provides DNS services.

New Configuration Method for the DHCP Client

As of LCOS 10.94, the WAN or communication layers “DHCP” and “B-DHCP” (Broadcast-DHCP) have been removed from the Communication Layers table. The configuration of the DHCPv4 client is now performed in the DHCP Client Interfaces table in LANconfig under: IPv4 → DHCPv4 → DHCP Client.

A separate entry must now be created for each WAN and LAN interface on which the DHCP client should be enabled.

Additionally, the configuration option for the DHCP client on the LAN has been moved from the DHCP Server settings into this new table. The DHCP client is now configured centrally in one place.

When updating to LCOS 10.94, the configuration is automatically converted to the new format.

Please note that downgrading to a device with LCOS earlier than version 10.94 may result in a device with a DHCP client WAN connection (e.g., WWAN connections) being unable to establish a connection, since no conversion back to the old DHCP configuration is possible. In this case, a previously saved configuration must be restored.

Please also refer to the general downgrade instructions for additional guidance.

5. Feature overview LCOS 10.94

5.1 Feature highlights

eSIM: The smart mobile communications solution built into the LANCOM router

With integrated eSIM technology, LANCOM SD-WAN gateways connect effortlessly to the mobile network. Instead of physical SIM cards that have to be managed and replaced manually, mobile contracts and profiles can be set up and managed digitally. The permanently installed eSIM (consumer version) is programmed via software with the provider's profile. This makes it possible to upload, change, update, and manage contracts or tariffs quickly and easily – without time-consuming card replacements or costly on-site visits. New devices are ready for immediate use, and rollouts across multiple locations or large device fleets can be completed in no time. At the same time, security is enhanced, since there are no physical cards that could be lost or misused. Whether for mobile workplaces, branch networks, or as a backup solution, eSIM ensures simple management of mobile connectivity while providing maximum flexibility and efficiency.

WireGuard

WireGuard support provides a fast and flexible solution for secure VPN connections — ideal for small-scale networking scenarios such as home offices or businesses with only a few VPN tunnels. Thanks to its streamlined design and intuitive operation, this modern protocol offers a simple and reliable way to establish secure connections. Cutting-edge cryptographic algorithms ensure robust protection. In addition, WireGuard is supported on all major operating systems, making it an excellent choice for heterogeneous IT environments.

Two-factor authentication (2FA)

The two-factor authentication (2FA) feature makes local device management with LCOS even more secure. In addition to the standard password, an additional security code can now be required — conveniently generated by a common authenticator app. This ensures that access remains protected even if the password is compromised. Setup is straightforward using standard apps and offers effective protection against brute-force attacks. By enabling 2FA, you enhance your security standards and reliably prevent unauthorized access to your devices.

You can find further features within the individual builds sections in chapter 6 "History LCOS 10.94".

6. History LCOS 10.94

LCOS improvements 10.94.0217 RU2

New features

→ In the SCEP client, the verification of the accessed URL against the server's identity can be configured in TLS.

→ There is now a status table for WWAN bridge mode.

→ The new 'Query-Timeout-ms' parameter in the DNS forwarder allows you to set a timeout in milliseconds. If this timeout expires, the forwarder selects the next DNS server.

Bug fixes

General

→ When the router enters cold standby mode, power to the SIM card is cut off, which is why the PIN must be re-entered after the router returns to active mode. Although the router recognized that the SIM had already been unlocked, it did not reset the status when entering cold standby mode. As a result, the cellular connection could not be reestablished after the router returned from cold standby to active mode.

→ When restarting the cellular modem on routers equipped with the Sierra EM/MC7421 cellular modem, the system incorrectly reported that the SIM card had been removed. If a SIM card was removed or inserted while the cellular modem was restarting, this could cause the router to restart unexpectedly multiple times.

The following mobile routers were affected by this issue:

- 1790-4G+
- 1790VA-4G+
- 1793VA-4G+
- 1800VAW-4G
- 1800VA-4G
- 1803VA-4G
- 1926VA-4G

→ If a Telekom Internet connection using a custom PPP user or the old default user 'internet-default@t-online.de' is first removed via the Setup Wizard's 'Delete remote station or access' option, and then an Internet connection is created using LANconfig 10.94 RU1 with the new default user '5200...' the connection to the Telekom ACS server was terminated with error code "9005".

→ When switching SIP servers, the Voice Call Manager continued to use the ‘REGISTER Expires’ value negotiated with the first SIP server. This could result in the ‘REGISTER Expires’ value having to be renegotiated each time a re-registration occurred.

→ When configuring a RADIUS accounting server in a public hotspot scenario, an invalid value for ‘Acct-Status-Type’ was sent in the ‘Accounting-On’ message, which is responsible for enabling accounting.

→ To address CVE-2026-27171, the zLib library has been updated to version 1.3.2. *

→ If an SNMP user was created via the WebConfig interface and an attempt was subsequently made to access the LANCOM router using that user via LANmonitor or other SNMP-compatible software, this did not work. Access only worked after the user created via WebConfig was deleted and then recreated using the command line or via LANConfig.

VPN

→ After saving the device configuration to the router (via LANconfig, WEBconfig, or LMC), all VPN connections were lost.

→ If a LANCOM R&S®Unified Firewall initiated a rekey during an existing IKEv2 connection to a LANCOM router, the IKEv2 connection might have been disconnected.

Wi-Fi

→ After updating the firmware of a WLAN controller (or router with the WLC Basic option) to LCOS 10.94, the configuration converter might have stored an incorrect value for the ‘Beacon Backup’ parameter in the encryption profiles. This resulted in the managed access points reporting a configuration error in LANmonitor, and WLAN networks with WLC tunnels were no longer functional. Furthermore, the WLAN controller’s configuration could no longer be saved via LANconfig. LANconfig then reported an incorrect value for parameter ‘1.2.37.1.1.1.60’.

→ When using 802.11r, each WLAN controller set its own MAC address as the R0KH ID. In a WLC cluster scenario, this caused 802.11r to malfunction. The string “CAPWAP” is now always used for the R0KH-ID.

→ In a WLAN controller scenario, changes made to the interfaces (e.g., switching from WLC tunnel to ‘LAN on AP’ or deleting or adding SSIDs) were not applied to the access points. This resulted in communication becoming impossible on some or even all SSIDs.

* LANCOM Systems keeps all program libraries used in LCOS firmware up to date with the latest security patches and fixes security vulnerabilities even if they cannot be exploited in the firmware.

LCOS improvements 10.94.0162 RU1

New features

→ Own VRRP advertisements are now ignored in the event of a network loop error, and a corresponding syslog message is generated.

Bug fixes

General

→ In a BGP scenario, if there were two identical routes in the RIB table (a static route to a local LAN interface and one received from another BGP router), the received route was not removed when the local LAN interface was inactive.

→ To fix CVE-2025-1118, the OpenSSL library was updated to version 3.5.5. *

→ In LCOS 10.94, the 'DHCPOE' layer for Internet connections has been removed. Instead, there is now a 'DHCP Client Interfaces' table in the 'IPv4 → DHCPv4' menu. This table contains all Internet connections that use DHCP, including the default connection 'INTERNET-DEFAULT.' Since entries in the 'DHCP client interfaces' take precedence over a static configuration (IPoE), this meant that when using the 'INTERNET-DEFAULT' Internet remote station with a static configuration after a firmware update to LCOS 10.94 Rel, this connection was no longer functional.
The configuration converter now first deletes the 'DHCP client interfaces' table and only then adds the Internet connections that use DHCP.

→ When updating the firmware from LCOS 10.80 to LCOS 10.94, the converters for the configured mobile connections might not have been executed in the correct order. This led to the 'DHCP client interface' for the mobile connection not being created, meaning that the mobile connection was not functional.

VPN

→ WireGuard packets were displayed multiple times in the 'WG packet' trace.

→ The IKEv2 encryption algorithms AES-CBC and AES-GCM or ChaChaPoly were sent in a joint ESP proposal instead of in separate proposals as required by the standard.

* LANCOM Systems keeps all program libraries used in LCOS firmware up to date with the latest security patches and fixes security vulnerabilities even if they cannot be exploited in the firmware.

LCOS improvements 10.94.0127 Rel

New features

WLC

→ The access point license limit of the LANCOM 2100EF has been increased to 60.
→ The target transmission power can now be configured separately for each access point.
→ The Wi-Fi encryption settings are now configured in encryption profiles. Existing configurations will be converted during the upgrade.
→ Discontinuation of AutoWDS

Bug fixes

General

→ When multiple service objects and a DNS target were used simultaneously in a firewall rule, the DNS target was not taken into account.
→ In the syslog of a LANCOM 2100EF, messages about temperature incorrectly displayed a reference to a WLAN module: “Temperature is back to normal, wireless is turned on again”.
→ The status of the ‘Remote Tables Last Change’ info field in the ‘Status/LLDP’ console path was not processed correctly if it was empty (zero). When reading the ‘Status/LLDP’ console path, this caused the CPU load to permanently increase to 100%.
→ If an IDS/DoS message was sent by the firewall after an IDS/DoS event, this could cause the router to restart unexpectedly.
→ The parameter ‘-E’ can be used to restrict the iPerf client on the console to a specific Internet peer. If this parameter was applied on a router with a configured load balancer, the iPerf client used all peers in the load balancer instead of restricting it to one connection. This led to incorrect measurements.
→ Due to a change in the file name format, updates for the BPJM filter could be downloaded but not unzipped. The message “Info-Request-failed” was then displayed in the console path ‘Status/Firewall/BPJM/Last-update-result’. This resulted in the BPJM filter not being functional.
→ After scanning the mobile network with the console command “do Scan-Networks -e -f,” it occurred on the LANCOM 1800EF-4G, 1800VA-4G, and 1803VA-4G, the mobile modem might remain in the ‘Registration Denied’ status for approximately 28 minutes, even though the registration in the mobile network was successful.

VPN

→ WireGuard data (both IPv4 and IPv6) was not included in the volume budget.

→ If the DNS resolution of the WireGuard remote station took too long, the initial connection attempt failed.

→ If a router acted as a WireGuard responder and packets had already been sent to the responder's network via the WireGuard connection before the WireGuard connection changed to 'Connected' status, the responder received the packets and forwarded them.

LCOS improvements 10.94.0093 RC2

New features

→ New ‘Always on’ switch for WireGuard remote stations

→ The BGP password can now be up to 254 characters long.

→ Support for RADIUS bandwidth limits in the PPPoE server via LANCOM vendor attributes LCS-TxRateLimit (2356-8) and LCS-RxRateLimit (2356-9).

Bug fixes

General

→ If two Ethernet ports were assigned to different LAN interfaces on a LANCOM 1640E / 1650E or a router from the 179x or 192x series and these were combined in a bridge group, the router was unable to forward ARP reply packets correctly and discarded them. This resulted in restricted communication within the network.

VPN

→ A WireGuard connection was not recognized as a VPN connection in the router firewall by an ‘Allow VPN’ rule (IPv4 - condition ‘for VPN route’, IPv6 - action object ‘ACCEPT VPN’). This resulted in IPv4 and IPv6 traffic being blocked by the ‘DENY-ALL’ rule of the destination router when a WireGuard connection was established between two routers.

→ When transferring IPv4 packets over an IPv6 connection via WireGuard between two routers, the checksum of the IPv4 header could sometimes be calculated incorrectly. This resulted in the packet being discarded and the process being acknowledged in the WG packet trace with the error message “Discarded, decapsulate wrong v4 header checksum.”

Wi-Fi

→ After updating to LCOS 10.94 RC1, there was an incorrect default parameter in the ‘Setup / WLAN Management’ path. As a result, the device configuration could no longer be edited with LANconfig.

LCOS improvements 10.94.0064 RC1

New features

General

→ Support for Wireguard
→ Support for eSIM
→ Two-factor authentication for local login to the router via WEBConfig, SSH, Telnet, TFTP, and outband
→ Support for the hybrid post-quantum algorithm mlkem768×25519-sha256 in SSH
→ Support for the hybrid post-quantum ECDHE-MLKEM key agreement for TLSv1.3 (X25519MLKEM768)
→ The DHCP client is now configured with one necessary entry per interface in a separate DHCP client table.
→ Support for the parameters Framed IP Address, Framed IPv6 Prefix, Delegated IPv6 Prefix, and Framed IPv6 Address in the RADIUS server user table
→ The syslog message for intrusion detection has been supplemented with information about the affected network.
→ The LMC status can be displayed in the WEBconfig dashboard.
→ E-mail notification in case of failed ACME retrieval and before certificate expiry
→ Support for Q-in-Q VLANs in PPPoE servers
→ If the provider transmits a 'LINE ID' (connection identification) in PPP, this is displayed in the status.
→ APN access data (user name, password, authentication method) can now be stored directly in the WWAN profile instead of via an additional entry in the PPP table. The configuration option in the PPP table remains available.
→ The LANCOM 2100EF now supports a maximum expansion of 60 access points in the WLC function with corresponding additional licenses.
→ Support for the new %w variable for the action table, which allows the IPv6 LAN prefix to be combined with a static interface identifier
→ Support for a history of recent commands in the CLI
→ Support for freely configurable alias commands in the CLI
→ Using firmware safe test mode for firmware updates via the LMC
→ Support for RADIUS Change of Authorization (CoA) for the 802.1X Ethernet port authenticator
→ Configuration option for MTU in the load balancer table

→ Support for DSL forum vendor-specific RADIUS attributes according to RFC-4679 in the PPPoE server and transmission to a RADIUS server
→ Show command for PPPoE user details in the PPPoE server
→ The device search in WEBconfig now displays the results sorted by IP address.
→ The internal WWAN carrier database for automatic APN selection has been updated.
→ Switch for IPv4 WAN Access to Internal DNS Services
→ Support for WWAN Bridge Mode

WLC

→ Support for the 'Beacon protection' parameter in the WLC network profile
→ Support for new Wi-Fi 7 access points in the WLC's central firmware management
→ Support for Wi-Fi 7 MLO configuration in the WLC

VoIP

→ Manipulation of the source number for outgoing calls to Company Flex connections
→ Ensuring a free voice channel for defined emergency numbers

Omission

→ The WAN layers DHCP and B-DHCP (broadcast DHCP) are no longer required. The DHCP client is now configured with one necessary entry per interface in a separate DHCP client table.
→ Removed the DHCP Client Mode configuration from the DHCP Server table
→ Discontinuation of AutoWDS
→ The "Exclusive" parameter for WAN RADIUS server operation is no longer applicable.
→ The 'Max WAN Queue Length' switch has been removed.
→ Support for the LANCOM Battery Pack is no longer available.
→ Removal of inheritance in WLC profile configuration

Bug fixes

General

→ The 'jsPDF' program library has been updated to version 3.0.2, which fixes the security vulnerability described in CVE-2025-57810.
→ The SFP trace (trace # SFP) could not be executed on the R903, even though the R903 is equipped with an SFP port.

7. 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.

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de | lancom-systems.com