

Release Notes

LCOS

10.92 RU2

Table of contents

02	1. Preface
02	2. The release tag in the software name
03	3. Device-specific compatibility to LCOS 10.92
03	LANCOM devices without support as of LCOS 10.92
03	4. Advices regarding LCOS 10.92
03	General notes on the update
03	Information on default settings
04	5. Feature overview LCOS 10.92
04	5.1 Feature highlights
04	Cloud-based network security with the LANCOM Security Essentials Option
05	6. History LCOS 10.92
05	LCOS improvements 10.92.0167 RU2
06	LCOS improvements 10.92.0098 RU1
09	LCOS improvements 10.92.0018 Rel
11	7. General advice
11	Disclaimer
11	Backing up the current configuration
11	Using converter firmwares to free up memory



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 10.92 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 features. 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 10.92

LANCOM products regularly receive major firmware releases throughout their life-time 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 10.92

- LANCOM R800V
- LANCOM LN-630acn
- LANCOM 1781VA
- LANCOM 1906VA-4G
- LANCOM L-322agn (R2)
- LANCOM LN-862
- LANCOM LN-860
- LANCOM OAP-830
- LANCOM OAP-1700B
- LANCOM OAP-821
- LANCOM OAP-822
- LANCOM IAP-1781VAW(+)

4. Advices regarding LCOS 10.92

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.

5. Feature overview LCOS 10.92

5.1 Feature highlights

Cloud-based network security with the LANCOM Security Essentials Option

With LCOS 10.92, you fulfill all the requirements to upgrade your devices with the LANCOM Security Essentials Option. The LANCOM Security Essentials Option provides an efficient and reliable solution to protect networks against threats such as ransomware, phishing, malware, and credential theft. The integrated Content Filter effectively blocks unwanted and illegal internet content – preserving corporate integrity and significantly reducing liability risks. At the same time, the BPjM module of the German Federal Review Board for Media Harmful to Minors (BzKJ) reliably shields minors from harmful content. The underlying database used to verify website content is hosted in a GDPR-compliant cloud provided by European security specialist Bitdefender. For maximum scalability, use of the option is not limited to a specific number of users – making it ideal for growing networks.

Note: The LANCOM Security Essentials Option is available as an upgrade for LANCOM SD-WAN gateways, SD-WAN central site gateways, and WLAN controllers as the successor product to the LANCOM Content Filter.

You can find further features within the individual builds sections in chapter 6 “History LCOS 10.92”.

6. History LCOS 10.92

LCOS improvements 10.92.0167 RU2

Bug fixes

General

- When TACACS+ was configured, opening the port forwarding table via WEBconfig could cause the router to restart unexpectedly.
- If the mobile network provider's network was in an error state, the router detected this and performed a reinitialization followed by a restart of the mobile modem in order to recover from the error state. This could take several minutes.
In such a case, the mobile radio modem is now reattached, thus minimizing downtime.

VPN

- A newly created IKEv2 connection under iOS 26 could not be established because a new iOS feature was not compatible with LCOS.

Wi-Fi

- When using client steering (not recommended; client management should be used instead), the WLAN controller could suddenly restart in environments with a large number of logged-in wireless devices.

LCOS improvements 10.92.0098 RU1

New features

- When using Dynamic Path Selection (DPS), the ICMP identifier is now changed after every 4096 measurements (for the default interval of 1 second this means every 70 minutes).
- The backoff time for a failed VPN tunnel establishment can be configured on the CLI.
- SIP-ALG: PMTU reduction and fragmentation are only carried out if the MaxTxRate is less than 1 Mbps. If no bandwidth is configured, no reduction or fragmentation is performed.
- The default country code for the LANCOM DECT N610 IP is 'Europe' instead of 'undefined'.
- Content Filter: If an override is executed by a user, this applies to the entire domain and regardless of the protocol used. This means that a direct call after an HTTPS redirect also works.

Bug fixes

General

- If a mobile radio module restarted due to a hardware reset, it could happen that the internal PIN status in LCOS was not reset. As a result, LCOS could no longer unlock the SIM and the mobile radio module could no longer connect to the mobile radio network.
- If a timeout occurred when using the internal HTTP server (e.g. to provide certificates) via a slow connection, this led to an immediate restart of the router.
- If a configuration was rolled out several times via the LMC to a device that was in offline status, this resulted in TACACS+ authentication being deactivated.
- When using LANCOM Security Essentials, it could happen that applications that were allowed or classified as secure (e.g. Office 365) and categories were still blocked by the content filter.
- When reading the hexadecimal password of the GPON module, the router converted it to lowercase letters. If uppercase letters were used in the PON password (under Interfaces / WAN / PON), this led to a permanent boot loop of the GPON module.

→ When deleting the ARP table after the 'ARP aging minutes' have expired, a request is made to the firewall for each deleted entry in order to delete the ARP resolution for affected sessions. In larger scenarios with many simultaneous sessions, this led to periodic short load peaks with every second deletion of the ARP table (i.e. every 30 minutes with the default 'ARP aging minutes' value of 15 minutes). This could lead to short-term connection problems.

ARP aging now has an interval of 30 seconds. Furthermore, the number of ARP entries that can be deleted simultaneously is limited (can be adjusted via the console path 'Setup / TCP-IP / ARP-Max-Remove', default value is 25). If more ARP entries are to be deleted and the ARP aging limit is exceeded as a result, ARP aging is reduced to 10 seconds.

→ On a vRouter operated in Hyper-V, the checksums for TCP and UDP were calculated incorrectly for a PPPoE connection. Depending on the network card used, this could lead to heavy packet loss, among other things.

→ If the router was assigned an IP address with x.x.x.255 during PPP negotiation and the dial-in router of the Internet provider also claimed this IP address, the router rejected DNS responses. As a result, no Internet connection could be established via the router. Furthermore, the router could not establish a connection to the LMC.

→ After updating the firmware of a LANCOM 1793VA-4G to LCOS 10.90, it could no longer establish a cellular connection with the default settings of the cellular profile 'WWAN-DEFAULT'. This meant that a zero-touch rollout was no longer possible.

→ If an action with a large number of characters was stored in a firewall rule via WEBconfig, this led to an immediate restart of the router.

→ If a vRouter operated in Proxmox with a VirtIO network card for the Internet connection routed data traffic with many simultaneous sessions via the Internet connection (such as a speed test), this led to heavy packet losses or even an interruption of the Internet connection.

Wi-Fi

→ If a 4-digit VLAN ID was entered in the 'Set up WLC profile' setup wizard, this could cause the device to restart immediately after completing the wizard.

VoIP

- The Voice Call Manager did not forward a busy signal to ISDN and analog subscribers.
- After an update to LCOS 10.9x, it could happen that a SIP client could no longer log on to a SIP PBX (e.g. a Cloud PBX) via a SIP PBX line set up in the Voice Call Manager.
- On the WEBconfig interface of a LANCOM 1803VA it was not possible to configure or activate ISDN interfaces.
- If the Voice Call Manager received a 'Provisional Update' from the SIP PBX for an outgoing call, the Voice Call Manager then sent a PRack with "RAck: 2 100 UPDATE" instead of "RAck: 2 100 INVITE" to the SIP provider. This resulted in the SIP provider terminating the connection with the message "481 Call/Transaction Does Not Exist".
- The Voice Call Manager could not process multi-part SDP messages and then sent the message "406 SDP Not Acceptable".
- If a SIP user established a call with a video and an audio stream to an ISDN or analog user, the Voice Call Manager removed the video stream and deactivated the audio stream (m=audio 0). This meant that no voice communication was possible.
In such a scenario, the Voice Call Manager now deactivates the video stream and leaves the audio stream active.

LCOS improvements 10.92.0018 Rel

New features

- Support for the LANCOM Security Essentials Option
- Change of the Content Filter to Bitdefender
Please note that some of the categories have changed and new categories have been added as a result of the change. It is recommended to check the configuration after the LCOS update. Please also refer to the [notes on the update](#).
- Support for the backup/restore function of the device
- Support for Dynamic RADIUS Caching
- The behavior for inter-tunnel traffic can be configured in L2TPv3.

Bug fixes

General

- When using an unmasked default route for an IKEv2 connection, it was incorrectly displayed that the DNS server could be reached from the WAN.
- The DSL line code has been updated to version 12.9.1.2.0.7 for devices of the 180xVA and 1926/1936 series.
- The password change of a logged-in TACACS user was acknowledged in WEBconfig with the error message "Not Found". As a result, the password change failed.
- When repeatedly reading out the console path 'Status/VDSL/Line-Type' (this also affected the higher-level path 'Status/VDSL') with the repeat command (e.g. "repeat 3 ls Status/VDSL/Line-Type"), the information was only output once.
- If no gateway was entered on the standby router in the DHCP network in a VRRP scenario (0.0.0.0), the standby router sent a DHCP offer without a gateway instead of using the VRRP IP address. If an end device first received the DHCP offer from the standby router instead of the master router, it did not accept the assigned IP address and communication was not possible.
- If the VLAN of a network - and thus also the routing tag of the network and the OSPF instance - was changed in an OSPF scenario, this resulted in the OSPF neighbor subsequently remaining in the 'down' status and the connection not being re-established.

VPN

- If a router with several active Internet connections and an IKEv2 connection with a specific routing tag received an IKE packet with the message type 'Redirect', the router changed the routing tag for the outgoing IKE_SA_INIT to 0 instead of retaining the previous routing tag. As a result, the VPN communication was then transmitted via the wrong Internet connection.

Wi-Fi

- The IAPP table can hold a maximum of 2048 entries. New access points can therefore no longer be added once the maximum has been reached.
If an access point could no longer be added to the IAPP table and therefore could not be found in the table, this led to an immediate restart of the access point.
- If there was an IP address entry for a freely accessible web server in the 'Setup/Public-Spot-Module/Free-Server' table, an error message was displayed when an HTML page of this web server was called up due to a missing HTML header.

VoIP

- If communication with a particular destination was only possible via a specific, dynamically learned route with 'next hop' (e.g. via BGP), but a statically configured default route without 'next hop' was also configured for the same remote station, but with a different routing tag, and the router received a packet for the destination network before the dynamic route was learned, the router did not replace the static route with the dynamic route for the session (the static route was not invalidated). As a result, the static route continued to be used and the destination network could not be reached via it.

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.

