Release Notes

LCOS
10.70 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 10.70 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 has been extensively and successfully tested in practice. It contains new features and improvements over previous LANCOM operating system versions. Recommended for use in productive environments.

Release Update (RU)
This is a further development of an initial release version and contains minor improvements, 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.

3. Device-specific compatibility to LCOS 10.70

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

Support for the following devices is no longer available as from LCOS 10.70:

- → LANCOM 1781EF+
- → LANCOM 1783VA
- → LANCOM 1781VAW
- → LANCOM 1783VA-4G
- → LANCOM R883VAW
- → Business LAN R800A

4. Advices regarding LCOS 10.70

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 10.70

5.1 Feature highlights 10.70

Advanced Mesh VPN

With classic, star-shaped VPN site networks, in which all branches are only connected via the headquarters and not directly to each other, the Internet line of the headquarters quickly becomes the bottleneck of the entire communication. With Advanced Mesh VPN, the branch offices are now directly interconnected, resulting in significantly less traffic at the headquarters and thus higher performance. The VPN tunnels are established dynamically as soon as data traffic is transported from one branch office to another. If there is no more communication, the VPN connection is terminated dynamically as well

5.2 Further features 10.70

Protection of minors according to official regulations

With LCOS 10.70 RC1, you can now maximize the protection of underage end users, e.g. in schools or youth facilities. For example, the official website list of the “Bundesprüfstelle für jugendgefährdende Medien” (German Federal Review Board, BPjM) is now also part of the LANCOM Content Filter Option or available separately via the software extension LANCOM BPjM Filter Option (as of LCOS 10.70 Rel). This means that domains whose content is officially classified as harmful are not accessible to the relevant target group in Germany. Continuous updates and extensions of this list are guaranteed.

Two-factor authentication – double security for your VPN

Whenever a high level of security for your sensitive data is required or, for example, compliance guidelines in your company demand it, double protection of network access via your LANCOM Advanced VPN Client is ideal. Thanks to two-factor authentication (IKEv2 EAP-OTP), you can now protect VPN access and thus also your network from unauthorized access. You can specify that users can only log in via the LANCOM Advanced VPN Client if they use two-factor authentication when logging in. In this case, the VPN password is supplemented by a time-based one-time password, which can be generated in an authentication app (e.g. Google Authenticator) on the cell phone. This feature can be used with all devices that have at least 25 VPN tunnels (either already integrated or upgraded with LANCOM VPN Option).

You can find further features within the individual builds sections in chapter 6 “History LCOS 10.70”.

6. History LCOS 10.70

LCOS improvements 10.70.0181 RU2

New features

→ Support for G.722 DTMF in the Voice Call Manager

→ Support for vRouter redundancy in Amazon AWS. In the failover case, the vRouter can change the AWS routing table via API call to switch between primary and backup vRouter.

→ RADIUS forwarder: the realm can be removed from the username during RADIUS forwarding

→ Support for new temperature sensor hardware on LANCOM devices:

- 1640E
- 1790EF
- 1790VA
- 1790VA-4G+
- 1790VAW

Bug fixes / improvements

General

→ After a WWAN network scan, the number 12 was displayed in the '/Status/Modem-Mobile/' table instead of the value '5G'.

→ The TR069 protocol did not work over arbitrary cellular Internet connections.

→ On some LANCOM devices with built-in cellular modem of type 'Sierra MC7455' (e.g. LANCOM 179xVA-4G, 1906VA-4G) the modem firmware update supplied with LCOS 10.70 REL could not be loaded.

→ With DSL sync in place, the ATM interface was not started on a LANCOM router of the 1926VAG series. This meant that no ADSL connection could be established.

→ If two Internet connections were configured on a router, each with an IP address from the same address range, and these were connected to the same upstream switch, the router responded to an ARP request from the upstream gateway via both Internet connections. The same MAC address was then assigned to both Internet connections in the router's ARP table. This meant that only one of the two Internet connections was still functional.

VoIP

→ In a scenario with a Swyx PBX and a CTI+ subscriber, the Voice Call Manager sent a Re-INVITE to the CTI+ subscriber when the call was forwarded to a cellular subscriber (VoLTE). The subsequent “SIP 200 OK” of the CTI+ subscriber contained a new record route header, which the Voice Call Manager adopted in the subsequent “ACK” instead of adopting the previous header. This resulted in the call being terminated by the SIP provider.

→ If the Voice Call Manager received a route header in the Provisional Response “181 Call is being forwarded” during call forwarding, this was not sent by the Voice Call Manager in the subsequent PRACK to the SIP provider. This resulted in the SIP provider terminating the call with the message “481 Call Leg/ Transaction Does Not Exist”.

LCOS improvements 10.70.0087 RU1

Bug fixes / improvements

General

→ LANCOM devices managed by the LANCOM Management Cloud (LMC) could experience irregular reboots with LCOS 10.70 REL due to a timing issue during TLS transmission between the LMC client of the LANCOM device and the LMC.

LCOS improvements 10.70.0086 Rel

New features

→ Support for Wi-Fi 6E and three radio modules in the WLC

→ The ‘loadfirmware’ command on the CLI has been extended with the switch ‘-e’, where the firmware is first downloaded, temporarily cached in flash and then installed.

→ The DECT frequency band and admin password can be provisioned for a DECT base station.

→ The device name is no longer displayed during WEBconfig access via WAN connections.

→ The Telnet(-SSL) banner is now only displayed after a login.

Bug fixes / improvements

VPN

→ With this release, VPN rules for creating network relationships (SAs) in the IPv4 firewall are no longer supported and replaced by the ‘Network Rules’ configuration option in the VPN menu.

Wi-Fi

→ A logical Wi-Fi network in a WLC scenario was still displayed in LANmonitor after removing it from the WLC configuration.

VoIP

→ If the router acted as SBC in a scenario with connected SIP PBX and received an incoming call where an update with a refresh was sent by both the SIP PBX and the provider after 15 minutes (session expires: 1800), the router used a new branch ID in the “200 OK” received from the provider when forwarding to the SIP PBX in the via header. This was not known to the SIP PBX and was therefore discarded. This resulted in the SIP PBX terminating the call after 15 minutes.
Furthermore, the router used the information from the last UPDATE packet instead of the INVITE (separate call) in the route header and in the request Uri. This caused the call to be terminated by the provider after 45 minutes with the message “481 Call Leg/Transaction Does Not Exist”.

LCOS improvements 10.70.0061 RC2

New features

→ Support for two-factor authentication (IKEv2 EAP-OTP) together with the LANCOM Advanced VPN Client.

Bug fixes / improvements

General

→ In the syslog of the LANCOM 1900 series cellular routers with dual SIM, the status of slot 1 was always used as the status for SIM card slot 2.

VoIP

→ If in a SIP line for the ‘Signaling Encryption’ the option ‘Automatic’ was used and at the same time an IP address was stored as ‘SIP Domain/Realm’, the SIP registration could not take place. In such a case UDP is now used as fallback.

LCOS improvements 10.70.0041 RC1

New features

→ Support for ETM-(Encrypt-Then-Mac)-SHA algorithms and sntrup761×25519-sha512 in SSH

→ When using administrative distances and line polling, separate routes with routing tags are no longer needed to prevent IDS messages.

→ In 802.1X, the RADIUS attribute ‘Chargeable User Identity’ according to RFC 4372 is supported.

→ The DHCPv4 client now supports the RFC 4361 client ID format.

→ Support for a stateless DHCPv4 relay function

→ The algorithm selection for TLS and SSH was adjusted to current methods after a device reset.

→ Support for the PRE64 option according to RFC 8781 in router advertisements and for the prefix discovery at 464XLAT

→ A graphical illustration for DSL connections has been added to the WEBconfig dashboard.

→ The DSL line code for the LANCOM 1926 series has been updated.

→ Support of a Wi-Fi scan function for the LMC

→ More providers have been added to the Auto VLAN provider table.

→ Support for ‘Naming Authority Pointer Resource Records’ (NAPTR) in the Voice Call Manager, this is the new default (automatic) value of the signaling encryption of a SIP line.

→ Support for ‚IPv6 Neighbor Discovery Proxy‘

→ The entries in the IPv6 routing table are now switchable.

→ In the IPv6 address table, addresses can now also be generated from the RA prefix or DHCPv6-PD prefix.

→ The ‘IPv6 Neighbor Discovery Cache Limit’ can be configured.

→ There is now a forwarding rule for delegated prefixes in the IPv6 firewall.

→ A comment field has been added to the action table.

→ A zero-touch rollout with the LMC is now additionally possible for routers via a LAN interface by default.

→ IKEv2 routing is now also supported in classic site-2-site mode and no longer only in CFG mode. This means that routes are automatically transmitted to the central site during tunnel establishment without the need for routes to be present in the routing table at the central site, for example.

→ In the IKEv2 default configuration, the DH groups have been raised or higher-level groups have been added to the list of allowed groups.

→ Support of ‘BGP Large Communities’ according to RFC 8092

→ Support for ‘BGP Resource Public Key Infrastructure (RPKI) to Router Protocol (RTR)’.
→ Support for ‘ BGP Administrative Shutdown Communication’ according to RFC 8203
→ Support for ‚BGP Graceful Shutdown‘
→ Support for ‚BGP Extended Messages‘ according to RFC 8654
→ BGP Show RIB commands on the CLI: ‘show bgp-v4-rib’ or ‘show bgp-v6-rib’.

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.