Release Notes

LCOS
10.72 RU5

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 10.72 RU5, 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 10.72

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 10.72:

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

4. Advices regarding LCOS 10.72

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.

Omission of VPN rules in the IPv4 firewall

As of LCOS 10.70, VPN rules for generating network relationships (SAs) are no longer supported in the IPv4 firewall and are replaced by the 'Network rules' configuration option in the VPN menu.
This mainly concerns scenarios with IKEv1 connections.

For more details see:
https://support.lancom-systems.com/knowledge/pages/viewpage.action?pageId=85885727

5. Feature overview LCOS 10.72

5.1 Feature highlights 10.72

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 10.72

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 10.72”.

6. History LCOS 10.72

LCOS improvements 10.72.0385 RU5

Bug fixes / improvements

General

→ On a LANCOM 1793VA-4G, the SIM card remained offline when the router was without power or a cold boot was performed via the command line.

→ A newly added ‘Virtual Link’ was not automatically detected with OSPF enabled. OSPF had to be globally deactivated and reactivated for this.

→ Running a script with the ‘beginscript’ & ‘exit’ commands sporadically caused existing BGP connections to be disconnected.

→ After an undefined time (possibly several weeks), the WWAN module switched itself off and was then in ‘Disabled’ status. As a result, an Internet connection was disconnected.

→ With cellular routers, it could happen that an error was displayed in the connection information of the cellular connection (Status/Modem-Mobile/Connect-Info), although the connection was established.

→ If a SFP-GPON-1 module with activated ‘Dying Gasp’ function was plugged into the LANCOM router, no automatic configuration change with subsequent restart of the module took place. As a result, the PON management connection did not start and remained in the ‘Opening management connection’ state.

→ On some LANCOM routers the OID 1.2.20.10 was missing in the configuration (path ‘Setup/LAN-Bridge/Protocol-Table’ in the CLI / menu ‘Interfaces / LAN / LAN-Bridge / Protocols’ in LANconfig & LMC).

→ LANCOM cellular routers could fail to re-initialize the USB module, resulting in an immediate reboot of the router.

→ If an incorrect APN was entered on a mobile router with a 5G module, this led to an immediate reboot of the router after a few minutes.

→ In individual cases, an 802.1X authentication of users with the ‘Framed-IP-Address’ attribute could result in an immediate restart of the router.

→ If several hundred or thousand messages were sent in the DNS in a short time, it could happen that this occupied more memory than was originally reserved for it. This led to an immediate restart of the router.

→ When using the 802.1X authenticator on a LAN port, the router learned the MAC address of a connected device even though it was not authenticated. This allowed communication with the connected device.
MAC addresses are now no longer learned automatically when using the 802.1X authenticator, thus preventing communication.

→ The TR-069 service sent its requests with the IP address instead of the DNS name of the ACS server. This caused the TLS connection to be terminated on a strictly configured ACS server with SNI because the URI and the name in the certificate did not match.

VPN

→ If a LANCOM router received an 'INVALID_SPI notification' from another router, the LANCOM router deleted the child SA of the associated IKEv2 connection. It could happen that the memory of the deleted child SA was occupied twice. This led to an immediate reboot of the router.

WLAN

→ In a 'Config Sync' scenario, the slave WLC restarted abruptly when four or more entries were written to a status table about errors in the configuration.

→ If a LANCOM access point was managed via LMC and there was an SSID with 802.1X (RADIUS) authentication to a RADIUS server with a name longer than 15 characters, it could happen that an incorrect RADIUS server was addressed. The reason for this was that there was no check in the LMC for the length of the RADIUS profile name and the LCOS only used names with a maximum of 15 characters.

VoIP

→ When DNS resolving SRV records via NAPTR, the output of the console command 'show vcm dns' always showed one SRV record more than was actually resolved.

→ In a SIP trunk scenario with gateway line to a SIP PBX, if the router received a 'RE-INVITE' from the SIP provider on the SIP trunk with 'refresher' in the 'Session-Expires' header (in this case 'refresher=uas'), the Voice Call Manager changed the 'refresher' in the "200 OK" to the SIP provider (to 'refresher=uac'), which is not allowed. This caused the call to be disconnected by the SIP provider.

LCOS improvements 10.72.0291 RU4

Bug fixes / improvements

General

→ After activating a VPN-25 option on a router (no reboot required), the device certificate could not be downloaded in WEBconfig via the ‘Download current CA certificate’ option when the CA was activated. The process was acknowledged with the error message ‘Not Found’. The download of the certificate was only possible after a restart.

→ On a serial device connection, an active session was not disconnected when using the ‘passwd -n’ command in a script.

→ The value specification for memory usage was incorrectly output on the display page for LANCOM devices with LCOS.

→ After a change of the LMC parameters by the LMC (Setup/LMC), the previous HTTPS session was still used. If the parameters were incorrect, this meant that the device could no longer reach the LMC after a restart.
The HTTPS session is now rebuilt after the LMC parameters are changed.
If the device can no longer reach the LMC with the changed parameters, a rollback to the previous parameters takes place.

→ Usually, Internet providers distribute the parameters of an IPv6 connection by initially sending a router advertisement. If an Internet provider instead initially sent the IPv6 parameters via DHCPv6 and only after a longer time sent a router advertisement with the gateway, the gateway was not displayed in the ‘Status/WAN/IP-Addresses/IPv6’ table.
After a change of the gateway, this is now taken over into the table.

→ When calling an SNMP path in the MIB-2, the information about the SFP port was read out twice in routers of the 1900 series and the memory was not released again. This meant that if the SNMP path was read out repeatedly over a longer period of time, no more free memory was available. This led to an immediate restart of the router.

→ If more than one MAC address was detected on a port when using the ‘802.1X Authenticator for ETH ports’, this caused the port to be shut down and thus no more communication was possible via this port.

→ In the console path ‘Setup/LAN/IEEE802.1X/Authenticator-Ifc-Setup’ there is now the option ‘Single-Host-Violation-Block’. If this is set to ‘No’, only the first authenticated device can communicate via the port. Traffic from other connected devices is then blocked.
If the command ‘Default’ was executed in the console path ‘Setup/COM-Ports/WAN/Devices’ on a 1900 series router with 5G module, the table was subsequently empty. This implicitly set the ‘Operating’ mode to ‘No’ for the 5G module, so the 5G module was disabled.
If a device is not present in the ‘Setup/COM-Ports/WAN/Devices’ table, the ‘Operating’ mode is now set to ‘Yes’.

→ If a LANCOM router received an idle time window for a firmware update from the Auto Configuration Server (ACS) via TR-069 (‘when idle’ mode), the update was not performed after the idle time window ended.

→ If telephony was also configured via TR-069 when the configuration was obtained from an Auto Configuration Server (ACS) of Telekom, the router always entered the URL ‘tel.t-online.de’ for the registrar, even if this was not transmitted by the ACS.

→ EAPoL frames can now be transmitted via mulicast if the corresponding option is enabled in the menu ‘Setup/LAN/IEEE802.1x/Authenticator/IFC-Setup’. In multi-host mode, this allows identity requests for RADIUS authentication of a LANCOM access point to be sent via multicast instead of unicast.

→ In the configuration of a LANCOM router it was possible to use a logical WAN interface (e.g. DSL-1) for several physical interfaces (e.g. SFP port and ETH port). In this case, problems could occur with (PPPoE) dial-up to WAN connections.

Wi-Fi

→ UDP traffic could also be transmitted without logging into the Public Spot, allowing some applications to communicate with their servers on the Internet.

VoIP

→ Since the LANCOM router did not support the ‘UNENCRYPTED_SRTCP’ parameter, calls were terminated by the provider after a few seconds because the unencrypted RTCP packets from the SIP client could not be passed through to the SIP provider.

→ If the LANCOM router was used as a session border controller (SBC) with an upstream PBX on a CompanyFlex connection, the DTMF in-band transmission did not work on an encrypted connection.

LCOS improvements 10.72.0203 RU3

Bug fixes / improvements

General

→ When forwarding to an external RADIUS server, the specified IP address was entered in reverse order in the configuration on a LANCOM 1800EFW.

→ If the feature activation is initiated via console and the license server is not accessible, the activation remains in the ‘processing’ state. If the feature activation was subsequently initiated again via console, this led to an immediate reboot of the device.

→ When an OSPF configuration was saved and route redistribution was added in a second step, the LANCOM router did not announce itself as an ASBR (Autonomous System Boundary Router).

→ OSPF interface costs were presented with incorrect values due to incorrect internal processing.

→ The data volume budget counter did not take into account data transmitted over IPSec connections.

→ Due to a problem with the initialization of the WWAN module, it could happen that an existing WWAN connection was no longer established on LANCOM cellular routers after a firmware update.

→ In the WEBconfig dashboard, the HTTPS port was displayed with ‘1’ instead of ‘443’ in the services overview for web services.

→ If in the OSPF configuration of a LANCOM router the value ‘Advertise-Default-Route’ was set to ‘Dynamic’, announcing the default route did not work, although the route was present in the FIB.

→ The DHCPv6 client ID was specified with the value ‘0’ instead of the respective MAC address for WWAN interfaces.

→ If a RADIUS server was used for authentication on a LANCOM router and this authentication did not work, the fallback to local authentication failed (login stopped) and the router performed an unmediated reboot after a few minutes.

→ If the SIM card was changed on a mobile router with a 5G module during operation, this led to an unmediated restart.

→ If no DNS server was stored when DNS forwarding was activated, the router did not report this to the requesting network subscriber.
In such a case, the router now sends the “server failure” message to the requesting network node.

→ If port forwarding is also to be possible for the connection with the higher value (backup connection) when using the ‘Administrative distance’ function, another routing entry must be created for this (dummy route). This dummy route was not taken into account during port forwarding, so packets could not be forwarded via the backup connection.

VPN

→ If an IKEv2 VPN connection was configured to AES-GCM, incoming fragmented ESP packets were dropped with an error message.

→ In individual cases, it could happen that the ‘Security Associations’ of a VPN connection were not terminated when switching to a backup connection. As a result, the VPN connection could no longer be established. In such a case, the message “VPN: local reconnect lock active” was displayed in a VPN status trace.

→ When using an IKEv2 connection via RAS Config Mode between two LANCOM routers with activated IPv4 routing, the stored networks were transmitted twice. In this case, a VPN status trace displayed the message “IKEv2 routes have already been exchanged”. This resulted in errors on the VPN connection.

Wi-Fi

→ A managed access point did not use the VLAN ID entered in the SSID in the WLAN controller, but always the VLAN ID available in its local configuration in the group key index. This meant that broadcasts and multicasts could not be decrypted and thus could not be transmitted.

VoIP

→ If, after resolving the ‘SRV Resource Record’, the Voice Call Manager determined that it was not connected to the SIP server with the highest priority, it initiated a switch to the highest priority server. To do this, the Voice Call Manager sent an Un-Register to the previous SIP server to disconnect it. If the unregister was not answered by the previous SIP server, the Voice Call Manager did not switch to the correct SIP server.

→ If the router received a Re-INVITE from the SIP provider with SDP parameters that the Voice Call Manager could not process, it sent the message “500 Server Internal Error” instead of the message “488 Not Acceptable Here”. This caused the SIP provider to terminate the call.
If the primary SIP server fails, a switch to a SIP server with low priority takes place. In this case, a switch back to the primary SIP server should only occur after 15 minutes.

Until now, the Voice Call Manager checked at each SRV resolution whether the SIP server with the highest priority was used and initiated a switch if necessary.
Furthermore, it could happen that the check of the used SIP server was already performed during the initialization if the IP addresses of the SIP servers were not yet transmitted.

→ If a SIP phone registered on the router performed call forwarding for an incoming call and directly sent a REFER followed by a re-INVITE instead of parking the call (hold), this resulted in two INVITE packets being sent by the SIP phone for the same call ID. The phone call was then disconnected by the provider, so that call forwarding was not possible.
In such a case, the Voice Call Manager now waives authentication for the re-INVITE of the SIP phone and sends this directly to the forwarding destination. The “SIP 200 OK” from the forwarding destination is then forwarded to the SIP phone, so that the double INVITE is avoided.

→ If in a scenario with an ISDN PBX a call forwarding via FACILITY message and call re-routing was successful, the source number was not taken over if the Voice Call Manager did not use SIP302 or the SIP provider did not support SIP302.

→ For an incoming call to an analog or ISDN phone, the Voice Call Manager only considered the original SDP Offer instead of the SDP Answer when selecting the codec for the RTP traffic. This could result in an incorrect codec being selected. In such a case, no voice transmission was possible and the call was terminated after a short time.
The Voice Call Manager now always uses the PCMA codec if it is offered in the SDP Offer.

→ If an outgoing telephone call was initiated by digit dialing in a scenario with an ISDN PBX, the telephone number was not transmitted completely if the individual digits were transmitted too slowly by the ISDN PBX. As a result, the telephone call could not be established.
The Voice Call Manager now uses a ‘Short Overlap Timer’ of 500 instead of 250 ms.

LCOS improvements 10.72.0092 SU2

Bug fixes / improvements

General

→ Security improvements due to an update of the OpenSSL version to 1.1.1t (CVE-2023-0286, CVE-2022-4304, CVE-2023-0215 and CVE-2022-4450).

LCOS improvements 10.72.0091 RU1

New features

→ With the DHCPv6 Relay Agent, up to 4 destinations can now be configured for forwarding to external servers.

→ The DHCPv6 Relay Agent supports a sending address towards the DHCPv6 server.

→ The BPJM module now has a CLI function to delete the current signature definition.

→ „Connection Refused“ messages are now displayed in the syslog with level ‚Info‘ instead of „Alarm“. This means that these messages are no longer displayed in the WEBconfig syslog by default. The behavior can be adjusted by a configuration change.

Note:

As of the next LCOS major version, the ‘Tx-normal’, ‘Tx-reliable’ and ‘Tx-urgent’ columns of the ‘Status/WAN/Packet-Transport’ status table are removed and no longer supported. The status table ‘Status/IP-Router/Protocol-Table’ is also omitted there. The last supported version is LCOS 10.7x.

Bug fixes / improvements

General

→ The BPJM feature could be configured even if there was no license for this option.

→ The WEBconfig setup wizard for setting up an IPv6 Internet connection wrote the comment field in the ‘Router’ column of the IPv6 routing table. As a result, the configured IPv6 connection was not functional.

→ If data was temporarily not transmitted via Deutsche Telekom's 4G / 5G Internet connection, it could happen that the WWAN Internet network connection was no longer functional after data transmission was resumed.

→ As soon as a new configuration was imported into a LANCOM 1900EF-5G via script, the WWAN modem remained in the 'Device Removal/Deactivated' state. The WWAN modem could only be put back into active mode by restarting the device.

→ If the password of an encrypted configuration backup contained a '+' character, the encrypted configuration backup could no longer be decrypted and transferred to the LANCOM device.

→ With an active backup via WWAN it could happen that after some time the routing between LAN and WAN did not work anymore and could only be restored by disconnecting the WWAN connection.

→ If a network subscriber in the router's local network repeats a DNS query too quickly, a second DNS query with the same source port is sent to the backup DNS server. After receiving the response from one of the two DNS servers, the port is closed. If the router subsequently also receives the response from the second DNS server, it is rejected.
This caused the "connection refused" message to be recorded in the syslog (priority 'Alarm'). This behavior could cause a lot of false positive messages to be recorded in the syslog. The priority of the "connection refused" message has now been changed to 'Info' so that it is not recorded in the syslog in the default configuration.

→ In individual cases it could happen that the DHCP server on a router in factory state (setting 'Automatic') did not start and thus could not distribute IP addresses.

→ If the router received a broadcast for a certain network on the interface of another network, this led to an immediate reboot of the router if a rule with the received broadcast address as destination was created in the firewall.

→ When using ICMP polling for an Internet connection, an unmediated reboot of the router occurred if an ARP request from the polling destination was answered before the Internet connection was established.

→ If multiple IP addresses were resolved in a DNS request from the LMC client, the device always used the 'smallest' IP address for communication via TCP instead of performing load balancing across multiple IP addresses. This behavior also affected other applications.
Now a random IP address is always used.

VoIP

→ If analog or ISDN devices were connected to the router, the Voice Call Manager always sent the codecs PCMA (G.711-a) and PCMU (G.711-u) in the ‘SDP Answer’ as soon as one of the two codecs was included in the ‘SDP Offer’.

Now all codecs except PCMA and PCMU are deleted from the ‘SDP Offer’ and the first codec is taken over into the ‘SDP Answer’. If PCMU is used, the Voice Call Manager transcodes this to PCMA, since ISDN and analog devices only support PCMA. If there is no ‘SDP Offer’ in the INVITE, the Voice Call Manager answers with PCMA and PCMU in the ‘SDP Answer’.

→ If the option ‘Automatic’ was selected for ‘Signaling encryption’ in a SIP line (NAPTR active), it could happen that the re-registration did not work and a new registration had to be performed. As a result, telephony no longer functioned during this period.

→ If a router with Voice Call Manager is used upstream of a SIP-TK interface, it acts as a session border controller (SBC). In such a scenario, when an incoming call from a mobile subscriber (VoLTE) was directly transferred via the ‘Connect without consultation’ (Blind Call Transfer) function, the Voice Call Manager did not negotiate the codec correctly with a specific SIP provider remote station. This resulted in the call being disconnected.

→ If a SIP provider used DNS SRV records with the same priority, the Voice Call Manager switched between these servers each time the DNS resolution was repeated. This resulted in a short interruption of the registration.

LCOS improvements 10.72.0015 Rel

New features

→ Support for Q-in-Q VLAN on WAN interfaces
→ Support of a sender address for the update process of the signature file at the BPJM filter
→ Master holddown time switch in VRRP
→ Support for RADSEC certificates in the SCEP client
→ In WEBConfig, there is a link to the Wi-Fi station table in the dashboard under Wi-Fi.
→ A LANCOM WLC supports the selection of the LANCOM LX-6500 in the firmware management.
→ Support for LANCOM ARC 2.0 together with the LMC

Bug fixes / improvements

General

→ Although no Content Filter option was active on a router, the 'Content Filter' menu was displayed in WEBconfig. However, the configuration dialogs were empty.
→ In WEBconfig, the configuration settings for the time server adjustment method were missing in the 'Date/Time / Synchronization' menu.
→ In the WEBconfig menu 'Setup Wizard / Manage Public Spot Users', users were displayed as 'unauthenticated' although they were successfully connected to the Public Spot.
→ In a WWAN connection where the address reference was configured via DHCP, the LANCOM DHCP client sent ARP requests, although these were not required for the WWAN connection.
→ The DNS servers stored in the 'IPv4 / Addresses' menu are bound to the LAN interface. If the local IP address of the router was stored as DNS server in this menu and a default route was created which pointed to the IP address of an upstream router in the same IP address range, this led to an immediate restart of the router.

Wi-Fi

→ If another user was to be added when the RADIUS user table was full, a page with JavaScript code was displayed instead of an error message.
→ In LCOS 10.70 it could happen that an incorrect reference to the MAC address of the connected Wi-Fi device was stored in the address table of the WLC tunnel used. As a result, communication via the WLC tunnel no longer worked.

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, LANCOM Systems, LCOS, LANcommunity and Hyper Integration are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. This document contains statements relating to future products and their attributes. LANCOM Systems reserves the right to change these without notice. No liability for technical errors and/or omissions. 09/23