Release Notes

LCOS
10.80 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 10.80 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 10.80

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 10.80

→ LANCOM LN-1700
→ LANCOM LN-1702
→ LANCOM LN-830acn
→ LANCOM L-822acn
→ WLC-4006+

4. Advices regarding LCOS 10.80

Important notes on extending the input length of the main device password
As of LCOS 10.80, the input option for the number of possible characters for the main device password and the other administrators has been extended from 16 to 128 characters. If more than 16 characters are used in LCOS 10.80, a downgrade to versions lower than 10.80 is no longer possible or supported. It is no longer possible to log on to a device after the downgrade.
Special attention must be paid to the WLC with managed access points in the case of password synchronization. If the longer password is used on the WLC, all managed access points must also be operated with LCOS 10.80. In this case, local logon is no longer possible on APs with LCOS lower than 10.80.
The above instructions apply only in case the new option of more than 16 characters is used for the password.

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 10.80

5.1 Feature highlights 10.80

Let's Encrypt for WEBconfig and the LANCOM Public Spot

Let's Encrypt is a certificate authority that offers free HTTPS certificates to standardize encrypted connections. WEBconfig and also the LANCOM Public Spot now support Let's Encrypt. This means that free and trusted certificates can be created, integrated via the gateway, and automatically renewed with just a few one-time and simple steps.

5.2 Further features 10.80

Zero-touch rollout for cellular routers

With the support of Zero-touch, the setup of LANCOM cellular routers is now even easier and faster. Where previously manual configuration of the cellular access point was required, it is now sufficient to insert a PIN-free SIM card into the device. Zero-touch rollout enables an automatic connection to the Internet and subsequently to the LANCOM Management Cloud to retrieve the appropriate configuration of the gateway.

LANCOM vRouter available via Google Cloud

With LCOS 10.80, you can now operate the LANCOM vRouter on demand with the cloud computing provider Google Cloud. This means that in addition to Microsoft Azure, VMware ESXi, Hyper-V, and AWS, you can now also use Google Cloud to move your own infrastructure to the cloud. The LANCOM vRouter guarantees a secure connection and handles encrypted communication between your site and your virtualized infrastructure in the Google Cloud. Furthermore, the virtualization of headquarters is also possible: the vRouter in the Google Cloud simply replaces the central hardware gateway.

WEBconfig in new corporate design

If you manage your devices via the web browser, LANCOM provides you with a graphical user interface via WEBconfig, which is directly integrated into LCOS and from now on shines with a new coat of paint in a modern design and maximum clarity.

You can find further features within the individual builds sections in chapter 6 "History LCOS 10.80".

6. History LCOS 10.80

LCOS improvements 10.80.0345 RU2

New features

→ The ping command can be executed via WEBconfig under ‘Extras / Execute ping’.

→ The Internet setup wizard for mobile radio has been expanded to include providers from France, the USA and the Netherlands.

→ The broadcast bit for the DHCP client can now be switched. To do this, there is the parameter ‘B-DHCP’ in the selection for layer 3 in the WAN layer table on the console or in the LCOS menu tree.

→ Adjustments to the QinQ VLAN on the WAN: The scenario is now supported that both Ethernet types (e.g. 0×8100) are identical, but only one tag is included, or is ‘0’.

→ Additional status parameters for mobile radio are supported in the TR-069 data model TR-181.

→ Support for displaying the WWAN firmware version in the LMC.

→ With the LANCOM ISG-8000, parameters such as backlighting for the device display can be configured on the console.

→ The interface or WAN connection used for SIP registration is now also displayed in the VCM status table ‘Line’.

Bug fixes

General

→ With a high volume of IPSec data, enqueue errors could occur if packets were to be added to a queue that had already been released. In individual cases, this could lead to an immediate restart of the router in connection with further encrypted data traffic (e.g. HTTPS).

→ The vRouter only supports one CPU core. However, it could happen that the vRouter assigned jobs to several virtual CPU cores, which then led to an immediate restart.

→ A security vulnerability in the SSH protocol has been fixed (‘Terrapin’ security vulnerability/CVE-2023-48795).

→ In a scenario with config sync, it could happen that no synchronization of the configurations was carried out due to a failed TLS handshake.

→ With a TACACS+ login, it was not possible to use user names with more than 16 characters. User names can now contain up to 32 characters.

→ In a VRRP scenario in which ICMP line polling was used for a remote station, it could happen that a switch back from the backup device to the master device failed.
→ After disconnecting from the Internet, it could happen that the MAC address of the router was used instead of the stored user-defined MAC address.
→ The ‘Layer 7 application detection’ could not resolve packets with QUIC, as a result of which the corresponding data traffic was not listed in the statistics.
→ When using the Safari browser under iOS / macOS, the configuration could not be saved via WEBconfig.
→ In a scenario with DPS (Dynamic Path Selection), switching the session to a better line (passive switchover for DPS) for UDP packets did not work on central devices.
→ On 5G routers with an IPv6-only mobile connection, an IPv4 context is set up in addition to the IPv6 context. The IPv4 context reports a ‘link down’ after two minutes due to inactivity. This incorrectly led to the entire mobile connection being terminated.
→ When using the test mode (flash no), it could happen in individual cases that the complete device configuration was deleted after writing a configuration.

VPN

→ The ICMP polling function used an incorrect routing tag during the polling process, which could cause the connection setup to fail for IKEv2 connections for which a routing tag was specified in the routing table.
→ In individual cases, the router could restart unexpectedly if a large number of VPN operations were carried out in quick succession.

Wi-Fi

→ After an update to LCOS 10.80, PoE negotiation via LLDP no longer worked. As a result, access points that require PoE according to 802.3at for full functionality were only supplied with PoE according to 802.3af. This limited the functionality of the access points.
→ When using the Public Spot mode ‘Login data is sent via SMS’, no country code could be selected on the landing page.

VoIP

→ If the Voice Call Manager routed an incoming call to an internal user with multiple registrations (SIP user with multiple SIP registrations or ISDN user with activated parallel call), who forwarded the call to another subscriber, the Voice Call Manager did not send a source phone number. As a result, the phone number of the original caller was not sent to the other subscriber.

→ The Voice Call Manager does not support RTP extensions. If the Voice Call Manager received an incoming call with RTP extensions, it also sent the RTP extensions in the ‘SDP Answer’. This meant that the called party could not hear the caller.
The Voice Call Manager no longer sends RTP extensions in the ‘SDP Answer’.

→ If the encryption function was activated in the settings of a SIP line, an IPv6 registration with the registrar forced in the ‘SIP domain/realm’ field with the suffix ‘?6’ did not work.

→ During a call via the Voice Call Manager, it could happen that reserved memory was overwritten. This led to an immediate restart of the router.

→ If the Voice Call Manager in INVITE received two alternative media streams (m=audio) with different ports from the SIP provider, the router only responded with one media stream in the “200 OK” to the provider. This resulted in the call being terminated by the SIP provider.

→ In a scenario with a connected SIP PBX, the Voice Call Manager incorrectly sent a CANCEL to the SIP PBX after forwarding an incoming call to an external subscriber via SIP302.

LCOS improvements 10.80.0233 RU1

New features

→ Support of Zero Touch commissioning for the LANCOM 1800 Blackline series and LANCOM 1900 series on the WAN Ethernet port. For this purpose, the device must be delivered with LCOS 10.80 RU1 or higher or a reset must be performed after the update to LCOS 10.80 RU1.

→ The operating mode for the rollout agent is now ‘Off’ by default.

→ If a connection is terminated, extended information is now displayed in the syslog for WWAN.

→ When displaying tables with many entries in WEBconfig, the entries are now displayed on several pages by pagination.

Bug fixes

General

→ Using WEBconfig, a maximum value of 2147483647 could be entered in the ‘Remote AS’ field in the ‘Configuration / Routing protocols / BGP / Neighbors’ menu, although higher values were also possible via the console and LANconfig.

→ If several ARF networks were configured on a router with the same IP address (separated by VLAN), a configuration change in the ARF networks triggered ‘gratuitous ARP flooding’ in each network. In scenarios with a large number of identical ARF networks, this could lead to severe packet loss and also to an immediate restart of the router.
After changing the configuration of the ARF networks, only one ‘gratuitous ARP’ is now sent for each network.

→ If there were a large number of routing entries on a router (e.g. learned via BGP) and all interfaces were read out by a monitoring tool via SNMP (SNMP path 1.3.6.1.2.1.4.24.4, RFC 2096), the router’s CPU was fully utilized. The router was then restarted immediately.

→ The 4G LED of the LANCOM 1800VA-4G was permanently lit blue, even if the cellular module was not active.

→ A faulty BGP base attribute could cause the BGP connection to be terminated (VU#347067).

→ If the remote destination (such as an access point) confirmed several packets with an ACK in an L2TP tunnel to a router, this meant that the sessions on the router were not deleted when the connection was terminated. As a result, the L2TP connections could not be re-established.
→ OpenSSL has been updated to version 3.0.12.

Wi-Fi

→ For access points with a fixed frequency band on a WiFi6 WLAN module, different frequency bands could be selected via WEBconfig.
→ In LCOS 10.80 Rel, the Public Spot templates no longer worked due to changes to the paths for the jquery libraries.
There are now new variables for the jquery libraries and new Public Spot templates. If you want to use your own templates with LCOS from version 10.80 RU1, you must use the new versions.

VPN

→ If the router received an 'Informational request' with a DELETE(CHILD_SA) message followed by a DELETE(IKE_SA) message when an IKEv2 connection was established, this led to an immediate restart of the router.
→ IDS blocked the keepalive packets of a GRE tunnel because the firewall expected at least 2 bytes of user data in GRE packets after the protocol field. As a result, the GRE tunnel was repeatedly taken down.
→ No certificate containers (PKCS12) could be uploaded to one of the VPN certificate slots via WEBconfig. The process was always acknowledged with the messages "Upload failed" and "Incorrect password or invalid file type".

VoIP

→ If the Voice Call Manager received a duplicate 'Connection Information' with different IP addresses during an incoming call in a dialog ("180 Ringing", "183 Session Progress" or "200 OK"), it could happen that the Voice Call Manager sent the answer to the wrong IP address. This led to a one-sided voice transmission.

LCOS improvements 10.80.0155 Rel

New features

→ Support of the re-init function for 5G modules
→ Support for N:N NAT for multicast data packets (not for SSM)
→ Support for WWAN status values RSRP, RSRQ and SINR and display in WEBconfig dashboard
→ Improvement of the hard disk performance of the LANCOM vRouter

Bug fixes

General

→ 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.
→ If an 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.
→ After an undefined time (it could be several weeks), the WWAN module switched itself off and was then in the 'Deactivated' state. As a result, an Internet connection was disconnected.
→ With mobile routers, it could happen that an error was displayed in the connection information of the mobile connection (Status/Modem-Mobile/Connect-Info), although the connection was established.
→ 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.
→ When forwarding to an external RADIUS server, the specified IP address was entered in reverse order in the configuration at the LANCOM 1800EFW.
→ 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 set to active mode by restarting the device.
→ On some LANCOM mobile routers, the built-in WWAN module did not provide a network identifier in text form. As a result, the 'Network' field remained empty after a query (e.g. via CLI with 'ls /Status/Modem-Mobile').

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.

→ 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.

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.

→ 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.

→ The source VLAN check (Setup/Public Spot modules/Check origin VLAN) in the Public Spot only worked for VLANs that were assigned via RADIUS. If the VLAN was assigned via another method (e.g., via circuit ID), the WLAN client was not logged out of the Public Spot and could communicate in other existing Public Spot SSIDs.

→ If a framing error occurred on the serial bus to the ePaper radio module, the connection to the ePaper displays was lost and the displays could no longer be updated. In such a case, the error messages “AccessPoint - An error occurred, need to restart WePaper Access-Point” and “SerialInterface - Error in communication with RF-Module!” were output in the syslog of the access points.

The connection between the ePaper radio module and the ePaper displays is now re-established even without a restart of the access point.

VoIP

→ In a SIP trunk scenario with gateway line to a SIP PBX, when 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.

→ 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 offer as soon as one of the two codecs was contained 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.

LCOS improvements 10.80.0124 RC2

New features

→ The DHCPv4 client supports the MTU option.

Bug fixes

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.

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

→ The IPv6 firewall used a non-existent content filter profile ‘CF-PARENTIAL-CONTROL-PROFILE’ instead of ‘CF-PARENTAL-CONTROL-PROFILE’.

→ Deprecated SSL/TLS default settings were used in the ‘Setup/Mail’ path. The following default values are now used:

- at least TLS 1.2
- no MD5/SHA1
- no 3DES
- exclusively Key Agreement with PFS

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

→ 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.

VoIP

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

LCOS improvements 10.80.0075 RC1

New features

→ Support for Let's Encrypt certificates (ACME client) for WEBconfig and the LANCOM Public Spot
→ Zero-touch rollout for mobile routers together with the LMC
→ WEBconfig in new corporate design
→ Support for Google Cloud (GCP) for the LANCOM vRouter.
→ Support for High Availability Clustering Option L for the LANCOM 1900 series.
→ Routers can record and store traces and Wireshark captures directly on a USB stick.
→ Entries in the action table can be tested or executed by a CLI command.
→ Support for the 'Automatic APN' feature on cellular routers.
→ Access to RPCap and LCOScap via WAN can be configured.
→ The GPON status can be displayed on the WEBconfig dashboard.
→ The GPON password can now also be entered in HEX format (20 characters).
→ Accounting in the router has been reworked and can now also be used to display the throughput of current sessions of stations in the analysis case.
→ Support for configurable responses to incoming SMS messages on cellular routers, e.g. sending reply SMS messages for re-billing when data volume is used up.
→ Support for cold standby on cellular routers
→ The input option for the main device password and additional administrators has been extended to a maximum of 128 characters. When using the new password length, a downgrade to older LCOS versions is no longer possible.
→ The status table 'Protocol-Table' under '/ Status / IP-Router' is omitted.
→ The 'LTE-Delayed-Attach' switch on cellular routers is omitted.
→ The 'Stack Errors' status counter of the IP router is omitted.
→ The 'Establish-Table' status table is omitted.
→ The 'Tx-normal', 'Tx-urgent' and 'Tx-reliable' columns in the '/ Status / WAN / Packet Transport' table are omitted.
→ Support for SSL 3.0 and ciphers with 56 bits or less has been removed.
→ Support for 3G (USB) WWAN modems has been removed completely.
→ WEBconfig certificates generated by LCOS now only have a maximum validity of 365 days.
→ 464XLAT and DS-Lite can be used as backup.
→ Support of the operating switch for SMS

→ Disabling syslog now also disables the regular writing of the syslog backup to the internal flash memory.
→ DHCP and DHCPv6 servers are displayed in WEBconfig under ‘Services’.
→ The ‘(VLAN) Priority Bit’ can be set for WAN connections.
→ Additional DHCP options can be configured on the DHCP client.
→ Additional DHCPv6 options can be configured on the DHCPv6 client.
→ Support for interim accounting in Netflow
→ Netflow now uses 64 bit counters internally.
→ Support for dual stack (IPv4 / IPv6) in Config Mode with IKEv2 against the LANCOM Advanced VPN Client.

Bug fixes / improvements

General

→ For routers with multi-core CPU (e.g. LANCOM 1800 series), only the utilization for CPU core 0 was displayed in the console path ‘Status / Hardware info’. Now the average value of all CPU cores is displayed.
→ 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.

VoIP

→ If the Voice Call Manager received both the P-Asserted-Identity (PAI) and the P-Preferred-Identity (PPI) in an INVITE from a SIP PBX, the Voice Call Manager then used the phone number in the PAI. If this phone number was not known to the SIP provider in a scenario with CompanyFlex connection (e.g. due to a missing digit), the call was disconnected and acknowledged with the error message “403 Forbidden”.
There is now an additional parameter ‘Prefer-Identity-Field’ in the path ‘Setup / Voice-Call-Manager / Users / SIP-Users / Users’. This can be used to select whether the PAI (Prefer-PAI) or the PPI (Prefer-PPI) should be preferred (default setting is PAI as before).

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