Release Notes

LCOS
10.42 SU14

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 10.42 SU14, 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 https://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 10.42

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

4. Advices regarding LCOS 10.42

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 10.42

5.1 Feature highlights LCOS 10.42

Dynamic Path Selection

With the new highlight feature Dynamic Path Selection, you can route mission-critical business applications in your SD-WAN always over the best quality line. The feature continuously monitors your WAN connections in terms of load, packet loss, latency, or jitter and dynamically decides the best route for specific applications depending on the current connection quality. You can flexibly define the performance policies for the WAN connection according to your application. Thus, you benefit from maximum performance and reliability in large-scale SD-WAN infrastructures with several WAN connections in active/active mode.

5.2 Further features LCOS 10.42

Dynamic DNS Service for the Public Cloud

The LANCOM Management Cloud (Public) becomes a DynDNS provider! Simply assign a fixed, self-selected subdomain (mycompany.dyndns-lmc.de) to the gateways implemented there in the sites settings. This subdomain can then be stored in VPN remote stations such as the LANCOM Advanced VPN Client. With the new LCOS 10.42, even gateways with dynamic WAN IP addresses remain accessible at all times via this domain name.

Cloud-managed Hotspot

Create a simple Wi-Fi hotspot with a few clicks – directly from the LMC. No additional gateway or WLAN controller with LANCOM Public Spot Option is required. Intuitive menus provide you with the opportunity to customize your hotspot welcome screen with your logo and corporate colors and integrate important information such as imprint and usage guidelines for your hotspot users. Afterwards you can assign the new hotspot to the respective location and it will be available to your visitors.

Best quality for digital business applications in large-scale SD-WANs

In infrastructures with several WAN connections and business-critical applications, reliable and high-performance connections are essential. With the new LCOS 10.42 feature Dynamic Path Selection, you can now benefit from maximum application performance and fail-safe data communication in your SD-WAN: Thanks to quality-based routing, your data traffic is always steered via the line with the best performance values.

You can find further features within the individual builds sections in chapter 6 “History LCOS 10.42”.

6. History LCOS 10.42

LCOS improvements 10.42.1400 SU14

Bug fixes / improvements

General

→ A security vulnerability in the web interface has been fixed, which allowed unauthenticated attackers to cause an unexpected device restart (DoS attack) by sending a manipulated packet. This affected administrative access via WEBconfig from the LAN and the WAN (if management access via HTTP/HTTPS from the WAN was enabled), as well as the web services IPSec-over-HTTPS, SCEP, OCSP server/responder, and the Public Spot. In the default configuration, access to the router from the WAN is disabled, meaning the router was not affected by this vulnerability in such cases. The TR-069 protocol was also not affected by the vulnerability.

LCOS improvements 10.42.1311 SU13

Bug fixes / improvements

General

→ A security vulnerability in the SSH protocol has been fixed (‘Terrapin’ 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.

VoIP

→ If a SIP user had registered on the LANCOM router without transport parameters, an INVITE was rejected due to the missing parameter and a call could not be established.

→ 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.

LCOS improvements 10.42.1231 RU12

Bug fixes / improvements

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 possible using the console and LANconfig.

→ After the LMC parameters were changed 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 reestablished after the LMC parameters have been changed. If the device can no longer reach the LMC with the changed parameters, a rollback to the previous parameters takes place.

→ 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.

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

→ In scenarios with configured OSPF, it could happen that the OSPF default route was not propagated.

VoIP

→ Due to incorrect information handling in the RTP streams of incoming fax transmissions, it could happen that these were interrupted.

LCOS improvements 10.42.1113 RU11

Bug fixes / improvements

General

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

→ The WWAN module of the LANCOM routers 1790VA-4G, 1790VA-4G+, and 1793VA-4G could be in the ‘disabled’ state. As a result, the routers could not establish a mobile Internet connection.

→ 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).

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

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 an upstream Session Border Controller in the ‘o line’ of the ‘SDP Offer’ sent a value close to the allowed maximum, it could happen that the Voice Call Manager in the ‘o line’ of the ‘SDP Answer’ sent a value which was above the allowed maximum. This resulted in the phone call not going through.

→ 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 using 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.

LCOS improvements 10.42.1037 SU10

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 10.42.1036 RU9

Bug fixes / improvements

General

→ A router with configured connection did not show masking of the WAN peer in backup state (checkable with console commands ‘show ipv4-fib’, ‘ls /status/ip-router/act.-ipv4-routing-table’). This was a display error because masking was enabled for the WAN peer.

→ Due to a DNS cache misbehavior in the cooperation with the LMC client, it could happen that a LANCOM router managed via LMC executed an abrupt reboot after some time after rolling out and activating a configuration.

→ 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.

→ Due to a change in DHCPv6 for DOCSIS-based Vodafone IPv6 Internet connections, it could happen that LANCOM routers could no longer be used on these connections.

→ The HTTP client could not process URLs with relative redirect. This resulted in an immediate reboot of the device during an automatic firmware update when using a URL with relative redirect in the ‘Automatic Firmware Updater’.

→ Neither via console nor in the LCOS menu tree the character ‘/’ could be stored for the parameter OCSP-AIA in the path ‘Setup/Certificates/SCEP-CA/Web-Interface/Profiles’.

→ In a scenario consisting of Internet connection with backup and VPN connection with backup, a fallback to the backup connection occurred after a failure of the Internet connection. This also initiated the establishment of the VPN backup. In individual cases, it could happen that the main VPN connection was established before the VPN backup. In this case, it was indicated that the VPN backup was still active (‘Status/WAN/Backup’ set to ‘Yes’).

→ In the syslog, the cellular provider name and the cell ID / location area codes were repeatedly output, although these should only be output when the data changed.

→ If the interface to the BGP peer was changed in a VRRP stenario (e.g., by changing the Internet connection), the BGP connection remained in the ‘idle’ state and was not re-established.

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

→ During a certificate update, the applicant's CA checks the certificate against the CRL. However, OpenSSL was configured so that this check was only possible for a root CA. This caused the update of a sub-CA via SCEP to fail.

→ Although the Config Sync service to the WAN was disabled in the configuration of a LANCOM router (default setting), the service was shown in the LMC as enabled and with the security status 'critical'.

→ A URL specified in the rollout wizard for a popup was handled incorrectly. Not only the URL parameters were encoded appropriately, but also the parts of the path before.

→ If the DHCPv6 client received a response with multiple identical DHCP options from the DHCPv6 server in response to a 'DHCP renew' (forbidden by RFC 8415), the DHCPv6 client discarded the response packet. This meant that the IPv6 address was not renewed and no communication was possible over this interface until after the DHCPv6 negotiation.
The DHCPv6 client now always uses the first DHCP option and ignores the remaining options.

→ In a TACACS+ scenario, when changing the main device password via the command line, the additional parameter '-n' was not recognized.

VPN

→ If a configuration was loaded as a script into a LANCOM router (*.lcs file) and this did not show any differences in the configuration of established VPN client connections, existing VPN client connections were still disconnected.

→ In rare cases, routing from the LAN to the VPN could stop working when the backup Internet connection over WWAN was active.

Wi-Fi

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

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 forwarding the call to a mobile 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 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”.

→ For outgoing calls it could happen that the LANCOM Voice Call Manager used a DTMF codec number twice in the SDP, which caused the call to be rejected by the provider with the message “488 SDP Parameter Error In SIP Request” and not to go through.

→ When switching to another SIP server (initiated by an eDNS message), the router sent the ‘Deregister’ to the new SIP server instead of the old one. A ‘Deregister’ is now sent to the old SIP server when the priority of the servers has changed or a switch to the highest priority server occurs.

→ If the SIP provider (e.g. Deutsche Glasfaser) transmits the parameter ‘refresher=uas’ (UAS = User Agent Server) in addition to the ‘Session-Expires Header’ (expiration value for the session, e.g. 1860 seconds) in INVITE for an incoming call, the SIP provider expects a session refresh from the router after half of the value in the ‘Session-Expires Header’ (in this example 930 seconds). For this purpose, a ‘Session Refresh Timer’ with a corresponding ‘Expiration Time’ is started on the router.
If the SIP provider sent a re-INVITE with a ‘Session Expires Header’ (e.g. 1860 seconds again) and the parameter ‘refresher=uas’ to the router shortly before the ‘Session Refresh Timer’ on the router expired, the router restarted the ‘Session Refresh Timer’ instead of letting the existing timer expire and renewing the session with the SIP provider. This resulted in the call being terminated by the SIP provider after the original ‘Expiration Time’ had expired.
A ‘Session Refresh Timer’ is now no longer restarted if it is already active, unless the new ‘Expiration Time’ is smaller than the remaining value of the timer. In this case, the new value is applied.

→ The Voice Call Manager checks for an outgoing call whether the SIP user exists locally. This involved going through the PAI, PPI, and FROM fields in the SIP header in the order specified, but only checking the first field with a phone number. If there was a number in the PAI or PPI field but it did not match the configured SIP user, the SIP user could not initiate outgoing calls.
The fields are now all checked in sequence, provided they contain a phone number and the user has not yet been verified.

→ When using a SIP PBX line, incoming calls to a subscriber contained in a call number block (combined in a call route with the wildcard #) resulted in a significantly longer call setup if the called subscriber had only one digit (the wildcard #), since in this case ‘overlap dialing’ was performed.

→ The Voice Call Manager checked its DNS cache every 5 seconds for expired SRV records (TTL=0) and then deleted them. If the response to a DNS query arrived at the Voice Call Manager only after the corresponding SRV record had been deleted, the SIP line was disconnected and the message “generic failure” was output in the syslog.
Expired SRV records are now removed from the DNS cache only after two checks (10 seconds in total). Furthermore, the SIP line is not disconnected as long as the existing connection to the SIP server is working.

→ When using CTI+ on a Netphone PBX, one-way voice transmission could occur in connection with the LANCOM VoIP router because the locally generated RTP headers were not synchronized with the RTP headers that were passed through.

→ When a user connected behind an Octopus Netphone PBX called a vSDP number with call forwarding set up to a VoLTE cell phone with sound logo, only the ‘Caller Ringback Tone (RBT)’ was heard by the caller and not the sound logo.

→ When registering a SIP line, DNS resolution with the highest DNS priority level ‘P-CFCS’ could not be performed.

→ When the Voice Call Manager received a ‘Session Progress’ packet with the tag ‘inactive’ in the ‘P-Early-Media Header’ during an outgoing call, the RTP streams were terminated and not restarted. As a result, no voice communication was possible.

→ In a scenario with a connected SIP PBX, if an ‘UPDATE request’ was received from the SIP provider during the ‘Early Media Phase’ of an outgoing call, the Voice Call Manager forwarded this to the connected SIP PBX, even though this was not possible at this time. The SIP PBX acknowledged this with the error message “500 Internal Server Error”. As a result, no RTP data could be transmitted and no voice communication was possible.
In such a case, the Voice Call Manager now answers the ‘UPDATE request’ with a “200 OK” and sends the SDP information in a ‘Reliable Provisional Response’.

→ If the Voice Call Manager in a scenario with CompanyFlex connection received a SETUP from an ISDN user for an internal call forwarding (AWS) with a second phone number in the ‘Calling Party Number’ field, which was not in the local phone number range, the Voice Call Manager then sent an INVITE with the second phone number as PPI to the provider. This was rejected by the provider with the error message “403 Forbidden”.

LCOS improvements 10.42.0890 RU8

New features

→ Support for new temperature sensor hardware on the LANCOM devices

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

LCOS improvements 10.42.0889 RU7

Bug fixes / improvements

General

→ A vulnerability in the OpenSSL library was fixed (CVE-2022-0778).

→ A vulnerability in the zlib library has been fixed (CVE-2018-25032).

→ If a LANCOM cellular router with an established cellular backup connection did not have a SIM card inserted and was switched to the backup connection, this led to recurring restarts of the cellular module. In isolated cases, this could also lead to sudden restarts of the device due to memory loss.

→ Local interfaces could not be read out via an SNMP walk to the ipAddrTable (.1.3.6.1.2.1.4.20). Instead, only information about the WAN interfaces was output.

→ In the table '/Status/Routing/BGP/Messages', illegible entries were present starting from a different number of entries, which were caused by an incorrect specification of the table size.

→ After reinitializing the WWAN modem on the LANCOM 1790VA-4G+ with the command 'do /status/usb/reinit', the modem was without function. Only a complete reboot of the router restored the functionality of the WWAN modem.

→ Since the SNMP EngineID on LANCOM devices is read out in Enterprise ID format, it was 1 byte too short when queried via an OID, which is why two characters were missing. As a result, the devices reported that they were using the same SNMP EngineID.

→ If an NTP network was entered for the NTP server via console, this did not apply. This resulted in devices in this network not being able to obtain time from this NTP server. The error message "LAN request received, but sender is not in networklist" was displayed in the NTP trace.

→ In LCOS 10.42 the cellular connection history in the path '/Status/Modem-Mobile/History' was extended from 100 to 512 entries. After a firmware update to a corresponding version, the table was not correctly converted to the new size and therefore a table with 100 entries continued to be used. If more than 100 entries were written, this led to an unmediated reboot of the router.

→ If an access point or router with at least two networks was used and the IP address in these networks was obtained via DHCP, it could happen that the HTTP client used the undefined IP address 0.0.0.0 instead of the LMC loopback address to establish the connection to the LMC. This resulted in an IP address from another network being used for the connection to the LMC and the connection to the LMC being terminated again and again.

→ The WEBconfig or TLS device certificate of a LANCOM device operated with LCOS was not automatically extended by the device beyond the expiration date in 2024.
→ An unmediated restart could occur when the router was sending an e-mail.
→ When using OSCP, an expired certificate was still used, even if it had already been renewed via SCEP.
→ If an empty TXT record was received in response to a sent TXT record, the DNS server in the LANCOM router could not process this response. As a result, it discarded the response.
→ On the LANCOM 1790VA-4G+, information about the cellular band in use was not displayed in the status.
→ In a VRRP scenario with individual WAN peers, in which these peers were additionally combined to form a load balancer, it could happen that the VRRP slave attempted to establish the WAN peers every second.
As a result, the CPU load of the device increased and a memory shortage occurred. A pause has now been programmed between the individual connection attempts, which means that the device is no longer pushed to its performance limit.

Wi-Fi

→ When using a WLC tunnel, data packets must have a packet size with a multiple of 8. Depending on the PMTU used, however, it could happen that the WLAN controller sent data packets with a packet size where this was not the case. In conjunction with access points with the LCOS LX operating system, this meant that they were unable to process the corresponding data packets and the packets were therefore discarded.
→ If only the netmask of an IP profile was changed in the configuration of a LANCOM WLAN controller in the menu ‘WLAN controller → AP configuration → IP parameter profiles’, the WLC transmitted this change to managed access points, but the IP configuration of the access points remained unchanged.
→ Via WEBconfig, no wireless client could be added in the LEPS configuration without specifying a passphrase, although specifying a passphrase was optional.
→ When using the LAN bridge on an access point or WLAN router (default setting), the MAC address of the LAN interface was always used for DHCP requests. This meant that access points or WLAN routers connected via a WLAN point-to-point connection or via AutoWDS rejected the DHCP offer and were therefore unable to obtain an IP address.
→ The character ‘ALT+34’ could not be used when assigning a WPA-PSK.

VoIP

→ With a ‘Vodafone Anlagenanschluss Plus’ it could happen with incoming calls that the ‘Hold’ function could not be executed, because no P-Preferred-Identity (PPI) was contained in the RE-INVITE of the Voice Call Manager.

→ Sending an SNMP trap with information about ISDN users could result in an abrupt restart of the router.

→ In a scenario where a Panasonic SIP PBX (SIP-TK KX-NCP500) was connected to a LANCOM router, call forwarding could fail due to faulty SDP communication on the part of the PBX. A workaround has now been implemented in LCOS which intercepts the error and enables communication.

→ If an outgoing call was forwarded from the called subscriber to a third subscriber and the third subscriber offered a DTMF menu for call handling, DTMF communication via key tones no longer worked. As a result, the DTMF menu offered by the third party could not be operated.

LCOS improvements 10.42.0740 RU6

Bug fixes / improvements

General

→ In a BGP community, the value “0” could not be used.

→ Successful admin logins into WEBconfig were recorded in the login table, but the counter for logins remained unchanged.

→ If a firewall rule with ‘conditional transmission’ was passed and no condition in another firewall rule was true, the packet was discarded in the IP router with the error message “Network unreachable (no route) ⇒ Discard” instead of allowing the packet afterwards via “ACCEPT”.

→ In private LMC installations, WEBconfig remote access via the web browser did not work if too many HTTP cookies were used.

→ An external modem that was connected to a LANCOM router and had a so-called APIPA address (Automatic Private IP Addressing) could not be reached by the LANCOM router because these addresses were not permitted in the proxy ARP from the LAN.

→ If an IP address was entered in the access station table, it was not possible to establish a WEBconfig session to a device from the LANCOM Management Cloud (LMC).

→ If port forwarding was set up with a port between 16384 and 65535, it could happen that this port was also used for a dynamic port negotiation of another network subscriber. In this case, the incoming packets were forwarded to the destination of the dynamic port negotiation instead of the actual destination.

→ In WEBconfig (e.g. in menu ‘Configuration / IP router / Routing / IPv6 routing table’) an IPv6 prefix was displayed incorrectly due to faulty HTML coding.

→ Due to an incorrect sorting of the port forwarding table, it could happen that port forwarding did not work correctly in case of overlapping entries (with different protocols).

→ In a VRRP scenario with individual WAN peers, in which these peers were additionally combined to form a load balancer, it could happen that the VRRP slave attempted to establish the WAN peers every second.
As a result, the CPU load of the device increased and a memory shortage occurred. A pause has now been programmed between the individual connection attempts, which means that the device is no longer pushed to its performance limit.

Wi-Fi

→ It could happen in a WLC cluster scenario that the sub-CA on the slave expired and no new certificate was obtained. This meant that the access points registered on the slave could not be managed.

→ It could happen that in the WEBconfig menu ‘Manage Public Spot Users’ no printouts of created Public Spot user data could be created.

LCOS improvements 10.42.0612 RU5

Bug fixes / improvements

General

→ A script upload via HTTPS no longer leads to a watchdog.

LCOS improvements 10.42.0611 RU4

Bug fixes / improvements

General

→ An access via LL2M to a device with hashed password failed and was acknowledged with the error message “user unknown on remote system”.

→ When using certificates with Elliptic Curve Algorithm for RADSEC, TLS negotiation could not be completed successfully.
Furthermore, the private key of a certificate with elliptic curve algorithm could not be uploaded to the RADSEC slot. The import process was aborted with the message “FAILURE”.

→ Creating a Wireshark trace via LCOSCap on a device with a hashed password failed and was acknowledged with the error message “cannot retrieve PSK”.

→ The ‘Dynamic Path Selection’ could not perform the DNS resolution via a loopback address. If a DNS server could only be addressed via a loopback address with a routing tag other than 0, this meant that DNS resolution of the measurement target (e.g. measurement1.cloud.lancom.eu) was not possible. As a result, incomplete data was displayed in the DPS graph in the LMC.

→ With the console command ‘passwd -n’ a password change can be performed without query. The change was not applied to SNMP access, so SNMP access was still possible with the old password.

→ When creating a RADIUS user via WEBconfig, the user profile could not be saved if no passphrase was entered there.

→ The rollout wizard was not started automatically with an existing rollout user, but you had to explicitly log on to the system as a rollout user for the wizard to start.

→ After an update to LCOS 10.42 RU3 it could happen that after a configuration synchronization with the LANCOM Management Cloud (LMC) a firewall rule containing a DNS destination could no longer be edited with LANconfig.

→ When using the LOCALNET station object in firewall rules, routes learned via RIP and BGP were assigned to LOCALNET. This could lead to the CPU of the router having a high load due to a very large number of filter rules.
Only networks in the ‘Connected LAN’ status are now assigned to the LOCALNET station object.

→ Running an LCOS script when using automatic network selection caused LANCOM devices with 4G module to terminate an existing WWAN connection, even if there was no configuration change to the WWAN connection that required the connection to be restarted.

→ If a LANCOM router or access point belonged to an ARF network that had a routing tag other than 0, the LLDP information displayed was not the IP address of the device but its MAC address.
→ Due to a misbehavior in the DHCP relay agent of a LANCOM router, it could happen that a network client could not obtain an IP address if the LANCOM router was configured as a DHCP relay.
→ When using TACACS+, the configuration could not be saved by a TACACS+ user via LANconfig if the main device password was present as an encrypted hash value.
→ If one of the default networks INTRANET or DMZ was not used (IP address 0.0.0.0) and 'Intranet' was selected as 'Network type', this network was treated as active by the router. If a self-created network was assigned the same interface as the default network (e.g. LAN-1), no communication was possible because the packets were discarded by the firewall with the error message "Filter info: packet received from invalid interface LAN-1".

Wi-Fi

→ In LCOS 10.42, the transmission channel between access point and ePaper display was not correctly transmitted to the ePaper server, which caused ePaper displays to be displayed as "Not reachable" and no communication between server and display could take place.
→ In LCOS 10.42, the ePaper module of the access point could not automatically report to the ePaper server due to a missing 'restart' command in the firmware. As a result, the access point lost the connection to the ePaper server. After restarting the access point, it reconnected to the ePaper server, but later lost the connection again.
→ If more than one voucher was created at the same time in the WEBconfig menu 'Setup Wizards / Set up Public Spot Users', the window for printing all created vouchers was not displayed at the end of the creation process.
→ In LCOS 10.40 or higher it could happen that certificate-based RADIUS authentication with ECDSA certificates failed. The ECDSA signatures have now been corrected.
→ When using the client management in the Wi-Fi, an abrupt restart could sporadically occur when the environment scan was performed.
→ For access points and Wi-Fi routers with IEEE 802.11ac Wi-Fi module, the base data rate (management frames) continued to be transmitted at 6 Mbps when the RX/TX transmission rates in the Wi-Fi were fixed at a value greater than 6 Mbps.

VPN

→ During the negotiation of an IKEv2 connection, the establishing router (VPN initiator) always sent the ‘MANAGEMENT_IP4_ADDRESS’ parameter of the ‘Dynamic Path Selection’ feature, even if this was not active. If this feature was not supported by the accepting router (VPN responder), this could result in the VPN connection not being established.

VoIP

→ If a VoIP client sent the parameter ‘rtcp-rsize’ with an outgoing call, the LANCOM router recognized this parameter as ‘Invalid’ and rejected the ‘Invite’ with the message “406 SDP - not acceptable”. As a result, the outgoing call did not go through.

→ With an incoming ISDN call it could happen that the external caller could not hear the called party (one-way voice transmission) because the ‘Media Attribute (a): nortpproxy:yes’ prevented the transmission of RTP data.

→ Forwarding an incoming external call from a SIP subscriber to an analog subscriber resulted in an immediate restart of the router.

→ It could happen that phone calls were not transmitted via the SIP-ALG because the external port was declared as invalid by the router. The packets were then rejected with the error message “ICMP Destination unreachable (Port unreachable)”.
Furthermore, the bandwidth reservation in SIP-ALG did not work anymore.

→ The functions ‘Consultation’ and ‘Switching’ did not work, because the router did not send SDP information in the “200 OK” after the Re-INVITE.

→ In a scenario with a Swyx Mediabridge a REFER with the actual destination of the call is sent in the ‘Refer-To’ header after call setup. Then the router sends an INVITE to this ‘Refer-To’ destination via the Swyx PBX. In case of an error the Swyx PBX did not answer with a “200 OK” but with the error message “500 Server Internal Error”. In this case the router tried to send the INVITE on another line. But since the replace information from the REFER was still used for this, the router sent the INVITE again via the gateway line to the Swyx PBX. An INVITE is no longer sent on a gateway line after the error message “500 Server Internal Error” has been received on this line. Furthermore the router waits for a “BYE” from the Swyx PBX and then terminates the call setup. If no “BYE” is received from the Swyx PBX, the router sends the “BYE” and terminates the call setup.

LCOS improvements 10.42.0473 RU3

Bug fixes / improvements

General

→ If H.323 is enabled in the configuration (default setting), this is disabled after an upgrade to LCOS 10.42 RU3. If the protocol is enabled again in the configuration, a syslog message is generated.

→ The cellular modem did not send regular router advertisements (RA) during IPv6 operation. This meant that after the router lifetime of 65,535 seconds (approx. 18 hours) had expired, the router no longer had a gateway and IPv6 communication was therefore no longer possible.
Shortly before the RA lifetime expires, a router solicitation (RS) is now sent to update the router lifetime.

→ If a router or access point was used as a DHCP client and a static routing entry with a gateway (next hop) was created on it, the gateway learned via DHCP was not adopted correctly. This resulted in no communication being possible via the static route.

→ When using particular DSLAMs on the provider side, it could happen with a LANCOM 1926VAG that the DSLAM did not transmit all the required parameters to the DSL modem due to an incompatibility between the installed DSL modem and the DSLAM. This meant that no DSL sync could be established and thus no DSL connection could be established.

→ The Wireless ePaper features ‘SyncProfile’ and ‘Label Events’ were not functional.

→ A disabled IPv4 firewall rule in which one or more port ranges were specified was misinterpreted when writing back the configuration, which meant that the configuration could not be written back to the LANCOM router.

VPN

→ If the router tried to send a packet over the VPN connection during a VPN connection setup in the time window between IKE negotiation and the change to the ‘Up’ state, all packets were dropped.

→ If a VPN connection was initiated by a downstream router with port forwarding active for UDP port 500, the response packets were not entered in the IPSec masking table by port forwarding. This resulted in the VPN connection not working.

Wi-Fi

→ The Public Spot ‘Idle Timeout’ could not be set via the XML interface. The value selected in the XML command was not accepted and the value entered in the device was output instead.

VoIP

→ In individual cases, it may happen that an UPDATE is sent by the caller instead of the called party during the early media phase of an incoming call. In such a case, the UPDATE was sent by the router back to the SIP line instead of to the local subscriber. This resulted in a one-way voice transmission.

→ In a scenario with a parent SIP PBX, if different codecs are used in the sessions between the router and the SIP client and the router and the SIP PBX for an outgoing call, the codec must be renegotiated with the SIP client in a re-INVITE so that the codec matches. If the SIP PBX sent a Re-INVITE to forward the call to the router at that moment, it was sent from the router to the SIP client even though the first Re-INVITE was not confirmed yet. This resulted in missing voice transmission in connection with noise at the calling subscriber.
The second Re-INVITE of the SIP PBX is now transmitted only when the first negotiation is completed.

→ If the Voice Call Manager received a REFER for call forwarding from a SIP PBX to a SIP client and received a ‘Session Progress’ with SDP data from the SIP PBX after sending an INVITE to the SIP client, the Voice Call Manager first sent a Re-INVITE to the SIP client and then, after receiving the message “200 OK” from the SIP client, erroneously sent an ACK to the SIP PBX, although the call negotiation was still open (such behavior will mainly occur in a scenario with a Swyx PBX in combination with a CTI+ client). This led to a call termination.

→ If the router received parameters in the ‘From and Contact’ field in an UPDATE that differed from the SIP registration, the router could not assign the SIP user. This led to a call termination.

→ In a SIP trunk scenario, it could happen that no call number tones were transmitted to the ISDN PBX. As a result, an outgoing call could not be initiated and established.

LCOS improvements 10.42.0383 RU2

Bug fixes / improvements

General

On ‘Deutsche Glasfaser’ Internet connections, the router advertisement is sent to the multicast IPv6 group and the unicast MAC address of the router. This caused the router to discard the router advertisement and thus Internet communication was not possible.
The router now accepts the router advertisements.

→ When writing back a configuration via SSH, it could happen that LANconfig reported “The configuration could not be written back to the device”, although the operation was successful.

→ With LANCOM Wireless ePaper access points (e.g. LANCOM LN-830E) it could happen that the connection to the Wireless ePaper Server was lost and not automatically re-established.

→ For some LANCOM devices it was not possible to download the SNMP device MIB via WEBconfig.

→ The fallback from IPv6 to IPv4 did not work correctly with the NTP client.

→ When using the ‘Dynamic Path Selection’ feature, if the firewall destination did not match the routing entry during the firewall check, the message “bad gateway: <host A> does not match <host B>” was issued and the next firewall rule was run. It could also happen that packets were dropped.
The gateway of the route is now checked before the route selection for the Dynamic Path Selection and the next rule is run through if the gateway does not match the firewall destination. Furthermore, the firewall trace displays the message “bad gateway: ACTUAL does not match REQUESTED”.

→ If the command ‘do Setup/Certificates/SCEP-Client/Update’ was executed via an addin script in the LMC on a device for the purpose of obtaining a certificate via SCEP client, this led to an immediate reboot of the device.

→ When using a load balancer, it could happen that the load balancer did not switch to the ‘connected’ status after the first line had been established. This resulted in further Internet remote stations not being set up.

VPN

→ If several VPN connections were assigned the same route (e.g. via IKE-CFG mode), the route of the first connection was displaced in the routing table when the second connection was established. When the first connection was terminated, the route was completely removed. This meant that communication via the VPN connection to this destination was no longer possible.

Wi-Fi

→ IGMP queries from the address 0.0.0.0 were not accepted. This caused the IAPP table to remain empty, resulting in disconnects during Wi-Fi roaming.

→ On a vRouter, after updating to LCOS version 10.42, the 'Login (Email to SMS)' page was duplicated in the Public Spot page table and the 'Fallback Error' page was missing. This resulted in the configuration not being rolled out via the LMC and instead being acknowledged with an error.

→ If the Public Spot page table in the path 'Setup/Public-Spot-Module/Page-Table' was filled with default values and changes were made to this table via LANconfig, the table contained empty values with "" characters after writing back.

VoIP

→ The table of active VoIP lines in the LCOS path 'Status/Voice Call Manager' displayed a maximum of 32 entries. If more than 32 lines were active, the remaining lines were not displayed. A maximum of 64 entries is now displayed.

→ Incoming SIP update packets via SDP were answered by the LANCOM router without SDP. As a result, calls in connection with a downstream PBX failed.

→ If the priority order of the offered DNS SRV records changed during a TTL DNS period, this was not noticed in the LANCOM Voice Call Manager, so that the LANCOM router did not connect to the new highest weighted site after the TTL expired. As a result, a SIP registration failed.

→ It could happen that an ISDN telephone displayed the destination number (connected number) in an unwanted format. It is now possible to suppress the connected number so that it is not sent in the ISDN 'Connect message'.

LCOS improvements 10.42.0280 RU1

Bug fixes / improvements

VoIP

→ Fixed issues with transferring phone calls using RE-INVITE, REFER methods, and related voice codec negotiation in scenarios with Swyx PBXs.

LCOS improvements 10.42.0277 Rel

Bug fixes / improvements

General

→ Requests from LANCOM-internal services (e.g. ICMP queries or ICMP measurements in the DPS) to the WAN which had a local sender address (e.g. 'ping -a INTRANET 8.8.8.8') were sent unmasked if only routes for load balancers were entered in the routing table and routes for the individual WAN connections were missing. As a result, the request failed.

→ Loading a LANCOM router configuration from a USB stick plugged into an unconfigured device failed.

→ The record for networks in the console path 'Status / DHCP client / LAN IP list' was always created with the maximum length instead of the actual length. This resulted in a blank page and the error message "404 Not found" being displayed when selecting an interface (e.g. INTRANET) in WEBconfig in the menu 'Tools / LCOS menu tree / Status / DHCP client / LAN-IP list / Ifc'. The information could not be read out via console either.

→ When logging DNS resolutions, the syslog was sent over port 512 instead of port 514.
As a result, the messages did not reach an external syslog server.

→ The Voice Call Manager in the LANCOM router sent e-mails in a text encoding in which, for example, umlauts were output illegibly. The e-mails are now sent UTF-8 encoded.

→ If a ping with a size smaller than 16 bytes was executed on the console (with the -s parameter), this resulted in an immediate restart, since the minimum packet size is 16 bytes.

→ If a process on the vRouter took a very long time (triggered by a lack of CPU resources), this could lead to a sudden restart.

→ The length check of ICMPv6 packets in the IPv6 firewall did not work correctly. This could cause ICMPv6 packets to be dropped by the router with the message "intruder detection".

Wi-Fi

→ The 802.11u parameters 'Include-in-Beacon-OUI' and 'Additional-OUI' only allowed lowercase letters to be entered on the console. In LANconfig, however, uppercase letters were also allowed for these parameters. Upper case letters are now converted to lower case letters.

→ When using 802.11u in conjunction with Passpoint R2, the NAI realm was not transmitted to the end device, so it could not establish a connection.

VPN

→ If the VPN partner requested multiple phase-1 proposals for parallel processing instead of sequentially as usual (e.g., SA1: AES-CBC, SA2:

Blowfish), the router restarted immediately.

→ After a firmware upgrade to LCOS 10.42 RC3 it could happen that IKEv2 VPN connections were no longer established via EAP authentication if no remote gateway was specified in them and 'No-Identity' was used as remote ID.

→ After establishing a dial-in VPN connection from a remote site, the routes were deleted and directly added again. This led to the fact that already existing sessions were also deleted and communication via this session was no longer possible (e.g. RDP).

VoIP

→ If a SIP provider sent an INVITE with a session timer that was too small, the router responded with the error message "422 Session Interval Too Small". If the SIP provider then did not send a new INVITE with an adjusted session timer, the call was disconnected and the caller did not hear a ringing signal. The message "422 Session Interval Too Small" is now only sent when using a 'Gateway line' to connect a SIP PBX.

→ If a SIP PBX sent the characteristic for SDP in lower case (rtp/avp) to the router in the message "200 OK", the router did not recognize the SDP and sent the "200 OK" without SDP to the provider. The provider responded with a BYE and the error message "488 Not Acceptable Here". This led to the fact that in such a case the telephone call did not take place.

→ If a SIP subscriber in INVITE sent the protocol in lower case in the SIP URI to the router (e.g. udp), the router rejected the packet with the error message "404 Not Found". The router is now case-insensitive.

LCOS improvements 10.42.0212 RC3

New features

Routing & VPN

→ IPv6 source address filter for IKEv2 VPN connections

Bug fixes / improvements

General

→ The table for the mobile radio history in the path ‘Status / Modem mobile radio / History‘ remained empty, regardless of whether a mobile radio connection was used or not, because the default value for recording the history in the path ‘Setup / Interfaces / Mobile radio / Logging interval‘ was ‚0‘ (switched off). The default interval has now been changed to 300 seconds (5 minutes).

→ The table ‘Status / Last-Admin-Logins‘ had a faulty structure, because the first column (the only index column) contained the IP address and not, as usual, a unique index value (e.g. a consecutive number).

→ The configuration reference via TR-069 when using an IPv6 address failed because the router‘s own IPv6 address was put into square brackets by the router’s TR-069 process and therefore was not recognized correctly.
In this case a fallback via IPv4 was performed.

Wi-Fi

→ In the table ‘Setup / WLAN Management / AP Configuration / IEEE802.11u / General‘ a profile name with a maximum of 32 characters could be entered for an 802.11u site profile. However, the same parameter was used in the table of Wi-Fi profiles with a name length of max. 31 characters. As a consequence, a profile name with 32 characters could not be configured in the Wi-Fi profile table because the maximum allowed number of 31 characters was exceeded.

→ In a WLAN controller scenario, the domain ID from the menu ‘WLAN Controller / 802.11u / Hotspot 2.0 Profile’ was not taken over by the access points, so the placeholder ‘0’ was used. This caused an incorrect domain ID to be passed to requesting Wi-Fi subscribers.

→ If an unsupported regular expression (RegEx) was entered for the ‘Venue Name’ in the console path ‘Setup / WLAN Management / AP Configuration / IEEE802.11u / General’ on a WLAN controller, the device rebooted immediately.

→ When using an individual start page in the Public Spot, only a white page was displayed when calling it, because the redirect URI (Uniform Resource Identifier) was passed on to the Public Spot participant with a wrong IP address.

LCOS improvements 10.42.0155 RC2

New features

General

→ The 802.1X authenticator for Ethernet ports is now included in all devices.
→ The 802.1X authenticator can now optionally immediately perform a check of the MAC address of the connected Ethernet device with a RADIUS server instead of an 802.1X negotiation.
→ In new configurations the MAC address of bundle interfaces is now ‘0’ and is converted to the system-wide, device-specific MAC address during operation. This simplifies the porting of configurations.
→ The HTTP(S) hit list of Layer 7 detection has been updated.
→ The ThinAP2.0/TLS protocol can now be used to connect to a Wireless ePaper Server.
→ In new configurations, the Telnet and Telnet-over-SSL management protocols are now disabled by default.

Routing & VPN

→ The line code of the LANCOM 179x series xDSL modem has been updated.

Wi-Fi

→ Support for Stanley-AeroScout RTLS tags
→ If the result of the channel evaluation of the automatic Wi-Fi channel selection consists of several channels of equal quality, one channel is selected from these using the system-wide MAC address. This improves scenarios in which several neighboring access points perform automatic channel selection simultaneously.
→ Support of a JSON-API to extract BLE and WLAN location data
→ The default WLAN passphrase is now empty. To activate an encrypted WLAN SSID, it is necessary to set a user-defined passphrase.
→ Support for PassPoint R2 configuration via WLC

VoIP

→ For SIP lines the transfer of a fixed PPI or PAI can be configured.
→ A loopback address can now be configured for SIP PBX lines.
→ The Voice Call Manager table ‘User Settings’ can now contain any number of entries.

Bug fixes / improvements

General

→ In the LANCOM OAP-1702B, the specific specification for the PoE power requested via LLDP from a PoE-capable switch was missing in LCOS.

→ LANCOM routers sporadically experienced CPU utilization of up to 100% due to a problem with the number of sessions in the IPv4 masking table of the devices. As a result, the high CPU load caused problems with IPv4 routing, among other things.

→ Communication with an external syslog server via a user defined port (not equal to 514) was not possible, regardless of the protocol used (TCP or UDP). The router ignored the setting and continued to use port 514.

→ The configuration could not be rolled out to a router managed by the LMC if a new object was simultaneously created in the DNS target list and referenced in a new firewall rule.

→ If a routing entry was created for a GRE tunnel that referred to an IP address from a local network, the GRE tunnel could not be established.

→ When changing the main device password with the console command ‘passwd -n‘, which included the escape character ‘\‘, additional characters were added to the beginning of the password. As a result, the device could not be accessed with this password and the password could not be reset with the ‘passwd -n‘ command.

→ If ‘Dynamic Path Selection’ was activated during the roll-out process of a complex configuration via the LMC, a sudden restart could occur.

LCOS improvements 10.42.0037 RC1

New features

General

→ The HTTP/HTTPS tracking list for the Layer-7 application detection has been updated.

Routing & VPN

→ SD-WAN Dynamic Path Selection

Wi-Fi

→ Omission of the standard Wi-Fi passphrase

→ A LANCOM WLC now configures the first Wi-Fi module (2.4 GHz) of a managed access point for 20 MHz channel width by default. This only affects access points that have newly been added to the management

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