Release Notes

LCOS
10.50 RU17

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 10.50 RU17, 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 10.50

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/software-lifecycle-management/product-tables-lcos-lifecycle-management

Support for the following devices is no longer available as from LCOS 10.50:

- → LANCOM 1631E
- → LANCOM 1781-4G
- → LANCOM 1781A
- → LANCOM 1781AW
- → LANCOM 1781VA-4G
- → LANCOM 730-4G
- → LANCOM 7100+
- → LANCOM 9100+
- → LANCOM IAP-4G
- → LANCOM L-151
- → LANCOM L-151E
- → LANCOM L-320 R2
- → LANCOM L-330
- → LANCOM WLC-4025+
- → LANCOM WLC-4100

4. Advices regarding LCOS 10.50

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 10.50

5.1 Feature highlights 10.50

Performance upgrade for the LANCOM ISG-8000

In large SD-WAN or site networking scenarios with a high number of IPSec VPN channels and high data volumes, the use of the LANCOM ISG-8000 central site VPN gateway is now even more efficient. By distributing the data load across multiple cores (multicore), the total performance of IPSec VPN connections is increased to 10 Gbps. Significantly more data can thus be exchanged in less time when using multiple VPN channels.

Fast failover for maximum operational reliability

Fast failover times are essential in infrastructures that require maximum operational reliability. By using Dynamic Path Selection (DPS) or BGP, switching from one IPSec-VPN channel to another takes less than a second now. Thus, in an active-active mode, the failure of a connection does not lead to any noticeable downtime, e.g. in business-critical processes such as payment transactions with EC cash terminals.

5.2 Further features 10.50

Extension of the IPv6 functionality

Benefit from even more future-proofing of your IPv6 site networking now: As of LCOS 10.50 RC1, functions such as 464XLAT with IPv6-only in cellular radio, NAT with IPv6 (NPTv6), load balancing with IPv6, and IPv6 polling are supported.

Platform expansion for the LANCOM vRouter

For even more versatile use, the LANCOM vRouter now also supports KVM (Kernel-based Virtual Machine) in addition to the hypervisor platforms Hyper-V, ESXi, and Azure.

You can find further features within the individual builds sections in chapter 6 “History LCOS 10.50”.

6. History LCOS 10.50

LCOS improvements 10.50.1635 RU17

Bug fixes / improvements

General

→ OpenSSL has been updated to version 1.1.1zb, which fixes some security vulnerabilities (CVE-2024-13176, CVE-2024-9143).

→ By updating the zLIB library to version 1.3.1, a security vulnerability has been fixed (CVE-2016-9840).

→ If IPv6 was active on a router, the router could restart immediately when Netflow analyzed an FTP data session that was transmitted via IPv6.

→ After a failure of the mobile network infrastructure of a mobile network provider, the used APN may be placed on a blacklist. However, on routers with Sierra MC7421, EM7421, and MC7455 cellular modems, the assigned timer for the entry in the blacklist was not interpreted correctly, so that the timer sometimes did not expire or expired very late. As a result, it was not possible to dial in to the mobile phone provider during the blocking state.

VPN

→ If DNS addresses were specified as IPv4/IPv6 target addresses instead of IP addresses in a VPN load balancer configuration, the table in the path ‘Status/VPN/Load-Balancer/Peer-Status/’ was filled with an infinite number of entries.

Wi-Fi

→ The mechanism for cleaning up the Wi-Fi ARP table did not work correctly, which could result in multiple entries for wireless clients. As a result, ARP packets for these wireless clients were not forwarded and communication was severely restricted.

LCOS improvements 10.50.1532 RU16

Bug fixes / improvements

General

→ After the maximum number of half-open connections for a connection source or a connection destination was reached, DoS (Denial of Service) detection dropped these packets until the runtime of all half-open connections for this source or this destination expired and these were deleted. This could lead to desired data traffic also being discarded.
DoS detection now allows communication after the maximum number of half-open connections has been exceeded, if the threshold is undercut by half again.

→ TR-069 also processed connection requests whose IP address or DNS name was not available in the Access Control List (ACL). Now only combinations of addresses that are also present in the ACL are processed.

VPN

→ In individual cases, when setting up / rekeying a Child_SA (ESP SA) on a LANCOM ISG-4000 / ISG-5000 / ISG-8000 and the vRouter, it could happen that a non-functional Child_SA was created. As a result, no data could be transferred via the VPN tunnel.

VoIP

→ SIP-ALG set the media endpoint for outgoing INVITEs in RTP to 0.0.0.0. As a result, no RTP session could be established and no voice transmission was possible.

→ If a call was sent from a SIP user with an Ascom end device to the LANCOM Voice Call Manager and then forwarded to an ISDN line, one-sided voice transmission could occur after the connection was established.

→ If an ISDN subscriber tried to retrieve the call after call forwarding via the Voice Call Manager, although the Voice Call Manager had initiated the call forwarding and thus disconnected the call from the ISDN subscriber's perspective, the Voice Call Manager rejected the request.
In such a case, the Voice Call Manager did not open the voice stream. This resulted in a one-sided voice transmission.

→ The Voice Call Manager did not take into account the 'Replaces' parameter in the 'To header'. If a SIP telephone sent the 'Replaces' parameter in the 'To header' instead of in a 'Replaces header', this resulted in the telephone call being terminated after a call was transferred.

LCOS improvements 10.50.1482 SU15

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 10.50.1481 RU14

Bug fixes / improvements

General

→ A security vulnerability in the RADIUS protocol has been fixed (VU#456537). For more information, please refer to the respective LANCOM KB article.

→ When using LACP and VRRP at the same time, the VRRP multicast packets were not transmitted via the LACP bundle. As a result, communication between the VRRP routers was not possible and flapping occurred.

WLAN

→ In scenarios where 802.1X authentication was used for SSIDs, clients with Windows 11 operating system could not connect to the SSID because authentication failed.

VoIP

→ If the Voice Call Manager received an error message in the SIP that belonged to a SIP call that no longer existed, this led to an immediate restart of the router.

LCOS improvements 10.50.1400 RU13

Bug fixes / improvements

→ 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.

→ 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.

→ 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.

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

→ If no SSL certificate is available for access via the web interface, LCOS can generate a temporary certificate from the “ssl_privkey”. If an ECDSA key instead of an RSA key was stored in the “ssl_privkey”, no temporary certificate could be generated. As a result, access via WEBconfig was not possible and the web browser used acknowledged the process with an error message due to an incorrect certificate.

→ If an IPv6 interface was activated for an EoGRE tunnel, it could happen that the EoGRE tunnel was constantly activated and deactivated again (flapping).

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.

VoIP

→ 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.

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

→ 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”.

→ 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 10.50.1301 RU12

Bug fixes / improvements

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

→ In individual cases, an 802.1X authentication of users with the "Framed-IP-Address" attribute could lead to an immediate restart of the router.

→ 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.

→ The execution of a script with the commands "beginscript" & "exit" sporadically caused existing BGP connections to be disconnected.

→ If multiple ARF networks were configured on a router with the same IP address (separated by VLAN), a configuration change in the ARF networks triggered a "gratuitous ARP flooding" in each network. In scenarios with very many identical ARF networks, this could lead to severe packet loss and also to an unmediated reboot of the router.
After a configuration change of the ARF networks, only one "gratuitous ARP" is now sent for each network.

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.

LCOS improvements 10.50.1180 RU11

Bug fixes / improvements

General

→ 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 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 the feature activation is initiated via console and the license server is not accessible, the activation remains in the ‘in 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).

VPN

→ When configuring an IKEv2 VPN connection to AES-GCM, incoming fragmented ESP packets were discarded with an error message.

→ When using the encryption algorithm AES-GCM, all incoming VPN packets were counted as errors. As a result, the counters for Rx-invalid and Rx-errors in the VPN statistics kept increasing.

→ 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 output in a VPN status trace.

Wi-Fi

→ A managed access point did not use the VLAN ID entered in the SSID of 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 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.

→ The Voice Call Manager simply forwarded RTCP packets so that the RTP headers remained the same. Certain remote stations cannot process these packets or reject them. This caused a call to be terminated after a while. The Voice Call Manager now supports RTCP, so the RTP headers are now matched correctly.

→ The area code stored in the ISDN interface (e.g. 02405) was interpreted incorrectly during call forwarding. With a CompanyFlex connection, this resulted in the wrong PPI being used in the direction of Telekom in such a case. The call forwarding was aborted as a result and the process was acknowledged by the SIP provider with the error message “403 Forbidden”.

→ 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.

LCOS improvements 10.50.1107 RU10

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).

→ 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 an IP address.

→ 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.

→ 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.

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

→ 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.

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

→ In the WEBconfig menu ‘Setup Assistant → Manage Public Spot Users’, users were displayed as ‘unauthenticated’ although they were successfully connected to the Public Spot.

→ 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.
→ OSPF interface costs were presented with incorrect values due to incorrect internal processing.
→ With an active backup WAN connection, routing packets were dropped for a short moment about every 20-30 seconds.
→ After running the WEBconfig setup wizard for Telekom CompanyFlex and SIP trunk lines, the wizard deactivated the interface 'Analog-2', although a phone number was stored for it.
→ General improvements have been made to the behavior of the content filter in the event of an error (e.g. if rating servers are not available).
→ If the cellular module performed a network scan and the SMS service accessed the cellular module during this, this led to an immediate reboot of the router.
→ When using the content filter, it could happen that proxy jobs were not terminated when the associated session was terminated and thus continued to occupy memory. This led to an immediate restart after some runtime of the router, since no more free memory was available.

VPN

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

VoIP

→ 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".
→ It could happen that in the output of the command line command "show vcm" the TTL specification was displayed in hexadecimal form.
→ Changing the password of a Public Spot user in WEBconfig did not work. After the change, the new password could not be used to log in to the Public Spot. If the e-mail address in a newly created user account was identical to that of an existing account, but the upper/lower case was different, a new user account was created even though it was the same e-mail address.

→ 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 ‘Un-Register’ 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.

→ Due to an unfavorable sequence during the LANCOM-internal search for configured SIP lines, it could happen that dynamic SIP lines were not found.

→ In case of a very fast call acceptance on the part of an ISDN telephone, it could happen that the Voice Call Manager sent the ‘200 OK’ before the ‘PRACK’ of the SIP provider. The telephone call was terminated as a result.

LCOS improvements 10.50.1050 RU9

New features

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

Bug fixes / improvements

General

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

→ A router with configured connection did not show masking of the WAN peer in backup state (testable with the 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.

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

→ When using an L2TPv3 connection, PMTU discovery only worked if an IP address was assigned to the interface. In scenarios where the interface could not be assigned an IP address, or it did not make sense to do so, this resulted in performance degradation when packets had to be transmitted repeatedly. PMTU discovery is now also supported in scenarios without an assigned IP address.

→ In the WEBconfig interface of a LANCOM 19xx series device, the status “internal error” was displayed for a functioning second VDSL connection on the interface ‘VDSL-2’/’XDSL-2’ at the interface ‘VDSL-2-1’/’XDSL-2-1’.

→ The TR069 protocol did not work over any cellular Internet connections. Via the provider ‘Deutsche Telekom’ TR-069 is still not possible via mobile radio.

VPN

→ If rekeying of a Phase 2 SA is done with different crypto parameters than for the first Phase 2 SA, the IPSec transport of the previous Phase 2 is still used. If the encryption was implemented in hardware in one case and in software in the other, this resulted in an immediate reboot of the router.

Wi-Fi

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

VoIP

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

→ If TR069 settings are changed after device configuration, this change is reflected in the ACS provisioning code, which must be synchronized back with the ACS server. However, the synchronization process was not performed so that, for example, changed firmware update settings were not performed according to the change.

→ The registration of a VoIP client on a higher-level PBX was sporadically disconnected by the Voice Call Manager of the LANCOM router. As a result, the analog client lost its connection to the PBX until the next successful re-registration.

→ In a scenario with a Swyx PBX and a CTI+ subscriber, the Voice Call Manager sent a Re-INVITE to the CTI+ subscriber when the call was forwarded to a 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 an analog or ISDN user at a LANCOM router initiates an outgoing call, the Voice Call Manager uses a codec list with PCMA followed by PCMU. If the far end also proposed a list with both codecs in reverse order instead of a concrete codec, the Voice Call Manager used the codec PCMA for the RTP communication. If the far end did not allow RTP communication using PCMA, this resulted in the voice transmission not working.
Now, when receiving a codec list, Voice Call Manager always uses the first codec.

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

LCOS improvements 10.50.0953 RU8

New features

→ DNS forwarding in the ‘Forwarding’ table is now also supported on LAN interfaces, not only on remote stations. For this, a DNS server must have been obtained via DHCP on the corresponding LAN interface.

→ The handling of ARP on bridge interfaces is now switchable.

Bug fixes / improvements

General

→ Due to a misbehavior of the DNS cache 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.

→ For the LANCOM vRouter, the information about the available RAM was not correctly reproduced.

→ In the syslog of LANCOM cellular routers of the 19xx series with dual SIM, the status for SIM card slot 2 was always the status of slot 1.

→ 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/’.

→ RIP networks are kept track of in a table to check whether the source address is located in the stored network. In case of a ‘Link Down’ event the network is removed from the table and in case of a ‘Link Up’ event it is added back to the table. After a ‘Link Down’ and subsequent ‘Link Up’ event it could happen that the network was not re-inserted into the table. Furthermore, the network was not added to the table after a router restart if the ‘Advertise this network to other networks via RIP’ function was not active.
In both cases this resulted in the RIP network not being propagated. In a RIP trace, the error message “bad source IP address → discard” was then issued.

→ Disabling the TR-069 function by an ‘Auto Configuration Server’ (ACS) of an Internet provider was not saved boot-persistently.

→ The NTP client always performed DNS resolution explicitly with IPv4 AND IPv6 during NTP synchronization, which could cause the continuous synchronization to fail if, for example, IPv6 was not used. DNS resolution is now always performed with IPv4 OR IPv6.

→ In a scenario consisting of an Internet connection with backup and a VPN connection with backup, a failure of the Internet connection was followed by a switch to the backup connection. This also initiated the establishment of the VPN backup. In individual cases, it was possible 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').

→ For 5G WWAN connections in standalone mode, the information about the radio mode and the frequency bands used was missing after a successful connection setup.

→ A DNS check for a DynDNS entry in the action table did not work if this DNS name was also present in the local network.

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

→ After reestablishing an existing 464XLAT connection that had learned the PLAT prefix via DNS record, no new DNS request was subsequently made for the PLAT prefix.

→ Due to an error in the detection of configured WWAN connections (4G/5G) on dual SIM-capable LANCOM routers (e.g. LANCOM 1906VA-4G) it could happen that the WEBconfig dashboard of the devices also showed connections as active which were not configured.

→ 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'.

→ 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.

→ No '5G Standalone' connection could be established via 5G router (for '5G Standalone' operation at least WWAN firmware 03.09.06 is required).

→ If, after pairing a device with the LMC, an incorrect configuration (e.g. a reference to a non-existent profile) was made via LANconfig when manual configuration changes were actively transferred to the LMC, the configuration was not converted correctly during a firmware update and was therefore subsequently marked as 'Not current' in the LMC. This led to an immediate restart of the device during a further firmware update.

→ If a SIM card was not inserted in a LANCOM cellular router with a cellular backup connection set up and a switch was made to the backup connection, this led to recurring restarts of the cellular module. In individual cases, this could also lead to sudden restarts of the device due to memory loss.
→ If one was connected to another LANCOM device via LL2M from the command line of a LANCOM router and wrote a script to the other device in the session, the router from which the LL2M connection was initiated would restart abruptly.
→ For routers with a 5G modem, the data throughput was not displayed and remained permanently at 0.
→ When a command was entered in the Secure Terminal of the LMC, it could sporadically happen that the first character of the issued command was missing.

VPN

→ OpenSSL could not process certain parameters in the X509v3 extension. After uploading a corresponding VPN certificate, the router could restart immediately.
Furthermore, an unmediated reboot of the router could also occur if such a certificate was used in a VPN client for an IKEv2 authentication with the router, but the certificate was not uploaded in the router.
→ 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.

Wi-Fi

→ If the client steering function was used in a WLC-managed wireless LAN and many wireless LAN clients were registered to one SSID, the WLC could restart immediately.
→ If the IP addresses of additional WLAN controllers (IP addresses of alternative WLCs) with a value >= 128 were stored in an octet on a WLAN controller in the Wi-Fi profile used, these were displayed incorrectly in a CAPWAP CTRL trace in the ‘Discovery Response’.
→ In a WLC scenario, if an entry was added to or removed from the ‘Setup/WLAN-Manangement/Static-WLC-Configuration’ table for a LANCOM access point connected via SSH with the VLAN module enabled, this could result in a loss of connection between the WLC and the access point.
→ If a radio field optimization was to be performed for a specific access point (by specifying the device name or MAC address), the optimization failed.

VoIP

→ Due to incorrect handling of information in the RTP streams of incoming FAX transmissions, it could happen that they aborted.

→ If a SIP client in the local network changed the IP address of the SIP registrar when SIP-ALG was active, SIP-ALG continued to use the old IP address. This resulted in the SIP client losing the registration and thus no more phone calls were possible.

→ If the primary SIP server is unavailable, a switch to the next available server occurs automatically. The Voice Call Manager then remained permanently connected to this server (thus even after the TTL expired) and did not switch back to the primary server unless the server order changed.

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

→ 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 a wrong PPI was stored in the INVITE of an outgoing call for a SIP single account (e.g. wrong format), the call was rejected by the registrar and was subsequently not established.

LCOS improvements 10.50.0819 RU7

New Features

→ Support of a DHCPv4 stateless relay

Bug fixes / improvements

General

→ A vulnerability in the zlib library has been fixed (CVE-2018-25032).
→ A vulnerability in the OpenSSL library has been fixed (CVE-2022-0778).
→ If the TR069 function was deactivated by the ACS server, communication stopped as desired, but after a reboot of the router, TR069 was executed again because the function was switched active again.
→ On a LANCOM ISG-8000 the table for selecting the communication protocols to be used was missing in the configuration path '/setup/lan-bridge'.
→ If the WEBconfig option 'Extras/LCOS-Menutree/Setup/Config/Passwords/Keep plain-text' was set to the value 'No', an immediate reboot of the device could occur.
→ If the length of a console path exceeded 100 characters, this caused an immediate restart when saving the configuration as a script (since words in German usually have more characters than the English name, this can occur more often when changing the console language to German).
The maximum character length of a console path has now been increased.
→ When using Hairpin NAT and Policy-Based NAT at the same time, Policy-Based NAT no longer worked when a Hairpin NAT session was terminated. In a firewall trace, the error message "inbound masquerading, packet rejected" was issued in this case.
→ Sporadic reboots could occur on a LANCOM ISG-8000 due to an error in the multicore support.
→ A loopback address stored in the console path 'Setup/Autoload/Network/Firmware' was not taken into account. This could lead to the download server not being reached and thus the firmware update not being performed.

Wi-Fi

→ If 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.

→ When using a WLC tunnel, data packets must have a 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 LCOS LX access points, this meant that they could not process the corresponding data packets and the packets were therefore discarded.

VoIP

→ The WEBconfig setup wizard for configuring an All-IP connection did not correctly create the configuration for analog users. For the user entries, a correct entry for the interface to be used (e.g. Analog-1) was only stored for the first entry.

LCOS improvements 10.50.0725 RU6

New Features

→ 5G performance enhancements for LANCOM 1926VAG-5G and 1900EF-5G

→ New DSL line code for the LANCOM 179x series with support for the DSL features ‘Save our Showtime’ (SOS) and ‘Robust Overhead Channel’ (ROC) to improve stability on DSLAMs that support these optional features

→ The TR-069 TLS default values have been adjusted to current encryption algorithms.

→ Improvements regarding the synchronization between the LANCOM Management Cloud (LMC) and TR-069

Bug fixes / improvements

General

→ After an update to LCOS 10.50 RU5 the function ‘Enable-HSUPA’ was missing in the configuration of a LANCOM 1783VA-4G in the path ‘/Setup/Interfaces/Mobile’.

→ 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.

→ If a bandwidth limit of more than 4 Gbps was entered in the table ‘/Setup/Interfaces/DSL’, an overflow occurred because a maximum of 32 bit values could be entered in the table column. This has now been changed to 64 bits.

→ Internet connections on devices of the LANCOM 1926 series could be interrupted and sync losses could occur at irregular intervals if the provider made frequent adjustments to the data rates (e.g. due to fluctuations in the interference level on the xDSL line).

VoIP

→ 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. In the process, the PAI, PPI and FROM fields in the SIP header were run through in the specified order, but only the first field with a phone number was checked. 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.

LCOS improvements 10.50.0619 RU5

New features

→ The USB print server is disabled by default after a device reset.

→ The network name can now be specified in the action table variables for IPv6 LAN address and LAN prefix (%x and %y).

Bug fixes / improvements

General

→ 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.

→ When establishing a VPN connection via the 5G module (WWAN) of a LANCOM 1926VAG-5G or 1900EF-5G, no communication was possible via the VPN connection.

→ A DynDNS match via the action table using IPv6 was not possible with a static prefix. Furthermore, the DynDNS match only worked for the network INTRANET, but not for other networks.

→ On a vRouter as well as on the LANCOM ISG-8000 the ‘Checksum Offloading Info’ was always added even if this was not required. This could lead to packets with a VLAN tag not being transmitted.

→ 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.

→ 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.

VPN

→ For an interface with MTU not yet negotiated, a default value of 1280 bytes was used. Since the adjustment to the MTU did not work correctly, the default value of 1280 bytes was still used. This meant that larger packets with the 'Don't fragment' flag set could not be transmitted over a VPN connection and communication was thus severely disrupted or only possible very slowly.

VoIP

→ When the LANCOM VoIP router received a call that contained optional information about the bandwidth used for the session, it copied these lines twice into the "200 OK" response that it sent when accepting the call. As a result, an incoming call did not go through.

→ When using SNOM DECT terminals, it could happen that they could no longer register with the LANCOM router because devices changed the 'Contact URI' during each registration process and the change sent in the REGISTER was not changed in the stored binding information of the LANCOM router.

→ 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.

→ 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 only arrived at the Voice Call Manager 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 the SIP provider announced a change in the priority of the SIP servers in an SRV response, the SIP line was taken down and the message "generic failure" was issued in the syslog.

The SIP connection is now only disconnected and re-established if the IP address of the currently used SIP server no longer corresponds to the IP address of the highest priority server. In this case, the error message "server order changed" is output in the syslog.

LCOS improvements 10.50.0530 RU4

New features

→ For the 802.1X authenticator for LAN connections, a separate RADIUS server can now be specified for the MAC authentication bypass.

Bug fixes / improvements

General

→ Changing the transmission mode in the WWAN configuration of a LANCOM 5G router had no effect. All possible operating modes were always used.

→ If the PPTP, PPPoE or L2TP server was active and remote access to the router was allowed at the same time, an attempt to connect to the router using the username ‘admin’ resulted in an immediate restart, which was triggered by writing the event log.

→ When calling HTTPS websites through the ‘Dynamic Path Selection’ feature, the HTTP client in the router did not discard the HTTPS sessions and also did not free the memory again. This led to an unmediated reboot of the router after some runtime when no more free memory was available.

→ In individual cases, the router could restart immediately if an internal IPSec table was not yet initialized correctly and an IPSec packet was received.

→ After adjusting the key length of an existing certificate authority (CA), it could not be reinitialized afterwards because the CA could not be started due to the different key length.

→ 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.

Wi-Fi

→ On a LANCOM ISG-8000 with the Public Spot option enabled, the maximum number of Public Spot users supported was 128 users instead of the unlimited number of users (maximum 2500 users recommended).

→ After performing an environmental scan to detect rogue access points, the respective Wi-Fi module remained in scan mode. As a result, normal Wi-Fi operation could not be used on the module.

→ When using a Wi-Fi interface in P2P mode, it uses the MAC address of the Wi-Fi card as the BSSID, and the logical Wi-Fi interfaces are assigned local MAC addresses as the BSSID.

When the P2P configuration was rolled out via the LMC using an addin script, the actions for assigning the MAC addresses could not be initiated correctly and thus the P2P interface and the other logical Wi-Fi interfaces received the same BSSID. This led to an immediate reboot of the access point. Furthermore, the P2P configuration was not adopted.

→ The character 'ALT+34' could not be used when assigning a WPA-PSK.

VoIP

→ The '#' character is encoded with '%23' in the ASCII character set. If in a call route a filtering of the called number e.g. with '#21#' was used, but in the 'To' header of the corresponding INVITE the character string '%2321%23' was specified, the Invite was processed incorrectly and a call was not established, because the character string '%23' was not treated as just one special character, but as three characters. In the LANCOM router, therefore, '%23' is now always first converted to '#' and later (for compatibility reasons) back to '%23'.

→ The Voice Call Manager negotiates and uses a value for the registration update (Min-Expires) with the SIP provider. In scenarios where the SIP provider specified a smaller 'Expires' value in the "200 OK" after the REGISTER in the Contact field, this was not taken into account by the Voice Call Manager. This caused the registration to abort after the 'Expires' value expired.

LCOS improvements 10.50.0434 RU3

New features

→ The status of the IPv6 firewall is now displayed in the WEBconfig dashboard.

→ For logins or login attempts to the device, the MAC address (if available) of the accessing station is now also logged.

→ LCOS 10.50 RU3 provides updated modem firmware for the LANCOM 1926 series DSL modems, which includes stability improvements for G-FAST and VDSL connections.

Bug fixes / improvements

General

→ In the command line, a filter option via @ character was no longer possible with the 'ls' command (e.g. ls Status/Voice-Call-Manager/Lines/ @ "WIZ_T-123456").

→ If no user name was specified when logging in to a LANCOM device with the user account of the root administrator, no user name was written to the respective log entry in the event log of the device.

→ 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.

→ Access via LL2M to a device in factory state without a set password was not possible. In this case, the error message "user unknown on remote system" was issued.

→ 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.

→ When a client made a NAPTR request to the router, LCOS 10.50 with DNS logging enabled in the syslog server caused the router to reboot immediately.

VPN

→ If the table for additional remote VPN gateways contained an entry with a routing tag for which there was no route in the IP routing table, a VPN connection was not established if the primary remote gateway was unreachable, even if there were entries in the 'Additional remote gateways' table with a routing tag for which a route existed.

Wi-Fi

→ 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.

→ If larger amounts of data were transferred on an access point with an active DSLoL connection (e.g., due to a download or a longer speed test), this could lead to an immediate restart of the access point.

VoIP

→ In a scenario with a SIP PBX, if a telephone call between two subscribers (A and B) was forwarded to a third subscriber (C) using the 'Hold' function, the LANCOM router answered the INVITE (without SDP) from the PBX itself instead of forwarding it. This led to the fact that no RTP data was subsequently transmitted and thus no voice transmission was possible between subscribers A and C.

→ Outgoing calls to a fax terminal could sporadically cause an immediate restart of the LANCOM router due to a "403 Error Response" to the Re-INVITE with the text "Forbidden - PBX Validation Failed" if the overlap dialing functionality was used on the LANCOM router.

→ 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.

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

LCOS improvements 10.50.0331 RU2

New features

→ Support for LANCOM SFP-GPON-1 module

→ Update of the DSL line code of the LANCOM 1926 series

Bug fixes / improvements

General

→ 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.

→ On the LANCOM 1790VA-4G+, information about the cellular band in use was not displayed in the status.

→ The LANCOM routers of the 1926 series could regularly terminate the ADSL and/or VDSL Internet connection. The Internet connections were also not automatically re-established after an interruption (reboot solved the problem until the next interruption).

→ If TR-069 functionality was enabled, the LANCOM router could reboot without warning.

→ Due to a limited character set, IPv6 link local addresses could not be used with BGP.

→ If an IPv4 address pool was stored in the configuration of a LANCOM router and a new VPN dial-in was created via the Setup Wizard in WEBconfig, the existing address pool could not be selected in the Setup Wizard.

Wi-Fi

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

VoIP

→ In a scenario in which 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 10.50.0235 RU1

New features

→ The activity status of the DNS forwarder is now also displayed in the WEBconfig dashboard under ‘Services’.

→ **VoIP:** For TCP-based SIP lines, a TCP keepalive packet is now sent every 60 seconds. The interval is configurable on the CLI.

Bug fixes / improvements

General

→ If a value 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).

→ When saving a script configuration file in WEBconfig, an invalid file extension was assigned to the file.

→ When the ‘show ip-addresses’ command was entered, the value for the DHCP lease time, if it reached 0, remained at that value.

→ 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 allowed by the proxy ARP from the LAN.

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

→ When using certain 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.

→ When a LANCOM router was operated as a DNS server, in some cases the device responded to SOA and NS queries with the trace message “bad coded request”. As a result, the request could not be executed.

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

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

→ When using a loopback address for sending e-mails via SMTP, the loopback address was not taken into account. If a routing tag other than 0 was specified in the loopback address, no transfer to the SMTP service took place for this and the routing tag 0 was used. This could lead to the fact that sending e-mails was not possible.

→ Due to a limitation in the number of registered MAC addresses, the VRRP function could only be used on the first 6 ARF contexts. This only affected routers with DPAA (19xx series, ISG-1000, ISG-4000, and WLC-1000.

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

→ 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.

→ 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'.

→ Matching the IP address with a DynDNS service did not work when using HTTPS because the traffic could not be transmitted due to a too high MTU.

→ Packets from a network with an associated LACP interface were discarded by the firewall because the intruder detection detected an incorrect interface. As a result, communication with this network was not possible.

→ If a backup connection was specified in the backup table whose name designation was shorter than that of the main connection, a firewall rule containing a station object with the name designation of the main connection could not be written to the device.

→ When using LACP, it could sporadically happen that the response to an incoming packet was sent over a different LACP interface. This caused the packet to be discarded.
On routers with hardware switch (17xx and 19xx series), the error message "sEthSwitchDrvrDscr: WARNING: physical port x is not part of function LAN-x (port mask 0×04), packet will be discarded" was issued in the Ethernet trace in this case. On routers without a hardware switch (ISG-x000, vRouter), the packets were silently discarded.

Wi-Fi

→ Access points with an old firmware (e.g. version 9.24) could not be managed by a WLAN controller due to a faulty TLS handling.

→ 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.

→ After a firmware update to LCOS 10.50, an OAP-830 without an active VPN option could sometimes experience a boot loop.

→ If a WLAN strength trace was executed when the WLAN trace MAC address was set, the device rebooted immediately.

VoIP

→ In scenarios where a Swyx server with software lower than version 12.30 was used, the fax transmission from the LANCOM router to Swyx could fail due to an incorrect transaction ID.

→ Because TCP keep-alive packets sent by the LANCOM Voice Call Manager contained a SYN flag, VoIP lines that did not use signaling encryption could lose registration.

LCOS improvements 10.50.0145 Rel

New features

→ Support for RADIUS Dynamic Peer Discovery according to RFC 7585

Bug fixes / improvements

General

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

→ 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 possible with the old password. (CVE-2021-33903)

→ 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”.

VPN

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

→ After taking down and then re-establishing a VPN connection (both IKEv1 and IKEv2) with IPv6 on a vRouter or LANCOM ISG-8000, the VPN rules (SA) were not established correctly. As a result, communication over the VPN connection was no longer possible.

VoIP

→ 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.

→ 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.

→ In individual cases, it can happen that an UPDATE is sent by the caller instead of the called party for an incoming call during the early media phase. 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 transmission of the second Re-INVITE of the SIP TC system is now transmitted only when the first negotiation is completed.

LCOS improvements 10.50.0129 RC3

New features

→ The status of the IPv6 firewall is displayed in the WEBconfig dashboard.

→ For logins or login attempts to the device, the MAC address (if available) of the accessing station is now also logged.

General

→ New DSL line code for LANCOM 1926 series devices

→ On the DSL routers of the 19xx and 179x series, it is possible to switch between the current and an alternative DSL line code.

→ Support of a DNS filter for detection and filtering of unwanted DNS data tunnels at the client side

→ Support for IPv6 prefix discovery with 464XLAT according to RFC 7050

→ The WLC disables DNS servers and DNS forwarders on managed APs.

→ New VPN analysis command ‘ikectl’ on the command line

→ Support for automatic path MTU detection with IPSec.

Bug fixes / improvements

General

→ In WEBconfig, only the user data of one selected Public Spot user could be printed. If multiple user records were selected for printing, the printing process ended in an endless loading loop.

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

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

LCOS improvements 10.50.0115 RC2

New features

Wi-Fi

→ Support for Fast Roaming over-the-DS

Bug fixes / improvements

General

→ After an update to LCOS 10.50 RC1 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.

→ It could happen in individual cases that sessions were not terminated properly (e.g. when using IPSec-over-HTTPS) and the reserved memory was not released again. This caused further packets to be dropped and communication was only possible to a very limited extent.

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

LCOS improvements 10.50.0091 RC1

New features

→ Performance optimization due to multicore support for LANCOM ISG-8000 with IPsec VPN
→ Support for Bidirectional Forwarding Detection (BFD) with BGP
→ (Sub Second) Session Switchover for Dynamic Path Selection (DPS)
→ DPS: ICMP measurement intervals now support intervals with a time resolution in milliseconds
→ DPS: In addition to ICMP, HTTP(S) is also supported as a measurement method
→ Support of the CLAT side of 464XLAT for IPv6-only in mobile communications
→ NPTv6 (prefix NAT) support for IPv6
→ The load balancer now supports IPv6
→ IPv6 line polling support
→ In the IPv6 firewall, MAC addresses can be configured as a station object (source).
→ In the IPv6 firewall, a delegated provider prefix can be configured as a station object to share a dynamic prefix in a router cascade.
→ In applications where DNS names can be configured, the preferred address family (IPv4 or IPv6) can be specified.
→ Dynamic Path Selection (DPS) now supports IPv6.
→ Support for Curve448 in SSH
→ Public Spot now supports IPv6.
→ Public Spot: The MAC address format is now configurable.
→ Support for RADIUS attributes according to RFC 5580
→ The DHCP client now displays the lease time in the status menu.
→ The Rx / Tx bandwidth limitation is now also evaluated for 802.1x RADIUS authentication.
→ The Layer7 application detection and DNS names in the firewall can now be configured in a common table.
→ Support for session cookie and anti-CSRF token in WEBconfig
→ Plain text passwords of the main device password are disabled after a device reset.
→ The IKEv2 lifetimes are adapted to the current BSI recommendations after a device reset.
→ SHA-1 is no longer included in the IKEv2 default proposal after a device reset.
→ The delegated IPv6 provider prefix can be transmitted to the VPN peer via IKEv2 routing.
→ Support for H.323 in the IPv4 firewall is removed.
→ The vRouter now supports KVM as a hypervisor platform.

Bug fixes / improvements

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.

→ When using SIP-ALG, it could happen that the port for RTP communication became invalid and an incoming RTP packet was rejected with the message “ICMP Destination unreachable (Port unreachable)”. This resulted in a one-way voice transmission on the part of the called subscriber during an outgoing telephone call.

→ The Voice Call Manager supports multiple streams with different codecs. However, these must be initialized during the call setup.
If a call was initially established with one stream (e.g. G.711) and a second stream was added in the re-INVITE (e.g. T.38), the Voice Call Manager could not process the second stream. As a result, data packets of the second stream were not transmitted anymore.

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.