Release Notes

LCOS
9.24 SU13

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 9.24 SU13, as well as the improvements since the previous version.

Before upgrading the firmware, please pay close attention to chapter 5 “General advice” of this document.

Latest support notes and known issues regarding the current LCOS version can be found in the support area of our website
www.lancom-systems.com/service-support/instant-help/common-support-tips

2. The release tag in the software name

Release Candidate (RC)
A Release Candidate has been extensively tested by LANCOM and includes new LCOS featurses. It is suitable for testing and is not recommended for use in productive environments.

Release Version (REL)
The release version has been extensively and successfully tested in practice. It contains new features and improvements over previous LANCOM operating system versions and is therefore recommended for use in productive environments.

Release Update (RU)
A release update is a further development of an initial release version in productive environments and contains minor improvements, security fixes, bug fixes and smaller features.

Security Update (SU)
Contains important security fixes for the respective LANCOM operating system version and ensures that your security level remains very high on an ongoing basis in your productive environment.

3. Device-specific compatibility to LCOS 9.24

LANCOM products regularly receive major firmware releases throughout their life-time which provide new features and bugfixes.
LCOS release updates including bugfixes and general improvements are available on a regular basis for devices which do not support the latest LCOS version. You can find an overview of the latest supported LCOS version for your device under www.lancom-systems.com/products/firmware/lifecycle-management/product-tables

LANCOM devices without support as of LCOS 9.24

- → LANCOM 1711+ VPN
- → LANCOM 1721+ VPN
- → LANCOM 1722 VoIP
- → LANCOM 1723 VoIP
- → LANCOM 1724 VoIP
- → LANCOM 1811n Wireless
- → LANCOM 1821+ Wireless ADSL
- → LANCOM 3850 UMTS
- → LANCOM 800+
- → LANCOM DSL/I-10+
- → LANCOM L-315agn dual Wireless
- → LANCOM OAC-54-1 Wireless
- → LANCOM OAP-310agn Wireless
- → LANCOM OAP-54 Wireless
- → LANCOM WLC-4006
- → LANCOM WLC-4025
- → LANCOM XAC-40-1
- → Swyx 1722 VoIP
- → Swyx 1723 VoIP
- → Swyx 1724 VoIP

4. History LCOS 9.24

LCOS improvements 9.24.0475 SU13

Bug fixes

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 9.24.0474 SU12

Bugfixes / improvements

General

→ A potentially security-relevant issue has been fixed on LANCOM routers in conjunction with IPv6.
This issue can occur when IPv6 networks are connected via IPSec (IKEv1 or IKEv2), and an IPv6 Internet connection is used simultaneously.
In this case, an update to the current LCOS version is strictly recommended.
This issue has been fixed in the following LCOS versions:

- LCOS 10.32 SU3
- LCOS 10.20 SU9
- LCOS 10.12 SU14
- LCOS 9.24 SU12
- LCOS 9.00 SU8
- LCOS 8.84 SU11

Wi-Fi

→ If on a dual radio acces point with two 802.11ac modules a client switched from one module to the other one, it could sporadically happen, that the client did not receive a unique association ID from the access point and the client could not transmit any data.

→ If a Public Spot login was executed per HTTPS (TLS 1.3), the user did not see the login page, but a browser information displaying a non-ignorable security message. As a result, a user could not authenticate to the Public Spot.

VoIP

→ Concerning particular setups with analog phones, a VoIP issue has been solved which resulted in unidirectional voice communication or no connection establishment. The update is available for the following devices:

- LANCOM 1783VA, 1783VAW, 1783VA-4G
- LANCOM 1793VA, 1793VAW, 1793VA-4G
- LANCOM 1906VA, 1906VA-4G
- LANCOM 883 VoIP

LCOS improvements 9.24.0472 RU11

Bugfixes / improvements

General

→ At the first obtainment of a device certificate, the SCEP client saved the initially received CA certificate directly to the configured VPN container. This resulted in an incomplete VPN container which could not be used by VPN. The CA certificate is now saved to a temporary container. Only when all elements of the container are complete, the SCEP client writes the data to the configured container.

→ The SCEP client erroneously used the command “GetNextCACert“ for the initial obtainment of a certificate instead of the command ”GetCACert“. This resulted in answering the request with an HTTP error ”400 Bad Request“ by the certification site.

→ When using Wi-Fi routers or access points with 802.11n Wi-Fi module, connection losses in the 2.4 GHz band could occur if a Wi-Fi client in powersave mode accepted smaller re-ordering frames as usual (e.g. 8 instead of 64 packets). Amazon ECHO devices were affected by this.

→ Simultaneous use of eBGP and iBGP could lead to routes with static eBGP prefixes being drawn back. As a result, communication between multiple AS (autonomous system) was no longer possible.

→ The request interval for obtaining certificates via the SCEP client in the path “Setup/Certificates/SCEP-Client/Check-Pending-Requests-Interval” was ignored and instead a fixed value of 60 seconds was used. Now the configured value is used again.

→ In certificate-based scenarios (VPN and WLC) which used the internal SCEP client of the LANCOM router for certificate distribution, the SCEP client did not renew expiring RA certificates automatically. As a result, e.g., certificate-based VPN connections could no longer be established, and WLC-managed access points could no longer establish a connection to the WLC. Further information on this behavior is available in the LANCOM Support Knowledge Base.

Due to a validity check error the device certificate could not be renewed when using the RA Auto Approve function.
As a result, certificates could not be received in WLC- and VPN scenarios. Further information on this behavior is available in the LANCOM Support Knowledge Base.

On certificate requests via SCEP client to external certificate authorities (e.g. Windows CA), it could happen, that certificates could not be accepted due to a wrong “mime type“. The certificate is now checked directly without considering the “mime type“.

LCOS improvements 9.24.0411 PR

Bugfixes / improvements

General

→ If a provider requested authentication data (user name and password) during the LTE attach phase, the LANCOM router selected wrong authentication data (from a different remote peer), if no further Internet or IPSec connection was established at that time.

→ The LLDP path request in SNMPv3 has been adjusted to correct the index generation.

→ In rare cases a miscalculation of a UDP checksum for masquerading (NAT) could occur.

→ Routes with a network address that was decimally completely filled out all four octets (e.g. 192.168.100.100/30), were propagated by BGP either falsely (e.g. as 0.0.0.0/26) or not at all.

→ The OpenSSL library has been updated to version 1.0.2o.

→ In the application firewall a configured action was executed already during the detect phase. Now, executing an action takes place only after the protocol has been confirmed.

→ An xDSL connection was not terminated immediately if the corresponding DSL remote peer was deleted from the configuration by script.

VPN

→ By optimizing the GRE protocol the routing performance of GRE tunnels (LAN-LAN as well as LANWAN) could be improved by approx. 15 %.

VoIP

→ A sudden router restart could occur if further digits were dialed while telephoning via a SIP trunk line.

→ In the menu „Voice Call Manager → Extended → Quality of Service → Prioritize outgoing packets“ the value “PMTU reduction & fragmentation” was activated by default after a factory reset, although the real default value „PMTU reduction“ should be configured.

→ A fax transmission via T.38 could fail if the RTP fax packets were smaller than the RTP audio packets, since a packet length check was done. This check is no longer done, because RTP fax packets can be smaller than RTP audio packets.

LCOS improvements 9.24.0358 PR

Bugfixes / improvements

General

→ In some cases routes with activated “sticky for RIP“ were not propagated accurately per RIP protocol.

→ SNMP access to a LANCOM router was not possible via WAN interface, if the SNMP right “read only” was configured for the WAN interface’s access rights.

→ Configuration changes in the VLAN provider table (path /Setup/WAN/VLANs/Provider-List) were activated only after a router restart.

→ The command „do /Status/Modem-Mobile/Scan-Networks“ (determine the best quality WWAN provider) could cause a sudden device restart if it was invoked by a CRON job.

VPN

→ No data was transmitted through a VPN tunnel if an IKEv2 connection was established via IPSec-over-HTTPS mode. Affected were IKEv2 connections between two LANCOM routers, and IKEv2 connections between Advanced VPN Client and a LANCOM router, too.

VoIP

→ “SIP” was written in capital letters within the URI of a SIP packet’s route header, which was not conforming to RFC and could result in calls being ended after 30 seconds.

→ On the ISDN, the LANCOM router communicated the call number from the field „P-Asserted-Identity“ as call number containing the attribute „screening indicator : user provided, not screened“. This caused these numbers being tagged as “unverified, non-serious” on some PBX systems.

LCOS improvements 9.24.0334 SU9

Bugfixes / improvements

Security update for LANCOM routers, gateways, access points, and WLAN controllers

→ This update fixes a security-related vulnerability in the management functionalities. Potentially affected are all devices running the following firmware versions:
LCOS 10.12 REL, SU1, RU2
LCOS 10.10 RU2, 10.10.0165 PR, 10.10 RU4
LCOS 9.24 RU6, SU7, RU8
This update is recommended for these devices. All other versions are not affected.

LCOS improvements 9.24.0330 RU8

Bugfixes / improvements

General

→ Packets which should be deferred by a firewall rule were transmitted if two QoS rules with activated linking were active in the firewall (“Observe further rules after this rule matches”), and the packets matched to one of these rules.

→ Two servers could not be specified as target under /Setup/DNS/DNS Destinations, if one or both were extended by an ‘@’ character. You can add a routing tag using the ‘@’ character.

→ No objects containing the ‘@’ character could be created in the firewall (LCOS menu tree: /Setup/IPRouter/Firewall/Objects; LANconfig: Firewall/QoS > IPv4 rules > Station objects), although the allowed character set included the ‘@’ character.

→ If the iperf command was entered incomplete or abbreviated on the LANCOM device’s command line (e.g. “iper” instead of “iperf”), the iperf server started displaying a warning message.

VPN

→ It was not possible to execute more than one Dynamic VPN negotiations simultaneously. Due to that, the corresponding VPN tunnels could not be established.

VoIP

→ If a VoIP configuration was written to the device using the setup wizard and a call was put through simultaneously via the still active previous VoIP configuration, a sudden device restart could occur.

→ The Voice Call Manager did not evaluate the allow headers of received SIP packets, but added his own fixed allow list when putting through a call.

LCOS improvements 9.24.0322 SU7

Bugfixes / improvements

Wi-Fi

→ A security issue within WPA2 authentication (KRACK attack) using 802.11r (Fast-Roaming) while in AP mode (base station) has been fixed:
CVE-2017-13082: accepting a retransmitted Fast BSS Transition Reassociation Request and reinstalling the pairwise key while processing it
Please check with the manufacturer of your Wi-Fi client for the availability of updates. These devices need to be updated, too.

→ A security issue within WPA2 authentication (KRACK attack) using WLAN client mode / WLAN station mode with 802.11ac-Wi-Fi modules as well as while using P2P connections with 802.11ac- and 802.11a/b/g/n Wi-Fi modules has been fixed:
CVE-2017-13077: reinstallation of the pairwise key in the Four-way handshake
CVE-2017-13080: reinstallation of the group key in the Group Key handshake
The WLAN client mode / WLAN station mode with 802.11a/b/g/n Wi-Fi modules is not affected.

Note:

LCOS is not affected by the following WPA2 security issues (KRACK attack):

→ CVE-2017-13084: reinstallation of the STK key in the PeerKey handshake
→ CVE-2017-13086: reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake
→ CVE-2017-13087: reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame
→ CVE-2017-13088: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame
→ CVE-2017-13078: reinstallation of the group key in the Four-way handshake
→ CVE-2017-13079: reinstallation of the integrity group key in the Four-way handshake
→ CVE-2017-13081: reinstallation of the integrity group key in the Group Key handshake

LCOS improvements 9.24.0314 RU6

Bugfixes /improvements

General

→ Proxy-ARP did not work for communication between identical IP networks which are managed by the LANCOM device.

→ When using a backup RADIUS server for device authentication the login was checked on the backup server first, instead on the primary RADIUS server.

→ When using the ‘sleep‘ command, only values between 5 and 7 were accepted when the units were set to hours. When using seconds as unit, values up to 900 seconds were possible.

→ If a server in the DMZ was sending too big packets (bigger than the MTU of the target remote station) with activated DF bit (don’t fragment) to a LANCOM router, the router did not answer with an ICMP error message “fragmentation needed” and discarded these packets.

→ An xDSL connection could not be stopped immediately, if the appropriate DSL remote station was detached from the configuration by script.

→ A script error occurred if the command ‘loadfile’ was invoked by a script. However, the command was executed.

→ Invoking the user-defined rollout wizard could lead to a sudden device restart, if more item values than item texts were defined in the rollout wizard’s list box.

→ If a BGP router provided a particular prefix, which was learned by the neighbor from a different source (and was propagated by the neighbor, too), a route-revoke for this prefix did not work for this BGP neighbor.

→ In a VRRP load balancing scenario with RIP, ICMP redirects were sent with the source IP address of the ARF context instead of the VRRP IP address.

VPN

→ Further IPSec rules were created if solely a super ordinate IPSec rule (e.g. ANY-to-ANY) was defined for a VPN remote station, but also one or more N:N NAT entries were defined for this VPN remote station, which included the super ordinate IPSec rule.

→ If no IPv4 address pool was created for an IKEv2 client connection, an IKEv2 client who got an IP address by the LANCOM router via IKE config mode did not get a DNS server entry. The LANCOM router allocates its own IP address as a DNS server address to the IKEv2 client if no IPv4 address pool was created.

→ If a masked IKEv2 VPN connection between two LANCOM routers was established with a one-sided transparently accessible DMZ (masking settings “only Intranet“), the DMZ was masked, too.
→ An IKEv2 connection with a digital signature profile „RSASSA-PSS with SHA-384 and SHA-512“ could not be established.
→ If only default routes with a routing tag different from 0 were configured on a LANCOM Router, IKEv2 connections could not be established, if the IKEv2 peer was not recognized by its IP address.

Wi-Fi

→ If profiles were defined under ‘Public-Spot > Wizard > Bandwidth profiles’, the according values were displayed swapped later in the wizard and on the voucher.
→ On the login page of the Public Spot gateway the page containing the terms of use could not be displayed for apple clients, if the Public Spot authentication method was set to ‘Login data will be sent by e-mail / SMS’.
→ A negative value was shown in LANmonitor for managed access points after radio field optimization on a LANCOM WLAN controller.
→ If a Public Spot was operated on a router with Wi-Fi module, and an access point within the same network broadcasted the Public Spot SSID, too, the entry for a client was deleted from the auto relogin table if the client was roaming from the router to the access point. This caused an additional login to the Public Spot.

VoIP

→ If a call group was intended to be used as a backup line, e.g. for a connection to a telephone system, this entry did not work.
→ If WEBconfig‘s “Configure Voice-over-IP / All-IP“ setup wizard was used for configuring an All-IP connection, the configured ISDN interface remained in “off” status after the wizard was finished.
→ Unidirectional communication could infrequently occur if an incoming call via SIP line was signalled by the LANCOM VoIP router to more than two interfaces (ISDN and analog interfaces).
→ After an analog call was finished, it remained in the call counter table of the LANCOM VoIP router in some cases.
→ In a phone call between a LANCOM VoIP router and a Unify SIP phone station unidirectional communication could occur if the call was continued after a ‘hold’.

LCOS improvements 9.24.0261 RU5

Bugfixes /improvements

General

→ Routes received via eBGP were preferred on path selection. The MED (Multi Exit Discriminator) was checked only afterwards.

→ If the LANCOM router had to send an „ICMPv6 packet too big“ message for packets which had to be routed to a destination interface without global address (e.g., VPN interface), this message was sent with the link local address.

→ After managed LANCOM access points received a profile from a WLAN controller, which was configured as a DHCP server, and additionally had a configured lease time smaller than default, the access points were accessible under the IP address stored within the profile, but lost their addresses after some time and remained in that state.

→ An SSH access could lead to a sudden device restart, if the SSH authentication was done with a public key, which was accepted by the device, but was sent with a signature by the SSH client, which could not be verified by the LANCOM router via public key.

→ The TFTP server in the LANCOM router could accidentally block the ports from 8192 to 16383, which could be solved only by a device restart. Therefore, problems with port forwarding for these particular ports could occur.

→ The WEBconfig setup wizard „Configure Internet access“ configured a downstream and upstream rate of 2176 kbps for the selected Ethernet interface under „Setup/Interfaces/DSL“, and an external overhead of 12 bytes, although these values had never been defined.

→ On an existing WWAN connection with network selection ‘By quality’ within the mobile radio profile the WWAN module does no longer select the previous successfully used network, but the best found network which was saved to the profile after doing a network scan using the CLI command ‘scannetworks –s‘, or using LANmonitor with the option ‘disconnect and select best network’.

VPN

→ In the IKE part of a VPN connection no CRL check was done after a configuration change, until the CRL client fetched the next CRL.

→ If an IKEv2 connection was configured with IKE-CFG mode, and the IPv4 address was configured in the IP parameter table, the LANCOM router asked for an IPv6 address when establishing a connection, although IPv6 was disabled in the configuration. Since the partner could not allocate an IPv6 address, the VPN connection was not established.

→ Usage of the CRL client could lead to a sudden device restart, if the client could not request the CRL URLs because the server could not be resolved.
→ If a disconnection request for an IKEv2 VPN connection is initiated by one station (e.g. after a configuration change), the phase-2 SA disconnect is done at both stations.
→ A simultaneous re-keying (both sites were starting the negotiation of new keys simultaneously) on an IKEv2 connection lead to the deletion of the new CHILD SAs, so that no data packets could be sent via the connection.

Wi-Fi

→ The timeline of the waterfall chart is shown again in the Spectral Scan display.
→ A LANCOM access point could send the IAPP handover request to the wrong IP address, if a LANCOM access point which was configured as a Wi-Fi client switched to another access point.
→ The counter „TX-Bytes“ and „RX-Bytes“ were not reset in time after a logout, so that a new immediate login was not possible if a configured maximum data volume („Setup/Public-Spot-Modul/Traffic-Limit-Bytes“ or „Public-Spot → Server → Access without authentication → Max. data volume) was reached. A new counter was added named „Unauthenticated-Bytes“, which shows the consumed data volume of a Public Spot user before his authentication.
→ The re-initialization trigger of the SCEP client could fail, if the client was currently initializing.

VoIP

→ If the analog port was disabled via CLI under „Setup/Interfaces/Analog“, this port could not be reenabled via LANconfig under „Voice Call Manager → User → Analog interfaces“.
→ Outgoing calls via SIP provider M-net could not be established, because the provider requires a second authentication after authentication via „INVITE“, and „PRACK“, too.
→ If identical numbers were stored in the Voice Call Manager for analog and ISDN users, and the ISDN phone was not physically connected to the LANCOM router, no “busy” signaling was reported to the SIP provider, if a call was done via analog phone, and a call was simultaneously coming in on the same number.
→ There were issues with T.38 fax transmissions on Telekom trunk lines. If the T.38 negotiation failed, there was no fallback to the G.711 protocol, and the fax transmission was aborted.

→ If a call was established via an ISDN phone system which is connected to the internal ISDN interface of the LANCOM router, and has a configured a call forwarding to external numbers, unidirectional communication could happen, if the call was finally forwarded to the provider via SIP by the VCM.

→ A SIP session which was tagged with a routing tag by a firewall rule and managed by the SIP ALG, could not be established, because the answer packets were tagged with the same tag by the SIP ALG, and thus were discarded by the IP router.

LCOS improvements 9.24.0212 RU4

Bugfixes / improvements

Network Connectivity

→ Local IPv6 networks can communicate with each other again, if one of these networks is allocated to a bridge group (e.g. BRG-1), and the other network to a logical network (e.g. LAN-2).

→ An unconfigured device in factory state can be reached within the local network by specifying an arbitrary DNS name.

→ If the device time is set (manually or by NTP server), milliseconds are reset, too.

→ An IPv6 address is generated on the WAN interface when connecting to internet providers SWN or Wilhelm-tel, too.

→ A standby device within a VRRP cluster which is addressed by a client as NTP server does not establish an internet connection if the NTP server service is enabled.

→ On a router with WAN-RIP-configured remote sites (e.g. L2TP or PPTP), an arbitrary configuration change leads no longer to a disconnect of remote sites without active RIP routes.

→ Data traffic limitation by firewall rules with trigger „per station“ works again, if a logical LAN interface (e.g. LAN-1) is allocated to a bridge group (e.g. BRG-1), and a logical LAN interface is explicitly allocated within the IP network configuration.

→ The second logical EXT interface was added to the MIB-2.

→ Devices without dual SIM do not show a second logical EXT interface in the status tree.

→ Routes which were learned dynamically via eBGP, iBGP or RIP are only added to their related routing context (routing tag) in the Fowarding Information Base (see LANCOM knowledgebase).

→ The IKEv2 dead peer detection (/Setup/VPN/IKEv2/General/DPD-Inact-Timeout) does not only work with intervals of 60 seconds.

→ IPv4 fragment forwarding (/setup/ip-router/1-N-NAT/Fragments/) with simultaneous QoS limitation is no longer classified as an attack. Communication is possible again.

→ Fixed an unexpected router restart while accessing SCEP-CA certificate information

→ Fixed the usage of a wrong certificate for WEBconfig

→ Password length can now exceed a length of 15 characters when changing the router password of a user with administrative rights.

→ The SNMP port 161 is no longer shown as closed, although SNMPv3 is allowed on the WLAN interface.
→ The services SNMPv2 and SNMPv3 can be displayed separately.
→ A CA fingerprint can now be applied to the internal LANCOM SCEP client, even if it consists of more than 59 characters.

VPN

→ An IKEv2 VPN connection is not disconnected after a while, if the dead peer detection (DPD) cannot detect a connection to the VPN remote site due to a no longer existing child SA.
→ An L2TP tunnel which was configured on one site only does not lead to a disconnect of an active second L2TP tunnel between the two routers.
→ A configuration change by use of the sleep command caused by a script does not lead to a disconnect of an IKEv1 IPSec tunnel which cannot be established again.
→ A „default -r“ within a script does no longer cause a VPN tunnel to not being established.
→ If a LANCOM Router has accepted an IKEv2 connection via LAN, the connection is also established if the routing tag of the source address is 0.

Wi-Fi

→ RADIUS authentication (IEEE 802.1x) of Wi-Fi clients in a WLC scenario is no longer aborted with the error message „missing private key“.
→ Public spot authentication of a disabled user account by the „Manage Public Spot Users“ wizard is no longer possible, even if the user is listed in the auto ReLogin table.
→ Access points can again connect via auto WDS, even if the applying frequency band within the WDS profile is set to “only 5GHz“.
→ In a public spot scenario with PMS connection the link for authentication via voucher is available again, even if the language settings of the Wi-Fi client are set to French or Italian.
→ Fixed an unexpected router restart which was caused by usage of the public spot user table (/setup/public-spot-module/user-table).
→ When printing a voucher again from within the public spot user management wizard the volume budget is displayed accurately on the integrated device templates.
→ The IPv6 data communication over a WLC tunnel between a Wi-Fi client and a LANCOM Wi-Fi controller works again.

VoIP

→ Fixed an unexpected router restart when transferring a DNS resolution to the Voice Call Manager (VCM)

→ A configuration update of the DECT base station LANCOM DECT 510 IP works after an address change of the provisioning update server (/Setup/Provisioning-Server). The base station is now provided with the information of an update URL change.

→ Identical SIP users can be handled by multiple handsets registered to the same base station.

→ DECT base stations are no longer listed with wrong IP address within the status table. The related LANmonitor display error is fixed.

→ After software reboot (warm start) a connection to the SIP server can be established again, even when using an external SIP trunk line. A power disconnect (cold boot) is no longer necessary.

→ When using a SIP trunk line, the „to“ field within the SIP header is now converted properly to the E.164 format.

→ With two configured SIP trunks it is now possible again to pass a call from one of the SIP trunks to a single SIP line account.

→ The „Registered Mode“ for a Telekom SIP trunk is now active by default within the ALL-IP wizard.

LCOS improvements 9.24.0153 RU3

Important notice to the update:
By default, SNMP access is disabled via WAN interface. If WAN access for SNMP was activated manually by configuration, access to SNMPv1 / SNMPv2 must be activated manually after the firmware update. The previous configuration setting for SNMP is retained for SNMPv3.

Bugfixes / improvements

Network Connectivity

→ Fixed an issue which led to noise interference on clearmode connections

→ Fixed an issue with noise interference on outgoing SIP calls

→ WLC script rollout works again

→ Improved IKEv2 re-keying

→ IKEv2 VPN connections are established reliably.

→ SIP phones can register to a superordinate VoIP phone system via SIP-ALG again.

→ Outgoing calls can be established via the designated line if more than one SIP trunks or single accounts are configured.
→ Unnecessary Wi-Fi modem load information have been removed from the bootlog.

Wi-Fi

→ The confirmation page after a successful login is hidden earlier.
→ Fixed a problem where no client could connect to a wireless network.
→ Stability improvements for 802.11ac P2P Wi-Fi connections

LCOS improvements 9.24.0076 RU2

Important notice to the update:
By default, SNMP access is disabled via WAN interface. If WAN access for SNMP was activated manually by configuration, access to SNMPv1 / SNMPv2 must be activated manually after the firmware update. The previous configuration setting for SNMP is retained for SNMPv3.

Bugfixes / Improvements

Network Connectivity

→ Reliable initialization of the integrated VDSL modem in particular situations

LCOS improvements 9.24.0075 RU1

Important notice to the update:
By default, SNMP access is disabled via WAN interface. If WAN access for SNMP was activated manually by configuration, access to SNMPv1 / SNMPv2 must be activated manually after the firmware update. The previous configuration setting for SNMP is retained for SNMPv3.

Bugfixes / improvements

Network Connectivity

→ The access rights for SNMPv2 can be switched separately now.

→ Fixed a problem that led to a non-working HTTPS communication from an Apple device with iOS 10 or macOS 10.12 to a LANCOM.

→ A problem with the LANCOM DECT 510 IP has been fixed.

LCOS improvements 9.24.0070 Rel

New Features

Network Connectivity

→ Auto provisioning support for LANCOM DECT 510 IP
→ Support for Call-Forking within the Voice Call Manager
→ Support for SIP methods PRACK and UPDATE
→ Support for Message Waiting Indication within the Voice Call Manager
→ The available Rx/Tx bandwidth can be configured manually for routers with integrated ADSL/VDSL modem.

Wi-Fi

→ Predefined bandwidth profiles for Public Spot
→ Support for RADIUS CoA (Change of Authorization) within the Public Spot

LCOS improvements 9.20.0683 RU2

Important notice to the update:
The Loader 4.18 has to be flashed before updating the firmware of the LANCOM 1631E, LANCOM 831A and Business LAN R800A to LCOS 9.20.

Bugfixes / improvements

Network Connectivity

→ Fixed a problem within the jitter buffer which led to a fax transmission abort.
→ Access attempts to certain WEBconfig configurations no longer trigger a device restart.
→ To avoid server problems, the HTTP client reads the complete server reply when authentication is needed before another request is started.
→ IKEv2 VPN with NAT traversal works as designed.
→ Fixed a problem with codec selection if a phone is directly connected to the LANCOM.
→ Clip no Screening works again as desired, if a telephone system is connected to the LANCOM via S_0 interface.

LCOS improvements 9.20.0647 RU1

Important notice to the update:
The Loader 4.18 has to be flashed before updating the firmware of the LANCOM 1631E, LANCOM 831A and Business LAN R800A to LCOS 9.20.

Bugfixes / improvements

Network Connectivity

→ As of now, BGP packets are marked with DSCP CS6.
→ Dial-up routes with simplified certificates for IKEv1 are set correctly.
→ The table for automatic VLAN provider selection can be edited.
→ DiffServ tags from inner tunnels as PPTP, L2TP, GRE or EoGRE are now applied to the outer VPN tunnel.
→ Improvements in IKEv2 re-keying
→ Interoperability improvements for TLS 1.2 connections
→ RIP propagates a conditional route if the remote station is connected.
→ ICMP polling works again with loopback addresses.
→ Fixed the active calls counter within the voice call manager.
→ LANmonitor displays the firewall rule of the first matching action.
→ No syslog message is sent if a broadcast is received and rejected on the LAN interface.
→ SMS can be sent and deleted via LANmonitor.
→ Improvements in SIP-ALG in conjunction with Mitel telephone systems. OPTIONS packets are sent from the correct port.
→ Fixed a problem with SIP ALG.
→ Fixed an issue where routing between local networks in conjunction with policy based routing did not work.
→ A forwarded call from an analog phone does not lead to unilateral voice transmission.
→ The rollout agent starts a rollout even if a config server URL is not transmitted via DHCP-Option 43, but instead is provided within the device configuration.
→ Fixed issues in conjunction with Swyx (CTI+, call forwarding, etc.)
→ Support for 1TR114 SIP methods PRACK und UPDATE by Deutsche Telekom vSDP
→ VLAN assignments per ISP are now possible.

Wi-Fi

→ OAP-830: The internal assembly of the Wi-Fi modules has been swapped to improve Wi-Fi performance. When running point-to-point connections with the OAP-830, please consider the following knowledge base article: https://www2.lancom.de/kb.nsf/0/2FD8349316D983AAC1257FF0002F850D?opendocument

→ Fixed a problem where remotely managed access points did not receive the configuration from a WLC if the WAN link MTU was too large.

→ An access point in client mode within an 802.11ac connection can re-connect to a base station.

LCOS improvements 9.20.0566 Rel

Important notice to the update:
The Loader 4.18 has to be flashed before updating the firmware of the LANCOM 1631E, LANCOM 831A and Business LAN R800A to LCOS 9.20.

Bugfixes / improvements

Network Connectivity

→ a Fixed a problem with T.38 fax transmission
→ a If the WEBconfig All-IP wizard is started a second time, all previous settings are replaced as expected
→ a PPTP tunnels are re-established after an item is added to the backup table
→ a Fixed a problem with enforced bandwidth reservation

Wi-Fi

→ Clients with an Intel AC-7260 chipset can connect to an Access Point running in „ac only“ mode.
→ Authentication via 802.1x under occurrent high packet load works again with 11ac access points.
→ CAPWAP does not set any host routes to targets within the local network, if a static IP address was allocated by a WLC.

LCOS improvements 9.20.0517 RC2

Important notice to the update:
The Loader 4.18 has to be flashed before updating the firmware of the LANCOM 1631E, LANCOM 831A and Business LAN R800A to LCOS 9.20.

Bugfixes / improvements

Network Connectivity

→ Fixed an All-IP wizard bug where not all entries were deleted as desired.
→ If an L2TP remote station is disconnected, the according RIP routes are no longer provided.
→ After a fallback to 2G the router does not remain in Edge mode permanently.
→ The iPerf server daemon is accessible via VPN, if WAN access is limited to VPN.

→ Fixed a problem where a SIP line could not register due to missing DNS resolution.
→ SIP packets bigger than 1024 bytes are no longer cut.
→ The iPerf server report can be received by the iPerf client if client packets contain a VLAN tag.
→ If a call is put on hold, music on hold playback is correct.

Wi-Fi

→ Location Based Services (LBS) is no longer configurable on devices without Wi-Fi or WLC option.
→ Public Spot template preview is visible only if a Public Spot option exists on the LANCOM device.
→ A configured Public Spot login text is displayed correctly.
→ Reduced menory usage with enabled aggregation and 802.11n modules.

LCOS improvements 9.20.0385 RC1

Important notice to the update:
The Loader 4.18 has to be flashed before updating the firmware of the LANCOM 1631E, LANCOM 831A and Business LAN R800A to LCOS 9.20.

New Features

Network Connectivity

→ Support for automated rollout via DHCP option 43
→ The SCEP client obeys certificate dependencies.
→ Support for DTMF conversion for All-IP
→ Support for SNMPv3
→ The Voice Call Manager supports now TCP for SIP connections.
→ The Voice Call Manager supports now Voice over Secure IP (SIPS/SRTP).
→ The amount of detected devices is shown with ll2mdetect.
→ The ADSL/VDSL state displays modem sync duration and connection count.
→ NTP client and server support IPv6
→ Option for changing EAP-TLS settings, if the LANCOM device works as 802.1x supplicant.
→ Support for IKEv2
→ Support for BGP v4

→ The device status display shows an active backup connection and the number of established backup connections.
→ A backup can be triggered if a memorized route is no longer available (Route Monitor).
→ The IPv6 firewall rule „Allow-IPSec“ is enabled by default.
→ Using syslog, DNS requests can be forwarded to an external syslog server.
→ LCOScap supports IPv6
→ Support for IPv6 VPN with IKEv1
→ A Syslog server can be enregistered as DNS name or IPv6 address.
→ SIP messages can be set to be only accepted from the SIP registrar.
→ Overlap dialing support for SIP trunks
→ WAN connection prio tags are taken over to the VLAN header according to 1TR-112 or DSCP.
→ Extended support for TR.069 and TR.181
→ The syslog shows the reason for a denied RADIUS server authentication request.
→ Support for ChaCha20-Poly1305 for SSH
→ CA support for SCEP message GetCaCaps
→ Adapted IKE and PFS default groups to DH group 14 within VPN
→ Registered SIP users are not deleted on configuration changes.
→ Support for ISDN parallel calls
→ Support for IPerf as server and client
→ Switchable configuration protocols
→ Added an open ports display in WEBconfig under the „Services“ tab
→ Powersaving for ethernet interfaces is enabled by default
→ Removed the VLAN tagging mode „Incoming mixed“
→ DHCP lease time is configurable per network
→ Password complexity for the main device password and further administrators can be forced.

Wi-Fi

→ IAPP is disabled if a CAPWAP tunnel is active
→ Support for Airtime Fairness
→ Radio-field optimization can be done on autonomous Access Points.
→ Multiple AutoWDS profiles can be configured on a WLC.
→ Support for Adaptive RF Optimization
→ Support for Wireless Intrusion Detection System (WIDS)
→ Average Wi-Fi error rates of particular Access Points can be read out on a WLC.
→ Using the URL variable „%r“, the MAC address of the Access Point to which a client is authenticated can be transmitted in a Public Spot redirect.

→ Specified data rates can be configured per SSID.
→ The Public Spot function „Accept Terms and Conditions“ is utilizable when using PMS.
→ The displayed columns can be configured within the Public Spot/Manage User wizard.
→ Surplus blank characters while typing usernames and passwords are removed automatically.
→ The assigned bandwidth profile for a Public Spot user can be shown on the voucher.
→ Brute Force protection can be realized by configuring a login blocker.
→ Added a switch to forward HTTPS connections from unauthenticated clients to the Public Spot gateway.
→ Added an option to preview the uploaded Public Spot templates via WEBconfig
→ Support for Spectral Scan for 802.11ac Wi-Fi modules
→ Improved Wi-Fi rate adaption
→ The current channel width and used MCS are now displayed in the Wi-Fi interpoints table and in the station table.

Bugfixes / improvements

Network Connectivity

→ Fixed a bug which led to a router restart when viewing the SMS inbox via WEBconfig.
→ Fixed a DNS resolution problem where an explicit DNS forwarding configuration was needed.
→ Port forwarding of VPN ports 500 and 4500 works again
→ Fixed the firewall packet action „Only when default route“.
→ Variable „DEVICE_URL“ works again when used with the „loadscript“ command.
→ If a VPN tunnel is established via DynDNS names, the name is re-resolved immediately after a disconnect, so that the tunnel is not established to the previous address.
→ A SIP phone call via SIP-ALG, which uses PRACK, is no longer disconnected.
→ The Internet configuration wizard sets the correct netmask within WEBconfig.
→ Fixed a problem which led to a router restart due to lack of memory.
→ A dynamic VPN connection can be established via Load Balancer.
→ The time display within the IPerf status table is shown more noticeable.
→ Outgoing SIP Trunk lines of a phone system via SIP-ALG are no longer disconnected.
→ Corrected the negotiated WAN interface MTU for IPv6.
→ Fixed a bug which prevented a 4G backup connection establishment.

Wi-Fi

→ Fixed a problem that only particular clients could authenticate to an 802.11ac accesspoint.

→ Fixed a bug which led to a several minute lasting inaccessibility of an accesspoint in client mode while roaming between base stations.

→ Configuration can be written again to devices with less memory.

→ Check of the DNS server response is now case insensitive.

→ Fixed a certificate error when an accesspoint tries to connect to a WLC.

5. 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.