LANCOM Release Notes

LCOS

10.32 RU10

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

Internet: http://www.lancom-systems.com

June 16th, 2020, MKoser

Table of Contents

LANCOM Systems

Table of Contents - continued

1. Preface

LCOS („LANCOM Operating System“) is the established LANCOM operating system for LANCOM routers, wireless LAN access points and WLAN controllers. In the context of the hardware given by the products the at a time latest LCOS version is available for all LANCOM products and is available free of charge for download from LANCOM Systems.

This document describes the innovations within LCOS software release 10.32 RU10, as well as the improvements since the previous version.

Before upgrading the firmware, please pay close attention to chapter 6 “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. Device-specific compatibility to LCOS 10.32 / 10.30

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

As from LCOS 10.30, support for the following devices is discontinued

- LANCOM 831A
- LANCOM IAP-322
- LANCOM L-451agn
- LANCOM L-452agn
- LANCOM L-460agn
- LANCOM OAP-3G

3. Advices regarding LCOS 10.32

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.

4. Feature overview LCOS 10.30

4.1 Feature highlights

SD-WAN – Application Routing

Enjoy significant performance gains when you operate modern business applications in the cloud (e.g. Office 365, SalesForce, etc). SD-WAN Application Routing detects cloud-based applications and routes them directly to the Internet (local break-out). This relieves the VPN path to the headquarters as well as the headquarters' Internet line.

SD-WAN – Layer-7 Application Control in the firewall

Keep control of which applications can operate on your network. Defining application-related rules in the firewall allows you to decide which Internet applications are allowed, blocked, limited or prioritized.

WLC functions in the vRouter (vWLC)

You decide which role your LANCOM vRouter should play: VPN gateway or WLAN controller. The LANCOM vRouter now supports the role of a virtual WLC (vWLC). This fully virtualizes the functions of a WLAN controller on virtualization platforms such as VMWare ESXi or Microsoft Hyper-V. The number of managed access points depends on the vRouter license category.

4.2 Further features

TLS 1.3

Support of the new TLS 1.3 protocol increases the security of device access via WEBconfig.

Elliptic Curve Digital Signature Algorithm (ECDSA)

IKEv2 now supports the Elliptic Curve Digital Signature Algorithm (ECDSA) authentication method. Shorter keys combined with high-efficiency encryption provide the same security.

IKEv2 split DNS

Split DNS allows DNS to resolve specific internal domains to a VPN tunnel, with other DNS requests using a public DNS server.

IKEv2 fragmentation

Fragmentation of IKEv2 messages (per RFC 7383) is handled by the VPN router itself, eliminating the need for the transport network to fragment IKE packets.

Enhanced client reservations in the DHCPv6 server

In the DHCPv6 server, client addresses or prefixes can now be assigned either by means of DUID, MAC address, interface ID (as per RFC 3315) or remote ID (as per RFC 4649).

Double the number of Public Spot users

For the LANCOM 178x and 179x series with the Public Spot Option, the number of users is increased from 64 to 128.

You can find further features within the individual builds sections in chapter 5 “History LCOS 10.32 / 10.30”.

5. History LCOS 10.32 / 10.30

LCOS improvements 10.32.0183 RU10

Bugfixes / improvements

General

- The configuration could not be rolled out to a router managed by the LMC if a new object was created in the DNS target list at the same time and this object was referenced in a new firewall rule.
- Layer 7 application detection did not work if it was restricted to a specific VLAN using the associated VLAN table (Setup/Layer-7-App-Detection/VLAN/).
- The router would restart abruptly if a DNS forwarding was deposited with an @ followed by a remote peer name instead of a routing tag. Only routing tags may be stored.

VPN

- If a new VPN dial-in access for the Advanced VPN Client was created in WEBconfig with the setup wizard "Provide remote access (RAS, VPN)", this resulted in existing dial-in accesses being deleted by the Advanced VPN Client.

Wi-Fi

- In the LANCOM OAP-170xB series devices, negative temperature readings from the temperature sensor were incorrectly handled, which could lead to a Wi-Fi module being switched off due to an incorrectly determined temperature value.
- When using the Fast Roaming feature, it was possible that when transferring the PMK via IAPP, the PMK was only transferred to the PMK cache of a BSSID. On an access point with two Wi-Fi modules, where the same SSID was broadcast on both modules, this caused the fast transition to be rejected with the error message "R0KH unreachable".
- If an access point was located in a network that was not configured locally in the WLAN controller (e.g. connected via VPN), it could happen in individual cases that the WLAN controller responded to requests from the access point with an IP address from another network.
  This meant that the access point could not be managed by the WLAN controller.
- A sudden restart could occur if the access point performed a scan of the WLAN channel before a DFS CAC (Channel Availability Check) and the timer ran out before the WLAN card reported the end of the scan.
- Transmission errors could occur with ePaper when transmitting very small contents (transmission time less than one second) if the display update was prolonged due to interference on the ePaper radio module because of transmission repetitions. As a result, the update of the next display by the ePaper server had to be rejected and rescheduled. If the end of the display update and the next scheduled update coincided, the update was not rejected but sent to the next display with a scheduled update

VoIP

- If a SIP response code unknown to the router was received (e.g. "101 Connected"), this was interpreted by the router as an error message and the call was terminated.
  All unknown SIP response codes are now treated as a message with the response code "100 Trying".
- An instant reboot could occur if an UPDATE request without via header was received.
- In a scenario with a VoIP router to which an analog subscriber was connected, it could occasionally happen that the caller (external subscriber) could only understand the called party (analog subscriber) very poorly during an incoming call because the volume of the analog subscriber was very low.

LCOS improvements 10.32.0176 RU9

Bugfixes / improvements

General

- A potentially security relevant cross-site scripting issue has been fixed that allowed JavaScript code to be executed from the LANCOM Public Spot login page. If such code was used, information could be infiltrated which could be used to attack a Public Spot user's system via a manipulated link.
- Previously, the LANCOM RADIUS server was unable to check the certificates of WLAN clients in 802.1X scenarios with external OSCPs or CRLs. This option is now available. The RADIUS server now first stores the various information of a client certificate and restores it if the OSCP response was positive.
- When using a vRouter under HyperV, checksums were sporadically miscalculated.
- With a high volume of TLS packets destined for the device, a sudden restart could occur in individual cases if the responsible packet buffer was full.
- It could happen sporadically that a finished call via the Voice Call Manager was not completely cleaned up, so that this led to a sudden device restart when the call was reestablished.

VPN

- If another remote identity was stored for an IKEv2 connection and a different authentication method was selected for this connection (e.g. RSA and PSK), the IKEv2 negotiation failed.

Wi-Fi

- If the setup wizard 'Configure Wi-Fi' was run on a LANCOM IAP-821, and the Wi-Fi operating mode was set to 'Client', and the feature 'Soft Roaming' was deactivated, the system restarted immediately after the setup wizard was completed. If a configuration file was uploaded to a LANCOM IAP-821 with soft roaming deactivated, a sudden restart also occurred.

LCOS improvements 10.32.0170 RU8

New features

- Support for OCSP checking of EAP-TLS certificates in the integrated RADIUS server

Bugfixes / improvements

General

- If in the table 'IPv6 Forwarding Rules' one or more self-created station objects were defined as source or destination, the configuration could not be written back to the device.
- If an interface tag was assigned to a network, sending a DNS request from that network to another non-local network by the router itself (for example, by pinging a DNS name using the console command 'ping -a' from the router) could result in a network with network type DMZ as the source network. This was caused by not taking the source tag into account and thus only the destination tag of the routing entry was used.
  Furthermore, networks of type DMZ were erroneously treated equally to networks of type INTRANET and the sorting of the networks was not purely dependent on the name, but partly also on the memory address. This could lead to DNS resolution not working if the DNS server could be reached over a VPN connection and the source network used could not communicate over the VPN connection due to missing VPN rules. Communication with the destination was not possible via the DNS name.
- If the path '/Setup/SNMP' was synchronized via an HA cluster, no configuration could be written to the slave device via LANconfig after synchronization.
  The reason for this behavior was that this SNMP table was read out incorrectly at one position and a wrong value was entered there.
- After activating the logging of DNS requests on an external syslog server, a sudden restart of the router occurred if a DNS response to a SOA or NSEC record was received as an 'unknown' record, because in this case an incorrect class was used in the processing by the DNS service.

VPN

- In large scenarios with multiple VPN concentrators, when using IKEv2 dial-up connections, it could occasionally happen that the VPN connection was not terminated correctly in the central site if the dial-up router (initiator) lost its VPN connection (e.g. after a DPD timeout or forced disconnection of the Internet connection).
  If the retry was made with another VPN concentrator in the central site, the connection on the first concentrator remained in the 'Connect' state, which caused a route to be propagated when using a routing protocol (e.g. BGP) that referred to a VPN connection that no longer existed.

Wi-Fi

- Due to a firmware-internal communication problem between the Wi-Fi of a device and its RADIUS client, a firmware update from LCOS 10.32 Rel to LCOS 10.32 from version RU5 onwards could lead to an unexpected

restart of the device.

- After a script rollout to managed access points via a WLAN controller, if the command 'show script' (rollout check) was entered on the command line while the script was still being executed, a sudden restart of the access points was reproducible.
- Until now, the LANCOM RADIUS server was unable to check the certificates of Wi-Fi clients in IEEE 802.1X scenarios with external OSCPs or CRLs. This option is now available, ensuring that withdrawn certificates can no longer be used.

VoIP

- In a scenario with a Netphone/Swyx PBX, an incoming call to one SIP subscriber with subsequent forwarding to another SIP subscriber resulted in a termination of the call after 15 seconds. The reason was that the LANCOM router did not respond to the provider's '200 OK' message with the message 'ACK' and the provider therefore terminated the call.
- In a scenario with SIP line and connected DECT station, a sudden restart could occur when rolling out a configuration via the LMC because the provisioning server for the DECT station and the config rollout service of the LMC blocked each other.

LCOS improvements 10.32.0164 RU7

Bugfixes / improvements

General

- If a LAN connection to a switch was physically removed (by pulling the Ethernet connector on the router or switch), the LANCOM router correctly called back the associated LAN network via RIP, but it was not republished after the LAN connection was restored.
- If SLA monitoring was configured on a LANCOM router, unplugging an Ethernet connector could cause the router to restart immediately.
- If the transmission modes 'UMTS(3G)+GPRS(2G)' or 'GPRS(2G)' were set in the mobile radio profile for the LANCOM 1780EW-4G+, 1793VA-4G, and 1790-4G devices, the devices always used LTE(4G) because the mobile radio module installed in these devices does not support the GPRS(2G) transmission mode.
  The devices now establish a connection to the 3G network.
- In individual cases, accessing a LANCOM router via WEBconfig using the TLS 1.3 protocol could result in a sudden restart.
- When writing data to the flash memory of a device, a sudden restart could occur sporadically if the write operation was performed at the same time as a cleanup operation started by an LCOS job (so-called 'garbage collection').
- If port forwarding was set up and activated on a vRouter for UDP port 500 (IKE), the vRouter itself could no longer establish a VPN connection.

VPN

- In big scenarios with multiple VPN concentrators, when using IKEv2 dial-up connections, it could occasionally happen that the VPN connection was not terminated correctly in the central site if the dial-up router (initiator) lost its VPN connection (e.g. after a DPD timeout or forced disconnection of the Internet connection).
  If the retry was made with another VPN concentrator in the central site, the connection on the first concentrator remained in the 'Connect' state, which led to a route being propagated when using a routing protocol (e.g. BGP), which referred to a VPN connection that no longer existed.

Wi-Fi

- In 2.4 GHz operation (802.11g/n mixed), Wi-Fi management packets for the announcement of the SSID and acceptance of Wi-Fi devices (so-called 'beacons') were sent at a data rate of 1 Mbps instead of 6 Mbps.
  Due to the significantly higher number of packets, the channel load increased sharply and could thus lead to lower achievable data rates in the wireless network.

VoIP

- During an incoming call the contact header was not included in the '180 Ringing' to the provider. This resulted in an external caller not hearing any ringing on MagentaZuhause Regio connections.
- The Voice Call Manager forwards the SIP header information of connected SIP PBXs or SIP clients to the SIP provider. If the SIP provider expected the 'Require: timer' flag in the SIP header of the '200 OK' and this flag was not set by the SIP PBX or a SIP client, the call was ended with a 'BYE' by the provider.
  The 'Require: timer' flag is now always set in the SIP header of the '200 OK' if the provider supports the 'timer' flag and the 'Session Expires' header is available.

LCOS improvements 10.32.0161 RU6

Bug fixes / improvements

General

- Port forwarding did not work with the vRouter if a map port was used which did not match the specified port.
- On a vRouter with configured port forwarding for TFTP GRE packets could not be allocated to the PPTP session. As a result, GRE packets were not forwarded and port forwarding for a PPTP connection did not work.
- If the vRouter was operated on a Hyper-V system or Microsoft Azure, packet loss could occur when sending multiple big aggregated packets. Furthermore, a packet buffer was filled up and no longer cleared.
  This could generally lead to transmission issues. Particularly on VPN connections the IKE negotiation and data transmission was faulty after some time.

VPN

- If an IKE packet had to be retransmitted while negotiating IKE on a router, the router sent the message 'ICMP Port Unreachable' immediately after retransmission.

LCOS improvements 10.32.0157 RU5

Bug fixes / improvements

General

- In the LANCOM 883+ VoIP the option to configure the AiRISTA Flow blink mode (path /Setup/Wlan/Blink mode/) was missing. As a result, the device could not be added to the LANCOM Management Cloud and an error message occured after the configuration change.
- If the local IP address of a LANCOM device was changed by the setup wizard "General settings", the device was not accessible under the new IP address after writing back the configuration because LANconfig did not receive the confirmation about the saved changes.

LCOS improvements 10.32.0156 RU4

New Features

General

- The execution of the DHCP server ARP request is now configurable.
- Propagating the default route can now be configured for BGP.
- The provider VLAN table has been extended by MagentaZuhause Regio.

Wi-Fi

- Support for Wi-Fi Alliance Passpoint® (Release 2)

Bug fixes / improvements

General

- A device restart could occur if the LANCOM router was accessed by the LANtools during an ISDN phone call.
- If a terminal device (e.g. network printer) sent a BOOTP request to a LANCOM router in forwarding mode in addition to a DHCP discover request in order to obtain an IP address, the DHCP reply of the answering DHCP server was discarded because the answer to the BOOTP request was expected. As a result, the terminal device could not obtain an IP address.
  BOOTP packets are now discarded once a DHCP discover is received from the terminal device.
- Adding and saving firewall rules via WEBconfig failed on LANCOM routers and access points. Furthermore, the device could not be restarted via WEBconfig.
- A sudden router restart could occur if a packet should be sent per L2TP while reconfiguring the device by script and closing all connections.
- The client binding table had been missing in the LCOS path "/Status/IP Router/Loadbalancer".
- SNMP traps with SNMPv1 / SNMPv2 have always been sent with community 'Public'.
- When creating new LEPS-U users on a WLAN controller a sudden device restart could occur independent from the number of created users.
- In a VRRP scenario with a VPN connection to another location it could happen that the VRRP slave established the VPN connection simultaneously to the VRRP master using the local IP address of the VRRP slave as the source IP address and sending the VRRP packets via the VRRP master.
- If the OSPF instance had been allocated a routing tag different from 0, the LANCOM router displayed the message 'No valid OSPF instance for routing tag 0', which led to the effect that no rules could be learned by OSPF.
- When using OSPF and activating the function 'Redistribute connected' via the table 'Connected' host routes were propagated, too. In conjunction with 3rd-party routers this led to ASBR routes being discarded by these routers which resulted in an inconsistent state.
  The following host routes are no longer propagated by OSPF:
  - /32 Connected LAN
  - /32 Connected WAN

  - Local WAN (all)
  - Local LAN (all)
  - DHCP (all)
- Invoking websites per HTTPS did not always work when using the Content Filter, if the Content Filter's destination cache renewal failed.
- The TR-069 protocol parameter "CWMPEnable" was missing for the LANCOM devices of the R88x series.
- With a configured ICMP SLA monitoring for performance monitoring of WAN- or VPN connections, allocated routing tags were not considered. As a result, routing tag '0' was used all the time.
- The TR-069 user agent did only contain the value 'LANCOM'. This value has been extended by device type and used LCOS version (e.g. „LANCOM 1781EW+/10.32.0152").
- No NMEA GPS data could be obtained from the LANCOM 1780EW-4G, because this function was not implemented to LCOS for the built-in radio module (MC7304).
- For routers of the 190x series a connection loss could occur on the combo port (WAN-1) when using a plain Ethernet connection if a parameter was modified in LANconfig and written back to the device.

Wi-Fi

- If the Wi-Fi module of a LANCOM access point was operated in client mode it could happen that the module stopped working after some time. LANmonitor then displayed the status 'None'.
- Due to a faulty value response of the access points to the WLAN controller it could happen that the SSID activation per CRON job for all access points did not work on the WLAN controller.

VoIP

- If outgoing calls were carried on to a 0800 calling number, these calls were terminated after 45 minutes.
- When using SNOM IP phones call terminations could occur when trying to use configured call forwarding on the phone via SIP 302.

LCOS improvements 10.32.0093 SU3

Bug fixes / 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

LCOS improvements 10.32.0092 RU2

New features

General

- The IPv4 firewall now supports an automatic forwarding / NAT of a GRE tunnel between the local network and a WAN connection.

Bug fixes / improvements

General

- If a "Deny all" rule was configured in the firewall of a LANCOM router, and an "Allow" rule was created for the communication between the VPN client and the local network with the name of the VPN remote site specified as source, no communication was possible via the VPN tunnel.
- The configuration tree "/Setup/SIP-ALG" was missing for the devices ISG-1000 and ISG-4000.
- In a BGP scenario where a route was learned by a LANCOM Router for being forwarded to another router, the AS number of the original router was not replaced by the own AS number. Instead, the AS_PATH contained both AS numbers.
- When using route redistribution in OSPF, the following route sources from connected networks are no longer propagated: Local LAN, Local WAN, DCHP, /32 Connected LAN, /32 Connected WAN.
- In an OSPF scenario with activated route distribution it could happen that LSAs were outaging from the database instead of being renewed if a LANCOM router had been allocated its own LSAs (this could happen after a restart,

for example).
This resulted in all routes learned by OSPF being lost after some time, and thus no communication was possible anymore.

- If the internal SMS management did a request on the network status exactly in the moment when the mobile radio module was disabled, this caused an unexpected restart.
- When receiving a DHCP server identifier (DHCP option 54), a DHCP client has to send a RENEW and a REBIND to the DHCP server identifier instead of the server from which the ACK has been received. When renewing the IP address, the LANCOM router sent the RENEW to the server from which the ACK had been received, which resulted in not being able to obtain an IP address.
  This caused Internet connection losses when the DHCP lease had expired.
- In a scenario with a /31 subnet mask (RFC 3021), in which the router's IP address was the broadcast address, too, several services did not work (e.g. ARP and DNS).
- When editing the field "Backup table" in the WEBconfig menu"Communication/Call Management/Backup table", a comma was used as a separator for multiple remote stations. However, this character was not permissible for the backup table within LCOS. As a result, the modified entry was not saved to the configuration.
- If the function "Secure terminal access" was used for accessing a LANCOM router or access point from the LANCOM Management Cloud, the device's event log displayed the access type "Outband" instead of "LMC".
- If two OSPF sessions were created whith identical routing tag, an unexpected restart could occur.
  As of now, an error message will be displayed within the OSPF trace, indicating that only one OSPF session is allowed per routing tag.

VPN

- VPN certificates have not been initialized when the VPN module was disabled.
  This resulted in not being able to establich the VPN connection after activating the VPN module.

Wi-Fi

- If a Wi-Fi point-to-point connection in exclusive mode has been created on a Wi-Fi router or access point by using the setup wizard, and the setup wizard has been started afterwards for configuring the public spot and creating a Wi-Fi network, an unexpected device restart occured.
- If a Wi-Fi device sent faulty parameters within the DSSS set, it could not connect to a hidden SSID of a LANCOM Wi-Fi router or access point. These parameters are ignored now.
- If in a Wi-Fi point-to-point scenario with 802.11ac Wi-Fi module devices the Wi-Fi module of the master was disabled (e.g. at a device restart), the point-to-point connection did no longer work until the slave's Wi-Fi module has been restarted.
- No Wi-Fi point-to-point connection could be established by Auto WDS.

VoIP

- A delayed call forwarding did not work because the forwarding timer was stopped too early.
- If, after an INVITE to a no longer existing call, the LANCOM router received the message "200 OK", the Voice Call Manager answered with the message "481 Call/Transaction Does Not Exist".
  The Voice Call Manager now answers with an ACK, and sends a BYE afterwards.
- An unexpected router restart could occur if a SIP client forwarded an accepted call which came in through the SIP provider to a further external subscriber.

LCOS improvements 10.32.0023 RU1

Bug fixes / improvements

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 10.32.0021 Rel

New features

General

- Support for the SSH hostkey processes rsa-sha2-256 and rsa-sha2-512 (RFC 8332).
- For SNMPv3 passwords a predefined password guideline can now be forced optionally with a configuration switch.

VPN

- For IKEv2 preshared keys a predefined password guideline can now be forced optionally with a switch in the general IKEv2 configuration.

Wireless ePaper

- Support for the ThinAP 2.0 protocol for connecting wireless ePaper access points to a central wireless ePaper server
- Support for the LANCOM Wireless ePaper USB

Bug fixes / improvements

General

- In the LANCOM 1790-4G, 1790VA-4G, and 1793VA-4G device configuration a print server was existing, although these devices are not equipped with a USB port for connecting a printer.
- While checking packets within the DNS server error messages and not working DNS requests could occur if the packet lenght of the DNS request was changed by another network component.
- If remote stations in an iBGP environment should be established or disconnected according to learned routes, this only worked once. On all further attempts no disconnect could be executed.
- If the names of the mobile radio profile, communication layer, and remote station were not identical for a mobile radio connection which was used as a backup, the connection could not be established in backup case.

VPN

- On IKEv2 connections UDP packets for a NAT keepalive contained a non-required "Non ESP marker". As a result, these packets were discarded by VPN products of other manufacturers, which, however, had no negative impact on the VPN connection quality.
- If two certificate-based VPN connections were existing, and both certificates had the same „Common Name (CN)", only the connection which was configured first could be established.
- VPN connections with IPSec encapsulation could lead to an unexpected router restart.

Wi-Fi

- After activating the LANCOM WLC Basic demo option on a compatible device the certification authority (CA) was set to non-selectable after the obligatory device restart and could not be activated within the configuration.
- When allocating IP parameter profiles via vWLC the IP addresses from the profiles were transferred to the access points in reverse order. This resulted in no access to the access points.
- When configuring static WLAN controllers in the menu "Wireless LAN / WLC / WLAN Controller" it could happen that a different locally configured network was used, although a sender address was specified. So no connection to the WLAN controller could be established via a VPN tunnel due to missing network relations (SAs).
- 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

- It could happen that an incoming call was terminated after 30 minutes, if the calling party did not use session timers. This led to a timer exppiration on the LANCOM router and connection termination without the remote station noticing.
- On an outgoing call where a tag was specified in the "To" field of the parameter "Call is Being Forwarded", the LANCOM router answered with a PRACK without tag in the "To" field. Due to this, the call establishment was cancelled. This could result in particular call numbers not being reachable.

LCOS improvements 10.30.0167 RU1

New Features

General

- Support for SD-WAN Application Routing in the LMC
- A loopback- / sender address is now configurable for use in the alive test.
- The table “Status / Config / Event log“ has been extended to 256 rows.
- LISP: Accepting packets from unknown ITRs is now configurable

Wi-Fi

- Added a configuration option for reducing the sensitivity for received Wi-Fi packets
- Passwords for already existing users are now editable in the Public Spot user management.
- If a channel preference is configured in the 5 GHz band, the access point falls back to the preferred channel after radar detection and the expiration of the respective lock wait.
- Support for IEEE 802.11r (fast roaming) in Wi-Fi client mode.

VoIP

- The Telekom All-IP wizard has been extended by the specification of the phone number block.
- Transcoding to T.38 can be disabled for SIP-to-SIP calls.

Bugfixes / improvements

General

- On some devices of the 1781x series it was not possible to activate the certification authority (CA) in WEBconfig, although the device was equipped with the requested requirements (activated VPN25 Option).
- On LANCOM devices of the 179x- and the R88x series, which were configured for multiple Internet connections (1x VDSL modem, 2x WAN over ETH interface), the integrated VDSL modem did not start. As a result, the WAN connection could not be established via the integrated modem.
- A LANCOM vRouter with expired license could no longer be monitored within LANmonitor, because the initial SNMP request of the LANmonitor was not processed.
- Due to a false SOAP header format in the LANCOM router the TR-069 negotiation was refused by the Auto Configuration Server (ACS). As a result, automatic configuration and firmware update by the ACS were impossible.
- When using a loadbalancer as default route issues could occur when connecting to the LANCOM Management Cloud (LMC).
- When using IPv6-only LTE connections, i.e. PDP context IPv6, the LANCOM router received no IPv6 address, because the router started the DHCPv4 client. As a result, the LTE connection could not be established.
- When a service (e.g. e-mail) was invoked by a local client via port forwarding (Hairpin-NAT), packet loss could occur on the Internet connection. As a result, the Internet connection was faulty for all further established sessions.

- With LANCOM routers of the 179x series and the LANCOM R883+ downstream data rates could drop or variate if the integrated modem was operated at a supervectoring connection and synced with ADSL2+.
- If a configuration was rolled out to a device via the LANCOM Management Cloud (LMC), and a TFTP access was executed simultaneously, this resulted in a sudden device restart.
- In a backup scenario with two configured mobile radio connections a LANCOM 1906VA-4G could not establish a backup via the SIM card in slot 2, if a faulty PIN was configured for the SIM card in slot 1. The system remained in the status "PIN invalid".
- In a PMS server scenario the LANCOM devices ISG-1000, ISG-4000, and WLC-1000 tried to reach the IP address 0.0.0.0 instead of the PMS server address, because the network loopback address was not recognized correctly. As a result, no communication to the PMS server was possible.
- In conjunction with VLAN, L2TPv3 supported no MMS clamping and path MTU discovery. This resulted in a performance loss, because packets had to be transferred multiply. Party, data could not be transmitted at all.
- A LANCOM router managed by the LANCOM Management Cloud (LMC) could be displayed as "offline" after a restart or configuration rollout, although the device was operable and accessible.
- In a LISP configuration, the router did not answer ping requests from unknown ITRs
- If the RADIUS server of the LANCOM device was specified as forwarding destination by a Windows NPS (Network Policy Server), it could happen that no authentication was possible. A proxy state attribute which is requested by the NPS has now been added, so that the communication works again.
- Issues could occur if a LANCOM router communicated with a server system which used switch-independent NIC teaming. Both the configuration access to the LANCOM router and the server accessibility with port forwarding from the Internet was faulty.

  For a working communication with switch-independent NIC teaming between the server and the LANCOM router, the option "IP-Router / Send packets from internal services via router" has to be activated in the configuration of the LANCOM router.
- A configured loopback interface for the LISP-ETR has not been rolled out.

VPN

- An EoGRE tunnel which was established through an IPSec tunnel became inoperable when the IPSec tunnel has been terminated.
- If a VPN client was connected to the LANCOM router via IKEv1 protocol, and the client received an IP address by the router via config mode, the address was not saved to the router's RIB/FIB table.

  If, additionally, under ‚IP-Router / General' the option „send packets from internal services via router" was activated, this resulted in no communication being possible from the LANCOM router to the client. The communication from the VPN client to the local network, however, was not affected.
- If an IPv6 context was added to a WAN interface although the Internet connection did not support IPv6, Internet connection establishment took a long time, because every connection attempt with an IPv6 address was cancelled only after 30 seconds. Furthermore, the router tried to establish the VPN connection via a local link address.
- L2TP supports endpoint identifiers with a maximum of 16 characters. A longer identifier will internally be used unshortened, but externally shortened to 16 characters (e.g. in a status table). The information of an L2TPv3 connection could not be refreshed in the status tables, because one byte over was copied.

- Unicast packets were discarded when using an L2TPv3 tunnel if no related session was existing, but the address was still contained in the ARP table. This resulted in network devices which rarely send broad- and multicast packets were no longer accessible via the L2TPv3 tunnel.
  L2TPv3 now sends all unicast packets to the bridge, even if no related session exists.
- On VPN dial-in connections with a superodinate VPN user (authentication by RADIUS server or certificate dial-in) the remote site names are created e.g. by Key-ID or the RADIUS user. Internally only the first 12 characters are used, followed by a 4-character hash value in order to not exceed 16 characters for the remote site name.
  It could happen that multiple VPN remote sites had been allocated the identical hash value. If the first 12 characters of the key ID were identical, this resulted in multiple remote sites with the same name. This led to establishment and connection clearing of the VPN tunnels, because VPN SAs could not be allocated uniquely.
- After a re-keying no communication via an IKEv1 VPN connection was possible, if the allocated values of the phase-1 and phase-2 lifetimes were identical.
- On IKEv2 VPN connections with HTTPS encapsulation a sudden LANCOM router restart could occur due to memory losses.

Wi-Fi

- After obtaining the Wi-Fi profile including the password the initial setup wizard is invoked when opening the access point's configuration in WEBconfig for the first time. If this wizard was cancelled by the user, any configuration changes on the accesspoint could be performed in WEBconfig without ever being asked for a configuration password.
- The idle timeout of no longer signed-in Wi-Fi clients permanently remained at 900 seconds. As a result, the Wi-Fi clients were not deleted from the Wi-Fi station table if the Wi-Fi authentication was previously rejected.
- Reduction of false detections of radar events (DFS) for IEEE 802.11ac Wave-1 and Wave-2 Wi-Fi modules

VoIP

- If an external call was answered by an ISDN phone box which forwarded this call to an external number, the call forwarding failed. The Voice Call Manager did not process the so-called REDIRECT correctly, so after processing, the line allocation was faulty.
- Call termination after 15 minutes could occur because the Voice Call Manager answered a VoIP provider's update request after 15 minutes with the message "200 OK". This message contained SDP information which could not be handled by the VoIP provider. As a result, the VoIP provider sent a "BYE" message which led to call ermination.
- When using a Telekom DeutschlandLAN IP Voice/Data line with activated VoSIP, no incoming faxes could be received by an analog fax device. The reason for this was, that the LANCOM Router switched to T.38, and for this, sent a Re-INVITE. Due to faulty encryption settings in the router's re-INVITE, the VoIP provider refused the Re-INVITE with the message "403 Forbidden".
- Multiple use of internal call numbers in different call groups which should be called successively cascaded was not possible. The internal subscriber was only signalled at the first time. When resolving the next groups containing the same internal subscriber it was not considered.
- If an active call via the Voice Call Manager was finished while e.g. LANconfig saved a configuration change to the LANCOM router, a sudden router restart could occur.

- If a SIP subscriber receives an INVITE with a too small session timer, it confirms the INVITE with the message ‚422 Session Intervall Too Small'. In a call goup scenario with multiple SIP subscribers the message ‚422 Session Intervall Too Small' was not sent to the caller. Due to that, the call could not be established.
- If, during an active phone call, a LANCOM router sent the parameter Require: timer in the RE-INVITE, it could happen, that the remote station refused this with the message ‚420 Bad Extension' with the parameter Unsupported: timer, although the parameter Supported: timer was included in the initial INVITE of the remote station. As a result, phone calls were cancelled after 10 minutes.
  The parameter Require: timer is no longer transmitted in a RE-INVITE, because it is not necessary.
- If, on an outgoing call, a LANCOM router received the parameter Require: 100rel in the '183 Session Progress' from the provider, the router sent the parameter Supported: 100rel in the '183 Session Progress' to the internal SIP subscriber.
  Due to this, the caller did not hear any call sign, and after the call was answered, no voice data could be transferred. Furthermore, the call was disconnected after 10 seconds.
- A Voice over LTE (VoLTE) subscriber offers multiple codecs in its INVITE, as well as 8 and 16 kHz sampling rates for DTMF. On an incoming call of a VoLTE subscriber the LANCOM router answered with a faulty DTMF payload type in its ‚200 OK'. Also, the Voice Call Manager supported only a DTMF sampling rate of 8 kHz.
  Due to this, no DTMF information could be transmitted. Partly, this resulted in no voice communication being possible.

LCOS improvements 10.30.0075 Rel

Bugfixes / improvements

General

- When a router or access point obtained its IP address by DHCP, an error occured on the DHCP interface while resolving routes when receiving IP packets from outside the local network. As a result, the device firewall refused the IP packets with the message "Intruder detection".
- 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.
- If a LANCOM router obtained the IP parameters for the remote station INTERNET-DEFAULT from a DHCP server, and a preceding gateway owned the IP address xx.xx.xx.254, an IP address conflict occured because the LANCOM router assigned itself the IP address xx.xx.xx.254, too. This resulted in no communication being possible to the Internet and to the LMC.
- The configuration rollout from the LANCOM Management Cloud (LMC) to a router which was connected to the Internet by IPv6 Dual Stack Lite could lead to a sudden router restart.
- If a DS-Lite tunnel was configured in a load balancer ("IP router / Routing / Load balancing"), a sudden LANCOM router restart could occur.

Now the DS-Lite tunnel can no longer be selected in the load balancer configuration.

- If IKEv2 was used in conjunction with IPv6 in the LAN, the IKE-Config-Mode server could not assign an IPv6 default route to a VPN client.
- If a LANCOM router obtained its IP parameters for a network with a tagged interface by DHCP, the automatically generated default route was allocated to networks with different interface tags. This resulted in packets being routed falsely in the affected networks, instead of discarding them.
- After executing the command "default -r" on the root level to reset the configuration to default values the table "Setup/Firewall/DNS-Destinations" has not been reset.
- The LANCOM vRouter was missing the function for determining and defining data- and time budgets.
- It was not possible to create an alternative boot configuration for the LANCOM devices ISG-4000 and WLC-1000.
- Invoking website URLs which were listed in the Content Filter whitelist took an unusually long time.
- The checksum calculation of Ethernet packets did not work accurately in the vRouter. This could lead to communication issues.

VPN

- If a router accepted a VPN connection which had been authenticated by a RADIUS server, all VPN rules of the connection remained active in the SADB, even after disabling the VPN module and disconnecting. DPD packets were sent further on.
- Split-DNS is intended to transfer DNS information via IKE config mode. While doing so, domains which were stored as subdomains in the DNS server were not transferred, but only those which had been configured as the router's own domain. Additionally, an empty entry in the device's own domain resulted in a display error in the appropriate status table of the receiving device.
- When using the Split-DNS function in an IKEv2-VPN connection the wildcard value "*." was saved to the client router when transferring the DNS wildcard value "*". So the wildcard entry could not be used correctly in the branch office.
- When using IKEv2 connections there is an option to authenticate via an externel RADIUS server. In doing so, RADIUS requests were not released by the LANCOM router, so that after a longer operating time no additional RADIUS requests could be performed. As a result, VPN connections could no longer be established.
- VPN connection establishment did not work if an entry was defined in the polling table for an IKEv2 connection, and the IKE config mode „client" was defined for masking packets behind the allocated IP address.
- If an IKEv1 VPN remote station which should be established over an IPv6 WAN connection, and an ISDN remote station were configured using identical names, the VPN connection could not be established.
- When using GCM encryption algorithms, a faulty VPN connection which should be authenticated via remote RADIUS server disconnected all VPN connections which had been successfully established by the RADIUS server.
- If in a LANCOM Advanced VPN Client dial-in profile the port was configured to 4500 in the menu "Extended IPsec options / UDP encapsulation", an IKEv1 client login failed with the message "IKE info: Phase-2 proposal failed".
- If a VPN connection was disconnected (manually) and reconnected, the OSPF protocol stopped working on this VPN connection.

Wi-Fi

- If a LANCOM device was operating both Wi-Fi and the Public Spot function, this resulted in the Public Spot user being deleted not only from the WLAN station table, but also from the Public Spot auto-relogin table after the default WLAN idle timeout was reached. As a result, a re-login to the Public Spot with identical user data was no longer possible.

VoIP

- A sudden router restart could occur if a LANCOM router received an encoded T.38 packet without audio contents.
- If a SIP phone box sent an INVITE with a very small session timer, this timer was applied by the LANCOM router. If this value was answered by the provider with the message "422 Session Interval Too Small" (displaying the minimal session timer), the router ignored this if the provider sent an UPDATE during the "Early Media Phase". As a result, the router cancelled the call with a "BYE" when the original session timer had expired.
- An incoming call on the Telekom connection was answered by NFON with the message "404 Not Found" in a scenario with a Telekom SIP trunk, or a Telekom All-IP connection and an NFON Cloud phone station connected by SIP trunk.

  The reason for this was the NFON expectation of the user ID in the field "P-Asserted-Identity" instead of the field "P-Preferred-Identity" when using a SIP trunk.
- When using ISDN devices which do not send a caller number on outgoing calls (e.g. door intercom systems) outgoing calls could not be established if a VoIP provider was used which did not accept an empty or "anonymous" "Calling party" field (e.g. SIPGATE).
- On incoming calls via SIP-PBX line no DTMF signals were forwarded to the users.
- If the message "181 Call Is Being Forwarded" was received from the SIP provider in answer to an outgiong call due to an active call routing, information was missing in the "to header" in the requested confirmation (PRACK). Due to this, the provider cancelled the call displaying the message "481 Call/Transaction Does Not Exist".
- Call termination after 15 minutes could occur because the Voice Call Manager answered a VoIP provider's update request after 15 minutes with the message "200 OK". This message contained SDP information which could not be handled by the VoIP provider. As a result, the VoIP provider sent a "BYE" message which led to call termination.
- If a SIP user sent a REGISTER packet without specifying the port within the contact header, the Voice Call Manager added port 0 to the following "200 OK". As a result, voice transmission could fail on incoming calls.
- On incoming calls an error could occur when converting DTMF signals, resulting in all RTP packets being discarded and incoming voice data no longer being transmitted.

LCOS improvements 10.30.0045 RC2

New features

General

- A target interface can now be specified for the CLI command “ll2mdetect“ (parameter “-i“).
- The output of the CLI command “show job“ now shows the complete CPU load.

Bugfixes / improvements

General

- The configured routing distance in the IPv4 routing table was no longer considered after a device restart.

Wi-Fi

- Connection losses with Amazon Echo devices could occur when using Wi-Fi routers or access points with an 802.11n Wi-Fi module.
- When using the WLAN-2 radio module on access points of the LN-17xx series the client mode did not work.

VoIP

- Processing incoming DTMF signals could cause the termination of voice transmissions.

LCOS improvements 10.30.0028 RC1

New features

General

- Adaption of the number of simultaneous Public Spot users on routers of the 178x- and 179x series to 128.
- The SMTP client’s internally used SSL/TLS version can now be configured.
- Jitter display within the ICMP-SLA monitor
- „clear“ command for deleting the current console display
- Support for TLS 1.3 in WEBconfig
- Support for the ThinAP 2.0 protocol for linking Wireless ePaper access points to a central Wireless ePaper Server
- Support for IPv6 in TACACS+
- Support for RSA-PSS signing in the SCEP-CA

Routing

- Application routing and -control in the IPv4- and IPv6 firewall
- Evaluation of DSCP tags in the IPv6 firewall
- IKEv2 IPv6 CFG mode addresses can be assigned to clients based on the prefix allocated by the provider.
- Support for address allocation in the DHCPv6 server

VPN

- Support for IKEv2 cookie notification
- Support for IKEv2 Split DNS
- Support for IKEv2 fragmentation
- ECDSA support for IKEv2 authentication

Wi-Fi

- The e-mail notification for Wi-Fi events can now be enabled/disabled via button.
- The 802.11n Wi-Fi module rate adaption now considers the configured transmission power limitation when selecting rates.
- As an alternative to transmission power limitation the target EIRP (transmission power) is now configurable for Wi-Fi.
- Support for 802.11k in Wi-Fi client mode
- Support for 802.11v in Wi-Fi client mode
- Support for the SAE authentication method in Wi-Fi client mode

6. 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.