LANCOM Release Notes

LCOS

10.40 Rel

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

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

May 19th, 2020, CBuersch

Table of Contents

LANCOM Systems

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 10.40 Rel, 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 10.40

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 10.40, support for the following devices is discontinued

- LANCOM 1780EW-4G
- LANCOM 1781A-4G
- LANCOM L-322E
- LANCOM L-1302acn
- LANCOM L-1310acn

3. Advices regarding LCOS 10.40

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 10.40

4.1 Feature highlights

Next-generation SD-WAN: LANCOM High Scalability VPN (HSVPN)

High scalability VPN significantly improves the extensibility and efficiency of your SD-WAN architecture. Previously each individual application needed its own individual VPN tunnel, but HSVPN now transports any number of networks on a single VPN tunnel to the remote site. Networks remains secure and strictly separated from one another. The advantage for your business: Significantly fewer VPN tunnels are required and faster recovery times in case of failover.

Modern look & feel: New WEBconfig

You can look forward to the completely new look and feel of LANCOM WEBconfig. Based on the modern and bright design of the LANCOM Management Cloud, WEBconfig has been completely redesigned to offer you an attractive and fresh appearance.

Multicast routing

Multicast data such as IPTV is now transmitted efficiently to multiple devices. Previously, separate data packets had to be sent to each recipient, whereas multicast routing now allows an IP stream to be transmitted to multiple recipients. This reduces the load on the router and makes better use of available routing capacity.

4.2 Further features

SD-WAN zero-touch deployment for DSL routers

Automatic installation of DSL routers at BNG Telekom connections with the LANCOM Management Cloud—without the laborious configuration of DSL access data on the router.

Netflow

With Netflow, network analysis information about the router's incoming and outgoing IP traffic (source, destination, ports, etc.) can be sent to a central server for processing.

IKEv2 VPN with Windows login

Mobile VPN clients using IKEv2 EAP can now authenticate against a central database such as Microsoft Active Directory or RADIUS without having to store VPN credentials on the LANCOM router.

More flexibility with backup scenarios

Route prioritization offers new levels of flexibility for backup scenarios.

New SD-WAN functions for the load balancer

On central-site gateways, VPN load balancers can be generated automatically with the help of RADIUS. Furthermore, multiple VPN channels are aggregated into tunnel groups, so that even in the case of failover, the VPN connects to a common gateway.

WLAN scheduling

Enables time-based activation and deactivation of SSIDs in the wireless LAN. Ideal for WLAN networks that should only be available at specific times, such as hotspots or Wi-Fi in educational institutions.

More security in the VPN

Support for new and modern encryption algorithms such as Chacha20-Poly 1305, digital signature with ECDSA, and new Diffie-Hellmann groups.

TLS 1.3 client mode

Support for the new TLS 1.3 protocol improves security for router accessing web services.

New filters for individual notifications

Configurable filter lists for SNMP traps and SYSLOG enable individualized monitoring notifications to be received.

You can find further features within the individual builds sections in chapter 5 "History LCOS 10.40".

5. History LCOS 10.40

LCOS improvements 10.40.0210 Rel

Bug fixes / improvements

General

- The routing option ‘Send ICMP redirect’ did not work.
- SNMPv3 traps were sent in a non-compliant format, resulting in status displays and value changes not being displayed e.g. in LANmonitor.
- Several issues related to SNMP accesses to a LANCOM device (e.g. opening in LANmonitor) were fixed because SNMP did not work properly with the new password hash function.
- New entries could be added to the whitelist of the LANCOM Content Filter (menu ‘Content Filter / Profiles / Whitelist Addresses’) using LANconfig, but these were not included when writing back the configuration.
- When using GRE tunnels, a sudden restart could occasionally occur if an established GRE tunnel reported an invalid connection channel to LCOS.
- If a certificate was created in WEBconfig which contained an e-mail address (E) as information, the certificate was not generated.
- After deactivating the function ‘Receive clear text password’, the respective password always had to be entered when editing the ‘Other administrators’ (e.g. the function rights). Otherwise the error message “Your input for ‘Password’ is incorrect” was displayed.
  Also, an empty password could be set if the ‘enforce device password policy’ function was disabled.
- A device managed by the LMC could sporadically reboot after the certificate renewal by the LMC client.
- VLAN IDs were not transmitted when using IPv6 if the VLAN ID was stored in the IPv6 networks but the VLAN module was not active. This caused communication problems.
- Incoming packets from an Internet connection with routing tag ‘0’ were not forwarded to a DMZ with a tag other than ‘0’.
  The procedure has now been modified so that a DMZ can be reached from all networks, including the Internet. This corresponds to the behavior in previous LCOS versions.
- When using several potentially matching firewall rules, communication between two networks was not possible if the first of these firewall rules did not apply when the session was established, but only a subsequent rule. As a result, the destination for the packet was the gateway of the Internet connection.
- When BGP and OSPF were used simultaneously, routes learned by BGP were not forwarded to the OSPF neighbor if the forwarding address was not accessible via an intra- or inter-area path. The forwarding address is now set to 0.0.0.0 by default.
- If a packet was sent from a local network to the IP address of the router in a DMZ, it was rejected by the router’s firewall if the Internet remote peer of the DMZ was defined as the connection target in the firewall rule.
  If an IP address of the router is addressed (loopback), the target interface is no longer checked in the firewall.

- 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.
- The LL2M function could not be used if no password was set in the configuration for the addressed device.

VPN

- An IKEv2 connection could not be established over a PPPoE and PPTP Internet connection because the negotiated MTU was not forwarded to the control level of the router and the MTU in the VPN was therefore too large.
  If there were several VPN rules (IKE_SA) for a RAS VPN dial-in that were not completely negotiated, the parent rule list for this VPN connection was deleted after the first of these rules expired. If the router then tried to send a DPD packet to the RAS VPN client despite the missing rule list, this resulted in a sudden restart of the router. This could occur if the RAS VPN client was incorrectly configured and did not respond to IKE_AUTH response packets from the router and instead re-established a connection.
- In a scenario with an active VPN load balancer, it could happen that when several VPN connections from the same dial-in router (configured by the LMC) were established simultaneously, a timeout of a not yet established VPN connection occurred after 30 seconds when renegotiating the DH group. As a result, all VPN connections established so far on the dial-in router were also terminated.
- If the authentication methods differ between a main VPN connection and another VPN connection that is configured as a backup VPN connection (e.g. certificate-based for main connection and PSK for backup connection), the backup VPN connection was not established in the backup case.
- If a VPN site-to-site connection was disconnected during a cron job, some existing client-to-site VPN connections were also disconnected.
- For VPN connections the counter for received IP packets (Rx-Packets Counter in path ‘Status / VPN’) was without function.

Wi-Fi

- If 2.4 GHz channels are explicitly selected on radio module 1 of a LANCOM WLAN controller in an access point profile for a device of the LN-17xx series, the access point converts the channel list so that a non-existent 5 GHz channel is used on the second radio module.
- Access points could not be managed by a WLAN controller in the vRouter (vWLC) due to an error in the DTLS negotiation.
- If the setup wizard ‘Configure Wi-Fi’ was run on a LANCOM IAP-821, the Wi-Fi operating mode was set to ‘Client’ and the feature ‘Soft Roaming’ was deactivated, a sudden restart occurred after completing the setup wizard. If a configuration file was uploaded to a LANCOM IAP-821 with soft roaming deactivated, a sudden restart occurred, too.

VoIP

- If a SIP client should register via SIP-ALG over a VPN connection, the registration process failed.
- Occasionally it could happen that a terminated analog call in the LANCOM router was still active. If the ‘Busy on Busy’ function was used, incoming analog calls were rejected.
- If, with e-mail notification configured, an incoming call via ISDN was not answered, the e-mail notification failed.

LCOS improvements 10.40.0166 RC3

Bug fixes / improvements

General

- The configuration of the device could not be written back in LANconfig if the option 'Force password rules' under 'Messages/Monitoring / Logs / SNMP settings' was initially activated and then deactivated and an SNMP user was created in the same step.
- 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.
- In individual cases, accessing a LANCOM router via WEBconfig using the TLS 1.3 protocol could result in a sudden restart.
- 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.
- During a UDP scan on the Internet, several thousand packets are sent within a few seconds from a fixed source IP address with a fixed UDP source port to any destination IP address to a larger UDP destination port range. If the destination IP address was part of the DMZ of a LANCOM router, i.e. the packets were routed, the router was then very busy and may have been busy processing the packets for several minutes.

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

- When using WLC tunnels, the packets in the LAN bridge were rejected with the message 'no forward to interface itself' when communicating from Wi-Fi devices within the same SSID, which were logged on to different access points.
- 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.
- A ring back tone generated by the provider (RTP stream) was not signalled to the caller during an outgoing call, because the Voice Call Manager only considered port 5060 instead of the current port with the session to the provider. If the outgoing call was initiated by an ISDN or analog subscriber, the ring back tone could not be signaled to the caller because the Voice Call Manager switched to 'Local Ringtones' for signaling. Subsequently, the message PROGRESS was sent to the subscriber, which canceled the ring back tone signaling.
  The message PROGRESS is now first sent to the subscriber and then the ring back tone is signalled.

LCOS improvements 10.40.0142 RC2

New features

General

- As from LCOS 10.40 RC2 the LANCOM vRouter is extended by the functions of the LANCOM High Availability Clustering Option as well as the LANCOM Public Spot PMS Accounting Plus Option.
  HA Clustering is valid for all LANCOM vRouters >= LANCOM vRouter 500
  PMS Accounting Plus is valid for all LANCOM vRouters
  Customers who have already purchased a LANCOM vRouter can have a replacement license generated by the LANCOM support if required.
- Support for MLD Snooping
- DSCP tags can now be set from within the SLA monitor.
- The cache time for using DNS objects in the firewall is now configurable.
- The main device password and the passwords for other administrators can now be saved using the hash algorithms SHA-256 and SHA-512.
- The CRL check is now switchable per IKEv2 remote station.

Bug fixes / improvements

General

- The LANCOM 883+ VoIP lacked the ability to configure the AiRISTA Flow Blink mode (/Setup/Wlan/Blink Mode/). As a result, a device could not be transferred to the LANCOM Management Cloud and error messages appeared after a configuration change.
- With the vRouter, port forwarding did not work if a map port was used that was not equal to the specified port.
- On a vRouter with port forwarding for PPTP, the GRE packets could not be assigned to the PPTP session. As a result, the GRE packets were not forwarded and the PPTP connection did not work.

- If a firmware update to an LCOS version greater than 10.12 was carried out on a router with an active VPN connection on which the sending of SNMP traps to a recipient accessible via VPN connection was set up, this led to three sudden restarts of the router. The old firmware was then reactivated. As a result, it was not possible to use the current firmware.
- With DHCPoE connections (IPv4 only), after the provider had renewed the IP parameters, the default route was rebuilt and all sessions were terminated. This could lead to a regular termination of all connections for certain connections.
  The default route is now only rebuilt if the gateway has also been changed.
- DNS targets in the firewall can be used, among other things, to block access to a specific website.
  Since end devices have their own DNS cache which holds the addresses longer than the router, access to the website was often still possible.
  It is now possible to specify a minimum time for the router to keep DNS entries. The default value is 180 seconds.
- If IP networks are separated from each other by assigning different interface tags not equal to 0, communication between the two networks can only take place by creating a corresponding firewall rule.
  Despite a suitable firewall rule, the DNS name was not resolved when a network participant in one of the networks tried to access a resource in one of the other networks using DNS. This prevented access to the resource.
- After configuring an Internet connection on a factory-installed LANCOM router, it could happen that DNS queries on the functioning Internet connection were not answered.
- With Hairpin NAT, a rewinding session was blocked by the LANCOM router's firewall if the firewall contained a ‚Deny All' rule and also a port forwarding ‚Allow' rule used the name of the Internet remote peer as source instead of the value ‚Anyhost'.
- Due to an unconsidered port member list, it could happen that the LANCOM router suddenly rebooted when a T-Entertain receiver was connected to it.

VPN

- An IKEv2 VPN connection using the Edwards-Curve Digital Signature Algorithm (EdDSA) could not be established due to an incorrect default value during the negotiation of the Security Associations (SAs).
- A minus sign could be set in the HSVPN profile in the routing tag list using WEBconfig, although this was not included in the list of allowed characters.

Wi-Fi

- A Spectral Scan on the WEBconfig interface of a LANCOM LN-1700UE was aborted with the error message ‚Data Connection Closed!'
- If the command ‚show script' (rollout check) was entered on the command line of LANCOM access points after a script rollout via a WLAN controller, the device was immediately rebooted.

VoIP

- In scenarios with active SIP-ALG, incoming telephone calls resulted in no voice data being transmitted in either direction.
- When using SIP ALG, a VoIP phone could not register with a VoIP PBX accessible via VPN connection because the source port of the VoIP phone was set to 0 instead of 5060 when the registration packet was sent via the VPN connection.
- If the remote terminal of a VoIP telephone connection sent a Re-INVITE to the LANCOM router, the router responded with an INVITE which included a ‚Require: timer'. However, this INVITE was rejected by the provider due to the ‚Require: timer' with ‚BAD EXTENSION'. Subsequently the call was terminated.
- 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 call termination 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.
- If the message '180 Ringing' was received from the remote party during the 'Early Media Phase' of an outgoing telephone call without an SDP message, the LANCOM router did not generate a service tone. As a result, the called subscriber did not ring. It was also possible that no voice data was transmitted and thus no telephone call was possible.

LCOS improvements 10.40.0103 RC1

New features

General

- New design for WEBconfig
- Syslog messages when switching firmware and firmware information when booting
- For IPv6 WAN access the DHCPv6 client is now started, even if no router advertisements have been received before.
- For the Deutsche Telekom's BNG line Zero Touch commissioning an appropriate Internet remote station has been added to the default configuration of the DSL routers.
- In the default configuration a main device password has to be specified at the first console login.
- Support for WAN connections with a provider-allocated DHCPv4 address with /32 mask
- An e-mail and/or syslog entry is now generated when having reached 80% of the configured volume budget.
- For QoS WAN bandwidths of more than 1 Gbps can now be configured.
- Support for High Availability Clustering within the vRouter for license "vRouter 500" and above
- Support for the TLS 1.3 client mode
- SNMP traps to be sent can now be filtered.
- Syslog messages to be sent can now be filtered.
- A sender address is now available for the alive test.
- The RADIUS dictionary can now be extended by user-defined attributes.

Routing

- Support for multicast routing
- Support for IGMP- and MLD proxy
- Support for PIM (Protocol Independent Multicast)
- Remote stations can now be established on demand even without existing routes in the routing table.
- The DHCP client now supports the option 121 (Classless Static Route) as per RFC 3442.
- The BGP connection retry timer is now configurable.
- The behaviour when propagating the default route within BGP can now be configured.
- BGP now saves a history containing sent prefixes.
- The IPv4 firewall does no longer support MAC addresses as target. Existing configurations remain working.
- The time-controlled default route has been removed.
- For static IPv4- and IPv6 routes the administrative distance can now be configured.
- Support for NetFlow/IPFIX
- The administrative OSPF distance is now configurable.
- A filter list can be configured for route redistribution via LISP and OSPF.
- The line “DMZ“ has been removed as default from some tables.
- The TFTP-Operating switch now offers the mode “Only sysinfo“.
- The IPv4 router scalability with many routes has been improved significantly.
- If the provider transfers the actual layer-3 bandwidth as an additional information within PPP, this value is used for QoS.

VPN

- Support for LANCOM High Scalability VPN (HSVPN)
- Support for IKEv2 EAP
- Support for ChaCha20-Poly1305 for IKEv2
- Support for EdDSA for IKEv2
- Support for Digital Signature with ECDSA as per RFC 7427
- Support for Curve25519 and Curve448 for IKEv2
- A VPN load balancer can be generated dynamically by RADIUS.
- Requesting an address in IKEv2 config mode is now switchable.
- Alternative gateways can now be grouped and prioritized.
- Removed IPCOMP for IKEv1
- Removed AH for IPsec

Wi-Fi

- Support for OCSP within the RADIUS server related to EAP(-TLS)
- Wi-Fi SSIDs can be enabled / disabled scheduled.
- A user-defined branding logo (“powered by LANCOM”) can now be used for Public Spot on the login page.
- Support for the LANCOM Public Spot PMS Accounting Plus option in the vRouter
- HTTPS is now selected by default for the Public Spot login page, if “HTTPS” is selected as the login page protocol. Before only the credentials and the status page have been transmitted via HTTPS.
- For Wi-Fi clients a threshold can be defined for disassociating clients when falling below.
- VLAN group keys are now allocated automatically.

VoIP

- Passwords for SIP lines can now consist of up to 64 characters.
- Support for “Telekom Company Flex“
- The “Connected Number“ format is now configurable.
- Support for Early Media
- Calls can be spread dynamically to different SIP lines.
- The maximum number of simultaneous calls for one SIP line is now configurable.

WLC

- “Unknown seen clients“ are no longer reported to the WLC in the default configuration.
- The client bandwidth limitation is now configurable on the WLC.

Bug fixes / improvements

General

- If a certificate was loaded to a LANCOM router’s VPN container via SCEP while having the same subject like an already existing certificate in a VPN container, the certificate was tagged with an unknown status and could not be rolled out.
- If the transmission modes “UMTS(3G)+GPRS(2G)” or “GPRS(2G)” were selected in the mobile radio profiles of the LANCOM devices 1780EW-4G+, LANCOM 1793VA-4G or LANCOM 1790-4G, the devices used LTE(4G) all the time, because the built-in mobile radio module does not support transmission mode GPRS(2G).
  The device now establishes a 3G connection.
- Besides obtaining the location, obtaining the time is possible via GPS, too. LTE routers with the MC7710 LTE module always reported “2001-01-01 00:00:00“ + router running time. The time synchronization by GPS is now disabled in case obviously false values are received.
  The following devices were affected:
  - 1780EW-4G hardware Rel. B and C (partly)
  - 1781VA-4G hardware Rel. B and C (partly)
  - 1781-4G
  - 1781A-4G (partly)

- If a script was rolled out to a router by the rollout wizard which set a single value within a table row, a sudden router restart occured.

VoIP

- The Voice Call Manager did not support multiple dialogs in the Early Media phase. On phone calls with multiple dialogs (e.g. when using call routing via a phone service) this resulted in no voice data being able to be transmitted after the call was established.
- In a scenario with a SIP phone box connected to a gateway line the session ID within the SDP information was not incremented by the LANCOM router on incoming calls. This resulted in call termination when answering the call.
- In the call routing table the number of possible entries was limited to a maximum of 128. This limitation has been removed.
- With Telekom VoIP connections it could happen that no “ring” was signalled on the line for fixed line calls initiated by SIP clients, because the provider sent a “Ringing” without Session Description Protocol (SDP). As a result, the call establishment remained unsignalled until call answering.
- On devices of the 1783x series WEBconfig showed all analog- and dial interfaces for an analog user as selected, if the user entry was saved with the analog- and dial interface 2 only.

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.