LANCOM Release Notes

LCOS

10.50 RU2

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

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

October 08th, 2021, MKoser

Table of Contents

1. Preface

The LANCOM family of operating systems—LCOS, LCOS SX, LCOS LX, and LCOS FX—forms the trusted basis for the entire LANCOM range of products. Within the scope of the hardware specified by the products, the latest firmware version is available for all LANCOM products and is offered by LANCOM Systems for download free of charge.

This document describes the innovations within LCOS software release 10.50 RU2, 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 10.50

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/

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

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

3. Advices regarding LCOS 10.50

Information on default settings

Devices delivered with LCOS 10.00 or higher automatically connect to the LANCOM Management Cloud (LMC). This functionality provides zero-touch installation for new devices. In case you do not want to use the LMC, this feature can be disabled while running the default setup wizard for the initial configuration, or at any time from within LANconfig under Management > LMC. You can manually re-enable the usage of the LMC whenever you want.

4. Feature overview LCOS 10.50

4.1 Feature highlights 10.50

Performance upgrade for the LANCOM ISG-8000

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

Fast failover for maximum operational reliability

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

4.2 Further features 10.50

Extension of IPv6 functionality

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

Platform expansion for the LANCOM vRouter

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

You can find further features within the individual builds sections in chapter 5 “History LCOS 10.50”.

5. History LCOS 10.50

LCOS improvements 10.50.0331 RU2

New features

- Support for LANCOM SFP-GPON-1 module
- Update of the DSL line code of the LANCOM 1926 series

Bug fixes / improvements

General

- Due to an incorrect sorting of the "port forwarding table" it could happen that port forwarding did not work correctly in case of overlapping entries (with different protocols).
- In a VRRP scenario with individual WAN peers, in which these peers were additionally combined to form a load balancer, it could happen that the VRRP slave attempted to establish the WAN peers every second.
  As a result, the CPU load of the device increased and a memory shortage occurred. A pause has now been programmed between the individual connection attempts, which means that the device is no longer pushed to its performance limit.
- On the LANCOM 1790VA-4G+, information about the cellular band in use was not displayed in the status.
- The LANCOM routers of the 1926 series could regularly terminate the ADSL and/or VDSL Internet connection. The Internet connections were also not automatically re-established after an interruption (reboot solved the problem until the next interruption).
- If TR-069 functionality was enabled, the LANCOM router could reboot without warning.
- Due to a limited character set, IPv6 link local addresses could not be used with BGP.
- If an IPv4 address pool was stored in the configuration of a LANCOM router and a new VPN dial-in was created via the Setup Wizard in WEBconfig, the existing address pool could not be selected in the Setup Wizard.

Wi-Fi

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

VoIP

- In a scenario in which a Panasonic SIP PBX (SIP-TK KX-NCP500) was connected to a LANCOM router, call forwarding could fail due to faulty SDP communication on the part of the PBX. A workaround has now been implemented in LCOS which intercepts the error and enables communication.
- If an outgoing call was forwarded from the called subscriber to a third subscriber and the third subscriber offered a DTMF menu for call handling, DTMF communication via key tones no longer worked. As a result, the DTMF menu offered by the third party could not be operated.

LCOS improvements 10.50.0235 RU1

New features

- The activity status of the DNS forwarder is now also displayed in the WEBconfig dashboard under 'Services'.
- **VoIP:** For TCP-based SIP lines, a TCP keepalive packet is now sent every 60 seconds. The interval is configurable on the CLI.

Bug fixes / improvements

General

- If a value was entered in the access station table, it was not possible to establish a WEBconfig session to a device from the LANCOM Management Cloud (LMC).
- When saving a script configuration file in WEBconfig, an invalid file extension was assigned to the file.
- When the 'show ip-addresses' command was entered, the value for the DHCP lease time, if it reached 0, remained at that value.
- An external modem that was connected to a LANCOM router and had a so-called APIPA address (Automatic Private IP Addressing) could not be reached by the LANCOM router because these addresses were not allowed by the proxy ARP from the LAN.
- In private LMC installations, WEBconfig remote access via the web browser did not work if too many HTTP cookies were used.
- When using certain DSLAMs on the provider side, it could happen with a LANCOM 1926VAG that the DSLAM did not transmit all the required parameters to the DSL modem due to an incompatibility between the installed DSL modem and the DSLAM. This meant that no DSL sync could be established and thus no DSL connection could be established.
- When a LANCOM router was operated as a DNS server, in some cases the device responded to SOA and NS queries with the trace message "bad coded request". As a result, the request could not be executed.
- In WEBconfig (e.g. in menu 'Configuration / IP Router / Routing / IPv6 Routing Table) an IPv6 prefix was displayed incorrectly due to faulty HTML coding.
- Successful admin logins into WEBconfig were recorded in the login table, but the login counter remained unchanged.
- When using a loopback address for sending e-mails via SMTP, the loopback address was not taken into account. If a routing tag other than 0 was specified in the loopback address, no transfer to the SMTP service took place for this and the routing tag 0 was used. This could lead to the fact that sending e-mails was not possible.
- Due to a limitation in the number of registered MAC addresses, the VRRP function could only be used on the first 6 ARF contexts. This only affected routers with DPAA (19xx series, ISG-1000, ISG-4000, and WLC-1000.
- In a BGP community, the value 0 could not be used.

- If port forwarding was set up with a port between 16384 and 65535, it could happen that this port was also used for a dynamic port negotiation of another network subscriber. In this case, the incoming packets were forwarded to the destination of the dynamic port negotiation instead of the actual destination.
- If a firewall rule with 'conditional transmission' was passed and no condition in another firewall rule was true, the packet was discarded in the IP router with the error message "Network unreachable (no route) => Discard" instead of allowing the packet afterwards via 'ACCEPT'.
- Matching the IP address with a DynDNS service did not work when using HTTPS because the traffic could not be transmitted due to a too high MTU.
- Packets from a network with an associated LACP interface were discarded by the firewall because the intruder detection detected an incorrect interface. As a result, communication with this network was not possible.
- If a backup connection was specified in the backup table whose name designation was shorter than that of the main connection, a firewall rule containing a station object with the name designation of the main connection could not be written to the device.
- When using LACP, it could sporadically happen that the response to an incoming packet was sent over a different LACP interface. This caused the packet to be discarded.

  On routers with hardware switch (17xx and 19xx series), the error message "sEthSwitchDrvrDscr: WARNING: physical port x is not part of function LAN-x (port mask 0x04), packet will be discarded" was issued in the Ethernet trace in this case. On routers without a hardware switch (ISG-x000, vRouter), the packets were silently discarded.

Wi-Fi

- Access points with an old firmware (e.g. version 9.24) could not be managed by a WLAN controller due to a faulty TLS handling.
- It could happen in a WLC cluster scenario that the sub-CA on the slave expired and no new certificate was obtained. This meant that the access points registered on the slave could not be managed.
- After a firmware update to LCOS 10.50, an OAP-830 without an active VPN option could sometimes experience a boot loop.
- If a WLAN strength trace was executed when the WLAN trace MAC address was set, the device rebooted immediately.

VoIP

- In scenarios where a Swyx server with software lower than version 12.30 was used, the fax transmission from the LANCOM router to Swyx could fail due to an incorrect transaction ID.
- Because TCP keep-alive packets sent by the LANCOM Voice Call Manager contained a SYN flag, VoIP lines that did not use signaling encryption could lose registration.

LCOS improvements 10.50.0145 Rel

New features

- Support for RADIUS Dynamic Peer Discovery according to RFC 7585

Bug fixes / improvements

General

- When creating a RADIUS user via WEBconfig, the user profile could not be saved if no passphrase was entered there.
- With the console command 'passwd -n' a password change can be performed without query. The change was not applied to SNMP access, so SNMP access was possible with the old password. (CVE-2021-33903)
- When using certificates with 'Elliptic Curve Algorithm' for RADSEC, TLS negotiation could not be completed successfully.
  Furthermore, the 'Private Key' of a certificate with 'Elliptic Curve Algorithm' could not be uploaded to the RADSEC slot. The import process was aborted with the message "FAILURE".

VPN

- If the router tried to send a packet over the VPN connection during a VPN setup in the time window between IKE negotiation and the change to the 'Up' state, all packets were dropped.
- After taking down and then re-establishing a VPN connection (both IKEv1 and IKEv2) with IPv6 on a vRouter or LANCOM ISG-8000, the VPN rules (SA) were not established correctly. As a result, communication over the VPN connection was no longer possible.

VoIP

- It could happen that phone calls were not transmitted via the SIP-ALG because the external port was declared as invalid by the router. The packets were then rejected with the error message "ICMP Destination unreachable (Port unreachable)".
  Furthermore, the bandwidth reservation in SIP-ALG did not work anymore.
- In a scenario with a Swyx Mediabridge a REFER with the actual destination of the call is sent in the 'Refer-To' header after call setup. Then the router sends an INVITE to this 'Refer-To' destination via the Swyx PBX. In case of an error the Swyx PBX did not answer with a "200 OK" but with the error message "500 Server Internal Error". In this case the router tried to send the INVITE on another line. But since the replace information from the REFER was still used for this, the router sent the INVITE again via the gateway line to the Swyx PBX.
  An INVITE is no longer sent on a gateway line after the error message "500 Server Internal Error" has been received on this line. Furthermore the router waits for a BYE from the Swyx PBX and then terminates the call setup. If no BYE is received from the Swyx PBX, the router sends the BYE and terminates the call setup.

- In individual cases, it can happen that an UPDATE is sent by the caller instead of the called party for an incoming call during the early media phase. In such a case, the UPDATE was sent by the router back to the SIP line instead of to the local subscriber. This resulted in a one-way voice transmission.
- In a scenario with a parent SIP PBX, if different codecs are used in the sessions between the router and the SIP client and the router and the SIP PBX for an outgoing call, the codec must be renegotiated with the SIP client in a re-INVITE so that the codec matches. If the SIP PBX sent a Re-INVITE to forward the call to the router at that moment, it was sent from the router to the SIP client even though the first Re-INVITE was not confirmed yet. This resulted in missing voice transmission in connection with noise at the calling subscriber.
  The transmission of the second Re-INVITE of the SIP TC system is now transmitted only when the first negotiation is completed.

LCOS improvements 10.50.0129 RC3

New features

General

- New DSL line code for LANCOM 1926 series devices
- On the DSL routers of the 19xx and 179x series, it is possible to switch between the current and an alternative DSL line code.
- Support of a DNS filter for detection and filtering of unwanted DNS data tunnels at the client side
- Support for IPv6 prefix discovery with 464XLAT according to RFC 7050
- The WLC disables DNS servers and DNS forwarders on managed APs.
- New VPN analysis command 'ikectl' on the command line
- Support for automatic path MTU detection with IPSec.

Bug fixes / improvements

General

- In WEBconfig, only the user data of one selected Public Spot user could be printed. If multiple user records were selected for printing, the printing process ended in an endless loading loop.
- An access via LL2M to a device with hashed password failed and was acknowledged with the error message "user unknown on remote system".
- Creating a Wireshark trace via LCOSCap on a device with a hashed password failed and was acknowledged with the error message "cannot retrieve PSK".

LCOS improvements 10.50.0115 RC2

New features

Wi-Fi

- Support for Fast Roaming over-the-DS

Bug fixes / improvements

General

- After an update to LCOS 10.50 RC1 it could happen that after a configuration synchronization with the LANCOM Management Cloud (LMC) a firewall rule containing a DNS destination could no longer be edited with LANconfig.
- It could happen in individual cases that sessions were not terminated properly (e.g. when using IPSec-over-HTTPS) and the reserved memory was not released again. This caused further packets to be dropped and communication was only possible to a very limited extent.
- When using the LOCALNET station object in firewall rules, routes learned via RIP and BGP were assigned to LOCALNET. This could lead to a high load on the router's CPU due to a large number of filter rules.
  Only networks with the status 'Connected LAN' are now assigned to the LOCALNET station object.

LCOS improvements 10.50.0091 RC1

New features

- Performance optimization due to multicore support for LANCOM ISG-8000 with IPsec VPN
- Support for Bidirectional Forwarding Detection (BFD) with BGP
- (Sub Second) Session Switchover for Dynamic Path Selection (DPS)
- DPS: ICMP measurement intervals now support intervals with a time resolution in milliseconds
- DPS: In addition to ICMP, HTTP(S) is also supported as a measurement method
- Support of the CLAT side of 464XLAT for IPv6-only in mobile communications
- NPTv6 (prefix NAT) support for IPv6
- The load balancer now supports IPv6
- IPv6 line polling support
- In the IPv6 firewall, MAC addresses can be configured as a station object (source).
- In the IPv6 firewall, a delegated provider prefix can be configured as a station object to share a dynamic prefix in a router cascade.
- In applications where DNS names can be configured, the preferred address family (IPv4 or IPv6) can be specified.
- Dynamic Path Selection (DPS) now supports IPv6.
- Support for Curve448 in SSH
- Public Spot now supports IPv6.

- Public Spot: The MAC address format is now configurable.
- Support for RADIUS attributes according to RFC 5580
- The DHCP client now displays the lease time in the status menu.
- The Rx / Tx bandwidth limitation is now also evaluated for 802.1x RADIUS authentication.
- The Layer7 application detection and DNS names in the firewall can now be configured in a common table.
- Support for session cookie and anti-CSRF token in WEBconfig
- Plain text passwords of the main device password are disabled after a device reset.
- The IKEv2 lifetimes are adapted to the current BSI recommendations after a device reset.
- SHA-1 is no longer included in the IKEv2 default proposal after a device reset.
- The delegated IPv6 provider prefix can be transmitted to the VPN peer via IKEv2 routing.
- Support for H.323 in the IPv4 firewall is removed.
- The vRouter now supports KVM as a hypervisor platform.

Bug fixes / improvements

VoIP

- If a VoIP client sent the parameter 'rtcp-rsize' with an outgoing call, the LANCOM router recognized this parameter as 'Invalid' and rejected the 'Invite' with the message "406 SDP - not acceptable". As a result, the outgoing call did not go through.
- With an incoming ISDN call it could happen that the external caller could not hear the called party (one-way voice transmission) because the 'Media Attribute (a): nortpproxy:yes' prevented the transmission of RTP data.
- When using SIP-ALG, it could happen that the port for RTP communication became invalid and an incoming RTP packet was rejected with the message "ICMP Destination unreachable (Port unreachable)". This resulted in a one-way voice transmission on the part of the called subscriber during an outgoing telephone call.
- The Voice Call Manager supports multiple streams with different codecs. However, these must be initialized during the call setup.
  If a call was initially established with one stream (e.g. G.711) and a second stream was added in the re-INVITE (e.g. T.38), the Voice Call Manager could not process the second stream. As a result, data packets of the second stream were not transmitted anymore.

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.