Release Notes

LCOS
10.90 RC3

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 10.90 RC3, as well as the improvements since the previous version.

Before upgrading the firmware, please pay close attention to chapter 7 “General advice” of this document.

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

2. The release tag in the software name

Release Candidate (RC)

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

Release Version (REL)

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

Release Update (RU)

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

Security Update (SU)

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

3. Device-specific compatibility to LCOS 10.90

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

LANCOM devices without support as of LCOS 10.90

→ LANCOM R800V
→ LANCOM LN-630acn
→ LANCOM 1781VA
→ LANCOM 1906VA-4G
→ LANCOM L-322agn (R2)
→ LANCOM LN-862
→ LANCOM LN-860
→ LANCOM OAP-830
→ LANCOM OAP-1700B
→ LANCOM OAP-821
→ LANCOM OAP-822
→ LANCOM IAP-1781VAW(+)

4. Advices regarding LCOS 10.90

General notes on the update

As of LCOS 10.90, the CLI menu for VRRP has been moved from '/Setup/IP-Router/VRRP/' to '/Setup/VRRP/'. The table structure and the associated OID path have also changed due to the support for VRRPv3 and IPv6.
Please note that add-ins for the LMC and any existing scripts for VRRP must be adapted for LCOS 10.90 and higher. Existing scripts for VRRP are not compatible with LCOS 10.90 and higher.

Information on default settings

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

5. Feature overview LCOS 10.90

5.1 Feature highlights

Ensuring business-critical applications with support for eight QoS queues

This feature allows you to configure up to eight different queues (service classes) with corresponding priority levels for network applications (e.g., „VoIP“, „Gold“, „Silver“, or „Best Effort“). Your data packets are assigned to the appropriate Quality of Service (QoS) class through DSCP markings or firewall rules. The gateway then sorts the packets into the correct priority level and ensures that the respective services only use as much upload bandwidth as you have pre-configured for their class, either as a percentage or in Mbps. In this way, it is ensured that important services like VoIP or video calls always receive sufficient bandwidth, even when the network is heavily utilized.

MOBIKE in the VPN for accelerated roaming

With the MOBIKE extension for IKEv2, VPN clients can seamlessly switch between different networks (e.g., from Wi-Fi to cellular) without having to re-establish the VPN tunnel. The LANCOM Advanced VPN Client or LANCOM Trusted Access Client sends an update message with its new IP address to the SD-WAN gateway when switching networks. For you, this means no interruptions during VPN roaming—the connection remains stable.

Proactive against quantum computers: future-proof VPNs with post-quantum preshared keys

The ongoing advancement of quantum computers presents fundamental challenges for traditional encryption technologies, including VPNs. This makes it even more important to prepare accordingly. With post-quantum preshared keys (PQ-PSK or PPK) for IKEv2, you can take the first steps toward enhancing security. This technology adds additional security mechanisms to protect VPN encryption against potential quantum-computer attacks.
Looking ahead, future LCOS versions will successively provide more features to further secure your networks—ensuring full protection even if quantum computers should become capable of breaking traditional encryption methods.

Maximum reliability with VRRPv3 for dual-stack networks

VRRPv3 for IPv6 enables you to implement router redundancy in IPv6 networks or in dual-stack environments (simultaneous use of IPv4 and IPv6). This increases operational security, as if one router fails, another can automatically take over. This function is ideal for modern networks that support both IPv4 and IPv6, as it ensures seamless redundancy in both protocols.

5.2 Further features

→ With LCOS 10.90 RC3, the router can dynamically assign VLANs via RADIUS to IEEE 802.1X clients on the LAN. Complex physical infrastructure, such as dedicated switches, is not required to perform VLAN separation and assignment. Since the router handles the entire LAN security structure, this feature is ideal for small locations.

→ Many other improvements for the administration and operation of modern networks

You can find further features within the individual builds sections in chapter 6 “History LCOS 10.90”.

6. History LCOS 10.90

LCOS improvements 10.90.0109 RC3

New features

→ The interface name of the WWAN module has been renamed from EXT-1 to WWAN-1 in the status menu and SNMP.

→ The status table of the VDSL modem connection history can now be deleted via CLI command.

→ The TCP alive test has been extended to four possible target addresses.

→ The WEBconfig TLS certificate can be obtained via SCEP.

→ The 'Maximum burst size' parameter can be configured in QoS.

Bug fixes

General

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

→ When trying to adjust the parameter 'Unique-Characters' in the console path 'Setup / Config / Passwords / Password-Complexity', it was always set to 0.

→ Users who dial in via the PPPoE server are assigned a RAS route (host route) for communication. In the case of multiple dial-ins, the additional routing entries were not deleted from the routing tables after the main connection was terminated.

In the case of multiple dial-ins, a RAS user ID is now appended to the additional user entries so that these connections can be terminated in a targeted manner.

→ The values in the console path 'Status / PPPoE / Connection-Tags' (SNMP-ID 1.3.6.1.4.1.2356.11.1.28.14) could not be read out via SNMP.

Wi-Fi

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

VoIP

→ The Voice Call Manager could not process SUBSCRIBE request packets (e.g. from an answering machine) correctly and kept executing the associated function. This led to an immediate restart of the router.

LCOS improvements 10.90.0076 RC2

New features

→ Support for IKEv2 EAP-OTP 2FA for the LANCOM Advanced VPN Client macOS

→ The TCP/HTTP tunnel can now also be created via CLI command.

→ **VoIP:** The Voice Call Manager now marks IPv6 RTP packets so that they are also sent to the Urgent Queue of the new QoS.

→ The maximum number of public key authentication attempts in SSH is now configurable.

→ **VRRP:** It is now possible to configure that a WAN connection is monitored, but that the establishment of the WAN connection is not suppressed in standby mode.

Bug fixes

General

→ If the command “find vrrp” was entered in the command line, the path information output did not contain any line breaks.

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

→ On some LANCOM devices connected to the LMC, a stack overlow could occur in the HTTP client, which caused the devices to restart abruptly.

→ In a VRRP scenario with VPN Load Balancer (VLB), in which IPv6 addresses were used, there was a timing problem between the start of the IPv6 VRRPv3 and the VLB after a restart. As a result, the VLB no longer started independently and had to be started manually.

→ A plain Ethernet remote station with a dynamically generated MAC address (‘MAC address type’ set to ‘Local’) of a vRouter operated in Hyper-V was not established, so that the Internet connection could not be established. Furthermore, in such a scenario, several plain Ethernet remote stations with dynamic MAC addresses created in the vRouter could not exchange ICMP packets (ping) with each other.

→ For cellular routers with Quectel 4G and 5G modules, the provider name in the ‘Network’ status field (console path ‘Status/Modem-Mobile/’) was limited to 16 characters. This could cause the name to be truncated.
The following LANCOM cellular routers were affected by this behavior:
- 1800EF-4G
- 1800EF-5G ab HW Rel C
- 1803VA-5G
- 1800VA-5G
- 750-5G
- IAP-5G

VoIP

→ Active calls were not disconnected after deactivating the Voice Call Manager and remained active.

LCOS improvements 10.90.0059 RC1

New features

General:

→ Extensions in QoS: Support of 8 QoS queues for IPv4 and IPv6.
→ Support of VRRPv3 for IPv4 and IPv6
→ Support for dynamic VLAN assignment on the LAN with 802.1X via RADIUS
→ Support of AES-CMAC in NTP according to RFC 8573
→ Support in the syslog client for formatting messages in accordance with RFC 5424
→ Support of TLS in the syslog client
→ Support of MTU 1500 in PPPoE according to RFC 4638
→ A comment field has been added to the Ethernet port table.
→ Support for stable IPv6 Privacy Interface Identifier according to RFC 7217
→ Support for RFC 8268 in SSH for additional DH groups
→ The TR-069 data model is now TR-181 by default.
→ The xDSL connection history is now boot persistent.
→ Support of the IPerf reverse mode parameter
→ The password policy for the main device password can only be configured more granularly.
→ The VDSL/ADSL line code has been updated.
→ Scripts can now also be imported and exported that only contain the encryption of passwords with a user-defined password.
→ A user-defined command has been added to the alive test, which can be executed once during the transition from the error case back to the normal state
→ Support of the Captive Portal API according to RFC 8908 and RFC 8910 in the Public Spot
→ The IAP-5G now supports TR-069, too.
→ The DNS forwarder now also supports administrative distances. If the default route changes due to administrative distances, the DNS forwarder now uses the new, better route.
→ Support of IEEE 802.1ag OAM functions
→ Support for Ethernet Link-OAM 802.3ah Remote Loopback Mode
→ WWAN firmware update support for the 1800EF-4G
→ The reboot command on the CLI now supports the option for time-controlled, one-time execution of the reboot
→ The 1TR-112 priority tagging for VLANs on the WAN connection has been adapted to the current valid standard.

→ Extensions in the IPerf to include additional CLI parameters
→ The ping command now supports the tracepath mode for determining the MTU of the ping destination (option -m).
→ If a logical DSL channel is assigned to two or more physical Ethernet ports, only the first (active) Ethernet port is used. It is no longer possible to operate two or more different active ETH ports simultaneously with one logical DSL channel.
→ Changes or omission for configuration parameters for USB autoload: The configuration and / or script files are only automatically loaded into the device if the device is in the delivery state.

VPN

→ Support for MOBIKE in IKEv2 as a responder role
→ Support of quantum-safe encryption using post-quantum Preshared Keys with IKEv2 according to RFC 8784
→ The subnet mask for IPv4 or prefix length for IPv6 can be assigned to IKEv2 config mode clients.
→ Support for zero encryption in ESP with IKEv2
→ The DH groups used in an active VPN tunnel are now displayed in the status under /Status/VPN/IKE and /Status/VPN/IKE.

Features omitted

→ Omission of Cast128 CBC, Blowfish CBC and DES encryption algorithms in IKEv1
→ Omission of the IKEv1 myVPN feature
→ Omission of analog modem connections and ISDN dial-ins
→ Omission of ISDN location verification
→ Omission of ISDN time reference
→ Omission of CLIP for RAS dial-in
→ Omission of ISDN remote terminal table (for dial-up connections)
→ Omission of the X.25 Bridge
→ Omission of AsyncPPP
→ Omission of Multilink-PPP
→ Omission of LANcapi, Fax
→ Omission of CBCP (Callback Control Protocol) in PPP
→ Omission of Dynamic VPN over D and B channel
→ Omission of the Least Cost Router
→ Omission of the support for external 2G/3G USB modems
→ Omission of the NetBios functions (Netbios-Proxy, NBNS)

Bug fixes

General

→ If an Internet connection could no longer be established (e.g. in the event of a VDSL modem retrain), the error message was displayed twice in WEBconfig.

→ After deactivating the IPv6 interface and deleting the delegation addresses on an IPv6 interface with statically configured delegation addresses, the delegation addresses were still available after activating the IPv6 interface.

→ An IPv6 interface should only not be set up if the DAD (IPv6 Duplicate Address Detection) is not successful for the primary link-local address. However, the IPv6 interface was also not set up if the DAD was not successful for a statically assigned IPv6 address that was checked before the primary link-local address.

→ On cellular routers with Quectel 4G and 5G modules, the field for the RSRP (Reference Signals Received Power) and RSRQ (Reference Signal Received Quality) was skipped when calculating the signal values. This resulted in incorrect and sometimes physically impossible values being output for the RSRP and RSRQ.

→ The following mobile routers were affected by this behavior:

- 1800EF-4G
- 1800EF-5G ab HW Rel C
- 1803VA-5G
- 1800VA-5G
- 750-5G
- IAP-5G

VPN

→ On a router with an IKEv2 client dial-in with RADIUS authentication via EAP-TLS, the router sends the EAP failure in the last EAP response received from the VPN client with the notification AUTHENTICATION_FAILED to the VPN client if the RADIUS server rejects it (e.g. due to incorrect login data).
The router now sends the EAP failure in the last IKE_AUTH response received from the VPN client with the EAP message code FAILURE.

7. General advice

Disclaimer

LANCOM Systems GmbH does not take any guarantee and liability for software not developed, manufactured or distributed by LANCOM Systems GmbH, especially not for shareware and other extraneous software.

Backing up the current configuration

Before upgrading your LANCOM devices to a new LCOS version it is essential to backup the configuration data!

Due to extensive features it is **not possible to downgrade** to a previous firmware without using the backup configuration.

If you want to upgrade devices which are only accessible via router connections or Wi-Fi bridges, please keep in mind to upgrade the remote device first and the local device afterwards. Please see the LCOS reference manual for instructions on how to upgrade the firmware.

We strongly recommend updating productive systems in client environment only after internal tests. Despite intense internal and external quality assurance procedures possibly not all risks can be eliminated by LANCOM Systems.

Using converter firmwares to free up memory

Due to numerous new functions within the LCOS firmware it may not be possible in some circumstances for older devices to keep two fully-featured firmware versions at the same time in the device. To gain more free memory, a smaller firmware with less functionality has to be uploaded to the device first. As a result, significantly more memory will be available for a second firmware.

This installation has to be done only once by using a “converter firmware“.

After having installed the converter firmware, the firmsafe function of the LANCOM device is only available on a limited scale. The update to a new firmware is furthermore possible without any problems.

However, after a failed update the LANCOM device works with the converter firmware which only allows local device access. Any advanced functionality, particularly the remote administration, is not available as long as the converter firmware is active.