LANCOM Release Notes

LCOS

10.30 Rel

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

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

May 9th, 2019, CBuersch

Table of Contents

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 10.30 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 10.30

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

LCOS 10.30 support for LANCOM access points of the E series will follow at a later time.

3. Advices regarding LCOS 10.30

3.1 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 10.30”.

5. History LCOS 10.30

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.