Information regarding

LCOS Software Release 10.12 RC1

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

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

19.07.2017, CBuersch

Table of Contents

1. Preface

LCOS („LANCOM Operating System“) is the operating system for all LANCOM routers, wireless LAN access points and Wi-Fi 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 10.10 RU2, as well as the improvements since the previous version.

Before upgrading the firmware, please pay close attention to chapter 3 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. New Features, improvements, and history

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.

LCOS 10.12.0041 RC1

Currently, devices running LCOS 10.12 RC1 can not be configured or managed via the LANCOM Management Cloud.

New features

General

- LACP - virtual ethernet port bundling for maximized reliability
- Public Spot support for the LANCOM vRouter
- Command for switching the firmware with automatic device restart
- File import per Copy & Paste
- Smart Ticket / SMS - Whitelist for area codes
- Elimination of the port 8080 for WEBconfig and Public Spot
- Content Filter enhancements by further categories
- IPv6 support for the Content Filter

VPN & Routing

- Freely configurable DHCPv6 options
- OSPFv2
- OCSP check in the TLS / Rollout wizard
- Switchable Not-HTTPS communication via port 443 in the Content Filter
- Support of AES-GCM for IKEv2
- Support of the elliptic curve Diffie-Hellmann groups (ECDH) 19, 20, 21, and the ECC Brainpool curves 28, 29, and 30 for IKEv2
- Support of RADIUS CoA for IKEv2
- Load Balancer for IKEv2
- Maximum VPN availability thanks to additional backup mechanics
- Support for TACACS shell authorization
- Variables for IPv6 LAN address and prefix in the action table
- ICMPv4 and ICMPv6 rate limiting
- Support for MD5 in NTP client and server
- NTP server for each ARF net available

Wi-Fi

- Multicast > Unicast transformation for Judder-free IPTV streaming in the Wi-Fi
- As of now, the menus for the Public Spot configuration are generally available within LCOS, but can only be used after successful activation of the Public Spot option.
- 802.1x: Availability check for RADIUS server
- 802.11ac Wave 2 features configurable via WLC
- Coordinated Wireless ePaper channel selection

VoIP

- The SIP user ID field can now be configured
- Overlap Dialing for a faster connection establishment

Bugfixes / improvements

General

- If the validity of an RA certificate ended before the validity of the CA certificate, the SCEP client did not update the RA certificate.
- If the spanning tree functionality on a LANCOM access point was enabled by LANconfig, this change was not saved correctly, so spanning tree was not enabled after saving the device's configuration.
- When uploading a vRouter configuration per WEBconfig, the configuration parameters were only applied completely after a warm boot of the vRouter following the upload.
- When using a backup RADIUS server for device authentication the login was checked on the backup server first, instead on the primary RADIUS server.
- If the DHCP client did a restart within the time of the DHCP request, it could occur that the LANCOM DHCP server did not allocate an IP address to this client after its restart. In this case, the DHCP trace log displayed the message "ARP in progress".
- Proxy-ARP did not work for communication between identical IP networks which are managed by the LANCOM device.
- On an internet connection, which was configured as DS-Lite, a LANCOM device did not use its IPv6 WAN address for IPv6 packets, but its IPv6 LAN address as sender address in some cases.
- A sudden device restart could occur if a periodic 300 seconds request was configured in the LCOS CRL client (LANconfig: "Certificates -> CRL-Client: Retrieve regularly (per CRL)") and the CRL client could not fetch the CRL (e.g., due to an error of the external CA).
- The table "Setup/DNS/DNS-Destinations" (LANconfig: IPv4 -> DNS -> Forwarding) accepted only values smaller or equal than 999 for the parameter "Rtg-tag" (Routing tag).
- The tables for configuring backup and accounting were missing in the LANCOM vRouter under "/Setup/WAN".
- If the command "show script" was entered on the CLI, the output did not contain a sesseion ID, so running scripts could not be stopped by using the command "killscript <Session-ID>".
- The setup menu (/Setup/WAN/RADIUS) for authenticating via external RADIUS server was not available in the LANCOM vRouter.
- An xDSL connection could not be stopped immediately, if the appropriate DSL remote station was detached from the configuration by script.
- Invoking the user-defined rollout wizard could lead to a sudden device restart, if more item values than item texts were defined in the rollout wizard's list box.

VPN

- If a DHCP request should be forwarded via VPN tunnel which got its IP address by config mode, the config mode address was set as GI address in the DHCP header.
- If an existing VPN connection was disconnected by a delete information, the VPN debug trace did not show any information about the disconnect reason.
- Name descriptors for two configurable parameters were missing in the WEBconfig configuration dialogue for IKEv2 rekeying parameters (Configuration -> VPN -> IKEv2/IPSec -> validity period).
- If an IKE connection which should be established between a vRouter and a VPN router was monitored by DPD, frequent disconnections due to a DPD timeout did occur. DPD was not executed properly on the LANCOM vRouter.

Wi-Fi

- The trigger for re-initializing a SCEP client could fail when the client was currently initializing.
- The value for limiting the data volume for automatically generated Public Spot users in the path "/Setup/Public-Spot-Module/Authentication-Modules/User-Template/Volume-Budget" was limited to a maximum of 4.000 Mbytes.
- When creating Public Spot users by HTTP command, a command which was included within the URL was not applied to the created user profile.
- A sudden device restart could occur if the access point provided a WLC tunnel (CAPWAP data tunnel) for Wi-Fi clients and tried to provide an ICMP packet „fragmentation needed" to a Wi-Fi client,because the received data packet was too big for the CAPWAP data tunnel.

VoIP

- If a call was established via an ISDN phone system which is connected to the internal ISDN interface of the LANCOM router, and has a configured a call forwarding to external numbers, unidirectional communication could happen, if the call was finally forwarded to the provider via SIP by the VCM.
- A country code starting with '+' (e.g. +49 for Germany) was not converted to the format 0049 by the LANCOM Voice Call Manager on outgoing calls, so that an ISDN phone station was not able to evaluate the call number.
- If a SIP line was disconnected on the CLI using the command "do /other/manual-dialing/disconnect <Connection>", the LANCOM Voice Call Manager was not informed about that. This resulted in showing lines which used this connection still as being registered.
- Outgoing calls via SIP provider M-net could not be established, because the provider requires a second authentication after authentication via "INVITE", and "PRACK", too.
- If a VoIP provider answered '400 Bad Request' to a SIP line de-registration, the LANCOM Voice Call Manager could not interpret this error message correctly, so the de-registration was constantly repeated.
- If a call group was intended to be used as a backup line, e.g. for a connection to a telephone system, this entry did not work.
- A SIP session which was tagged with a routing tag by a firewall rule and managed by the SIP ALG, could not be established, because the answer packets were tagged with the same tag by the SIP ALG, and thus were discarded by the IP router.
- A SIP line which was registered using OPTIONS packets was interpreted as non-registered line by the SIP ALG, so incoming calls (INVITE packets) could not be assigned correctly.
- Due to the parameter "transport=UDP" in the contact header of a SIP packet some local SIP clients lost their registration to the LANCOM VoIP router after a few minutes.
- An infrequent issue with LANCOM VoIP routers occured at calls with the involvement of the LANCOM N510 DECT station. If an external call on a SIP line reached the LANCOM VoIP router and was answered internally by a handset of the LANCOM N510 DECT, the caller could hear the internal user, but the internal user could not hear the caller.

- A sudden device restart could occur if the received OK packet on a SIP line did not contain an EXPIRES value within the CONTACT header.
- Unidirectional communication could infrequently occur if an incoming call via SIP line was signalled by the LANCOM VoIP router to more than two interfaces (ISDN and analog interfaces).
- A SETUP, which was received on the ISDN and did contain a target number of type "National Number", was not completed with zeroes by the call routing, like it is the case with numbers of type "International Number". Thus, call routing using service numbers did fail.
- After an analog call was finished, it remained in the call counter table of the LANCOM VoIP router in some cases.
- A Linphone SIP client was rejected while registering at the Voice Call Manager (VCM) due to client specific parameters within the registration.

3. Important advice

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

Notes

- 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/lcos/lifecycle-management/product-tables/

Device-specific advice

LANCOM 178x 4G:
To avoid delayed connection establishments within mobile radio (eg in case of backup) it is recommended to use the **latest firmware version 3.5.24 for the LTE mobile modem** (Sierra MC-7710). Please refer also to the following Knowledgebase article: Link

Using converter firmwares

To use any firmware from version 8.8 in your LANCOM 1722 1723, 1724 and in the L-320agn, L-321agn and L-322agn (less than hardware release E), enough space must be available in the memory of your device. Due to the implementation of several new features within the current build of the firmware, it is no longer possible to store two main firmware versions side by side. To gain more free space for the current version, it is now necessary to upload a converter firmware into your device. The converter-firmware has a much smaller size, so that it is now possible to store the main release of the firmware besides the converter-firmware.
This setup is only necessary once for a single device and is done with the so-called converter-firmware (see readme.pdf of the affected devices).
After having flashed the converter-firmware the firmsafe function of the LANCOM device is available only on a limited scale. The update to a newer firmware is furthermore possible. However, in case of an update failure the LANCOM will only work with a minimal-firmware which allows just local access to the device. Any extended functionality, in particular remote administration, is not possible when running the minimal-firmware.

Dynamic VPN registration

By reason of patent you have to register the functionality „Dynamic VPN“ with IP address transmission over ISDN. This operating mode is usually required when you configure a VPN tunnel with dynamic IP addresses on both sides without dynamic DNS services.
Any other Dynamic VPN operation mode (e.g. transmitting the IP address via ICMP, provoking a callback etc.) does not require registration.
The registration process is fully anonymous - no personal or company data will be transmitted.

The registration of the Dynamic VPN option requires administrator rights on the LANCOM device.