SECURE. NETWORKS.

LANCOM
Systems

Information regarding

LCOS Software Release 10.12 SU1

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.

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

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

25.10.2017, 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 10.12 SU1, 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 improvements 10.12.0082 Rel ▶ 10.12.0084 SU1

Bugfixes / improvements

Wi-Fi

- A security issue within WPA2 authentication (KRACK attack) using 802.11r (Fast-Roaming) while in AP mode (base station) has been fixed:

  CVE-2017-13082: accepting a retransmitted Fast BSS Transition Reassociation Request and reinstalling the pairwise key while processing it

  Please check with the manufacturer of your Wi-Fi client for the availability of updates. These devices need to be updated, too.

- A security issue within WPA2 authentication (KRACK attack) using WLAN client mode / WLAN station mode with 802.11ac-Wi-Fi modules as well as while using P2P connections with 802.11ac- and 802.11a/b/g/n Wi-Fi modules has been fixed:

  CVE-2017-13077: reinstallation of the pairwise key in the Four-way handshake
  CVE-2017-13080: reinstallation of the group key in the Group Key handshake

  The WLAN client mode / WLAN station mode with 802.11a/b/g/n Wi-Fi modules is not affected.

Note:

LCOS is not affected by the following WPA2 security issues (KRACK attack):

CVE-2017-13084: reinstallation of the STK key in the PeerKey handshake
CVE-2017-13086: reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake
CVE-2017-13087: reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame
CVE-2017-13088: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame
CVE-2017-13078: reinstallation of the group key in the Four-way handshake
CVE-2017-13079: reinstallation of the integrity group key in the Four-way handshake
CVE-2017-13081: reinstallation of the integrity group key in the Group Key handshake

LCOS improvements 10.12.0059 RC2 ► 10.12.0082 Rel

Bugfixes / improvements

General

- After a restart of the LANCOM device all ports remained in disabled status, although Spanning Tree was activated.
- An LMC domain which was allocated per DHCP option was ignored by the LANCOM device when it was working as a DHCP client.
- An ADSL connection with encapsulation VC-MUX and transparent Layer-2 (instead of PPPoE) could not be established successfully.
- After the lease time expiration no new IP address was obtained by an Internet remote station with layer DHCPoEoV, and the connection was temporarily cut.
- If a server in the DMZ was sending too big packets (bigger than the MTU of the target remote station) with activated DF bit (don't fragment) to a LANCOM router, the router did not answer with an ICMP error message "fragmentation needed" and discarded these packets.
- If a VLAN ID was stored in the network definition of the LANCOM Management Cloud which was bigger than 999, this configuration was not accepted, although VLAN IDs up to 4096 are allowed in network definitions.
- If an NTP server was configured within the network INTRANET, the configuration of the device could not be written back by LANconfig after any configuration change.
- Within a bridge group (e.g. BRG-1), routed multicasts (e.g. video streams to DSL-1) were bridged to the interface LAN-1 past the IGMP snooping and to WLAN-1, too, if a client was registered to the wireless network. This caused the wireless network to be flooded with multicast packets with increasing Wi-Fi channel load, resulting in a wireless connection which was not performing well.
- In a VRRP load balancing scenario with RIP, ICMP redirects were sent with the source IP address of the ARF context instead of the VRRP IP address.
- No data was transmitted through an EoGRE tunnel which had not been allocated any bridge goup under interfaces > LAN > Port table.

Wi-Fi

- By AutoWDS, no point-to-point connection could be established between LANCOM access points. The configured access points for AutoWDS were shown under the appropriate SSID in LANmonitor, but no connection could be established.
- Clients which were registered initially to the LANCOM Public Spot could not connect to the WAN, because DNS requests of the initial domain were not forwarded to the preceding device (which provided WAN access).
- When reading the configuration of a LANCOM WLAN controller by LANconfig the wireless IDS profile "Default" was not read, which caused that the configuration data could not be written back to the LANCOM WLAN controller.

VoIP

- If WEBconfig's "Configure Voice-over-IP / All-IP" setup wizard was used for configuring an All-IP connection, the configured ISDN interface remained in "off" status after the wizard was finished.
- If the "busy on busy" function was enabled for a user within the user settings of the LANCOM Voice Call Manager (Voice Call Manager > Users > User Settings), this user could not receive any calls.

VPN & Routing

- An IKEv2 connection with a digital signature profile „RSASSA-PSS with SHA-384 and SHA-512" could not be established.
- If no IPv4 address pool was created for an IKEv2 client connection, an IKEv2 client who got an IP address by the LANCOM router via IKE config mode did not get a DNS server entry. The LANCOM router allocates its own IP address as a DNS server address to the IKEv2 client if no IPv4 address pool was created.
- On an IKEv2 connection which was authenticated by IKEv2 RADIUS no outgoing data was sent after 24 hours. The lifetimes for RADIUS authentication had not been applied correctly by the LANCOM router.
- Only UDP and ICMP packets were transmitted through an established VPN tunnel on an IKEv2 connection with AES-GCM encryption. TCP connections did not work at all (SSH, HTTPS etc.).
- If the command "show vpn" was entered on the command line of a LANCOM router, the output displayed VPN rules of configured IKEv2 connection as IKEv1 rules.
- If a masked IKEv2 VPN connection between two LANCOM routers was established with a one-sided transparently accessible DMZ (masking settings "only Intranet"), the DMZ was masked, too.
- Dynamic VPN connections (IKEv1 via UDP) between two LANCOM routers with a private IP address on the Internet connection for the dynamic site (behind a NAT router) could not be established. A dynamic VPN connection via ICMP worked.

LCOS improvements 10.12.0041 RC1 ► 10.12.0059 RC2

New Features

General

- WAN access availability can now be configured for the COM port server
- Dynamically generated VLAN memberships can be shown on the CLI using the ‘show vlan’ command.
- Updated service lists for the Layer 7 application detection
- The Layer 7 application detection now supports QUIC session detection.
- Support for Ethernet OAM based on 1TR112

Wi-Fi

- The driver for the IEEE 802.11ac Wave1 Wi-Fi module of the following devices has been updated: LN-630acn dual Wireless, LN-830acn dual Wireless, LN-822acn dual Wireless, LN-830E Wireless, L-1310acn dual Wireless, L-1302acn dual Wireless, IAP-821, IAP-822, OAP-821, OAP-822, OAP-830

VoIP

- ‘Busy-on-Busy’ is now configurable for call groups

Bugfixes / improvements

General

- The category ‘Cloud applications’ was defined as forbidden within three default Content Filter profiles. This was now changed to ‘allowed‘.
- The time which is periodically set by the LANCOM Management Cloud (LMC) was overwritten by a WLAN controller within the same network while announcing the time to a managed LANCOM access point.
- The option for configuring the LACP interfaces ‘Bundle-1’ and ‘Bundle-2’ was missing in the configuration interface of the LANCOM 1783VAW.

VPN & Routing

- If VPN connections using AES-GCM encryption were terminated on a LANCOM router, the values for the columns ‘Crypt-Alg’ and ‘Hash-Alg’ were missing in the LCOS table /Status/VPN/ESP.
- If only default routes with a routing tag different from 0 were configured on a LANCOM Router, IKEv2 connections could not be established, if the IKEv2 peer was not recognized by its IP address.
- Further IPSec rules were created if solely a super ordinate IPSec rule (e.g. ANY-to-ANY) was defined for a VPN remote station, but also one or more N:N NAT entries were defined for this VPN remote station, which included the super ordinate IPSec rule.

Wi-Fi

- The country profile 'Australia' has been fixed.
- ARP packets are now transmitted reliably when using the client bridge mode with IEEE 802.11ac capable Wi-Fi modules.
- If profiles were defined under 'Public-Spot > Wizard > Bandwidth profiles', the according values were displayed swapped later in the wizard and on the voucher.
- The IEEE 802.11ac module of a LANCOM access point was sending beacons with a data rate of 1 Mbps in the 2.4 GHz band in 802.11gn/mixed mode, as well as in Greenfield mode. This lead to beacons being visible even on an 802.11b client, although the 802.11b mode was disabled in the access point configuration.
- No logout link is shown on the status page for the Public Spot authentication mode 'login via agreement'.
- On the login page of the Public Spot gateway the page containing the terms of use could not be displayed for apple clients, if the Public Spot authentication method was set to 'Login data will be sent by e-mail / SMS'.

  If a Public Spot was operated on a router with Wi-Fi module, and an access point within the same network broadcasted the Public Spot SSID, too, the entry for a client was deleted from the auto relogin table if the client was roaming from the router to the access point. This caused an additional login to the Public Spot.
- A negative value was shown in LANmonitor for managed access points after radio field optimization on a LANCOM WLAN controller.

VoIP

- Unidirectional communication could occur while operating a VoIP line (SIP trunk) over BNG as internet connection and using an ISDN phone system behind a LANCOM VoIP router. The internal ISDN user could not hear the external subscriber anymore.
- Phone calls from an internal SIP phone system via a LANCOM VoIP router to a 'Deutsche Telekom' SIP trunk line were disconnected after approx. 15 minutes.
- If one or more prefixes for internal calls were configured in the menu 'Voice-Call-Manager > Advanced', the configured prefix was not added to the source call number. Thus, an outgoing call could not be established.
- After successful registration of a SIP line via IPv6 incoming calls did not work due to INVITE packets were answered with 'ICMP port unreachable' by the firewall of the LANCOM VoIP router. This happened even though an existing inbound firewall rule was configured for the SIP server.

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

- IKEv2 Load Balancer for load balancing of incoming VPN connections
- 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.