LANCOM Release Notes
LCOS 10.20 RC1

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

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

20.06.2018, 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 10.20 RC1, 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 10.12.0378 RU7 > 10.20.0097 RC1

As from LCOS 10.20, support for the following devices is discontinued it LCOS 10.20

- LANCOM IAP-321
- LANCOM IAP-321-3G
- LANCOM OAP-321
- LANCOM OAP-321-3G
- LANCOM OAP-322
- LANCOM IAP-3G
- LANCOM 1781A-3G

New features

General

- LANCOM vRouter: Support for Microsoft Hyper-V
- LANCOM vRouter: Support for firmware updates via UPX files
- WEBconfig: Requests for the unencrypted site on port 80 are automatically redirected to the secure site (port 443). This behavior is activated automatically after a device reset.
- ‘Boot-Cause’ is available as an environment variable.
- The RADIUS server supports user-defined RADIUS attributes per RADIUS user.
- A search on the CLI is possible via ‘find’ command.
- Administrators from the table ‘Further administrators’ do no longer have read- or write permission within this table.
- The readscript option ‘-o’ suppresses the output of passwords within scripts.
- The DSCP tag for internal services can now be configured.
- Physical Ethernet ports are now enclosed within the Ifx- and If-tables of the SNMP-IF-MIB.

Routers & VPN

- The configuration logic of the IPv6 WAN interfaces has been changed.
- WAN Policy-Based NAT: WAN Policy-Based NAT allows address translation (masking) of connections based on firewall rules.
- DSL bridge mode for all LANCOM VDSL routers: As of now, all VDSL routers can be set into a DSL bridge mode.
- OCSP responder/server for online certificate check
- Support for LISP (Locator/ID Separation Protocol)
- Configurable target port for IKEv2 and switchable encapsulation (UDP, HTTPS)
- Adaption of the IKEv1/IPSec default crypto algorithms to current standards
- Adaption of the TLS default crypto algorithms to current standards
- Adaption of the SCEP default crypto algorithms to current standards
- BGP: Support for LISP route redistribution
- BGP: The administrative routing distance can be configured per policy.
- A particular sender address can be configured for DNS forwarding.

- Besides the Rollout wizard another four programmable WEBconfig wizards can be uploaded.
- The form for Dynamic VPN registration is no longer available
- Enhanced support for DHCP option 43 in the DHCPv4 server
- Support for DHCP option 82 in the DHCPv4 server
- A sender address (loopback address) can be configured via the DHCP relay agent.
- The function automatic WAN tag creation has been omitted, see knowledgebase article
- Option for automatic WAN tag generation omitted.
- The switch for configuring the building of the IPSec SAs is no longer available. IPSec SAs are now built combined.

Wi-Fi

- **WLAN Client Management**
  WLAN Client Management permanently directs Wi-Fi clients to the ideal access point and frequency band. As a consequence, this feature improves the quality of wireless networks regardless of their dimension - whether or not in standalone operation or orchestrated via the LANCOM Management Cloud. The popular, but so far separated functions Band Steering and Client Steering are hereby combined and provided even without operating a WLAN controller.
- **LEPS-U**
  LEPS-U (LANCOM Enhanced Passphrase Security - User) gives you the opportunity to specify an individual Wi-Fi password for an SSID for individual clients or whole groups.
- Public Spot user accounts / RADIUS user accounts can be imported and exported via CSV files.
- Public Spot with login after statement of agreement: The point of time for the the day account limits reset is now configurable.
- Active Public Spot sessions are terminated when deleting the user via the ‘Manage user’ wizard.
- The former Public Spot user list has been removed and is no longer supported. Existing configurations are converted to RADIUS entries automatically.
- Support for a dynamic negotiation of the PoE power via LLDP instead of class-based
- Support for DSLoL over WLAN for all access points and Wi-Fi routers
- The configuration item ‘Transfer only unicasts, suppress broad- and multicast’ is now available for LANCOM WLC devices.
- The WLC-controlled automatic radio field optimization now considers DFS channels, too.

Bugfixes / improvements

General

- In the LCOS path '/Setup/Certificates/SCEP-CA/Client-Certificates' the fields 'Challenge-Passwords' and 'General-challenge-password' were not defined as password fields.

Routers & VPN

- When specifying an IKEv2 remote gateway, a maximum of 40 characters could be used. This value has been increased to 64 characters.

Known issues

- Obtaining DHCP addresses via WLC- or EoGRE tunnel may fail due to IP packet related processing problems. Rarely, this may lead to a sudden router restart, too.

LCOS improvements 10.12.0292 RU6 > 10.12.0378 RU7

New features

- Support for the Mediasec headers for encrypted VoIP connections
- IKE packets are now tagged with DSCP CS6 for prioritization.

Bugfixes / improvements

General

- If VLAN and VRRP was configured simultaneously per LANconfig on the slave router, or the configuration was imported (from a regular configuration file or script), the router did not see the VRRP packets of the VRRP master. This resulted in the slave router propagating itself as VRRP master.
- If a long name for a cellular network was specified in the configuration of a LANCOM cellular router, a firmware update could cause a sudden router restart with a fallback to the previous firmware.
- Minimum bandwiths set up under LCOS 10.12 RU6 did not work when solely an Internet connection of the type „PPP over Ethernet (PPPoE)“ or „IP over Ethernet (IPoE / DHCPoE)“ was configured on the device.
- Cloud-ready devices connect to the LANCOM Management Cloud autonomously via PSK. If this process was denied once by the pairing server, the device still tried to connect using the PSK, even if the user wanted to connect the device manually by using an activation code.
- An additional “5” was added to the IP address in the LLDP standard MIB. This could lead to problems if monitoring applications tried to read the IP address of a device.
- If both VDSL modems were used by a LANCOM 19xx device, a connection establishment to an Internet site which was configured on the VDSL1 interface could lead to an error message on the VDSL2 interface.

Routers & VPN

- A sudden device restart could occur with certificate-based VPN connections, if the device tried to establish a VPN connection before the certificate was created, while its creation was still in progress by the SCEP client.
- Infrequently, a sudden device restart could occur if the VPN load balancer was activated on the device, and a script containing VPN parameters was uploaded to the device.
- If a faulty certificate container was referenced in the configuration for a certificate-based IKEv2 connection, this could lead to a sudden device restart.

Wi-Fi

- A sudden device restart could occur, if the IP address was written faulty in an iperf bandwidth test (e.g. „iperf c 192.168.5022“).
- In a Public Spot scenario which accepts logins via a VLAN-separated LAN interface, it could happen that previously logged in Public Spot users who afterwards changed their VLAN could no longer communicate with the network.
- When using DSLoL as remote site type it could happen with LCOS 10.12 RU6 that the remote station did no longer work.
- A Spectral Scan with a LANCOM 1783VAW was not started in a new window (like usual), but in the same window. Pressing the “back” button in that window did not terminate the Spectral Scan. Only a router restart terminated the Spectral Scan.

VoIP

- If a LANCOM VoIP router received an „INVITE“ which SDP part contained two m-lines, the device answered with a SIP packet containing only one m-line in the SDP part. This was not RFC-compliant and could lead to failed calls when interacting with third-party manufacturers.
- Outgoing encrypted calls to the provider Telekom were rejected, if the SIP line was configured for „Signaling encryption“. The “INVITE” was answered with a „503 Service Unavailable“.
- On outgoing calls of an extension only the main office number was transmitted. The “P-Preferred Idenitity” was not set correctly by the SIP mapping.
- On incoming calls to a Telekom SIP trunk the LANCOM Voice Call Manager did not forward the PAI header parameter “user=phone“ to the SIP user.
- If a SIP PBX line was established from a LANCOM VoIP router to a preceding O2 box, it could happen that incoming calls were rejected by the LANCOM router showing the message „Missing Mandatory Headers“.
- The LANCOM VoIP router deleted SIP calls which were terminated by a connection timeout. As a result, the remote station was not informed with a CANCEL message.

LCOS improvements 10.12.0243 RU5 > 10.12.0292 RU6

New features

- When selecting a mobile radio network depending on signal quality, you can now create a blacklist for allowed mobile radio networks.
- The service lists of the layer-7 application detection have been updated.
- The devices L-1302acn dual Wireless and L-1310acn dual Wireless indicate a non-sufficient PoE power supply by a permanent orange power LED.

Bugfixes / improvements

General

- Cisco cable modem types 3208, 3212, and 3925 stopped working due to an incorrectly assembled TCP packet by the LANCOM router, and could only continue to work after restarting them. The incorrectly assembled TCP packet is no longer sent.
- A router which was managed via TR-069 (Carrier device management↱) and IPv6 could not be accessed by its WAN IPv6 address after taking over the configuration.
- The layer-7 application detection showed a massive increase of the kbps counter for the category "unknown" within two minutes.
- If DTMF signaling was configured to „Telephone events – fallback to in-band" for SIP users (Voice Call Manager > SIP users), as well as for SIP lines (Voice Call Manager > SIP lines > Advanced), events were transcoded into RTP events on incoming calls.
- If the command "default -r" was inserted after the parameter "flash no", and the command "flash yes" was deleted from the end of a script which was generated using the command "readscript -m -i", a sudden router restart occurred, if the modified script was executed using the command "beginscript" and inserting the script file.
- If the configuration snapshot of a device within a cluster scenario which had to be synchronized was bigger than 1 Mbyte, config sync did not work.

Routers & VPN

- If a firmware update to LCOS 10.12 SU3 was performed on the initiator of an IKEv2 connection with configured IKEv2 load balancing, the VPN connection to the IKEv2 load balancer could no longer be established.
- The CA status of the LANCOM 9100+ generated the error message „Maximum size of certificate list reached. No new certificates will be created.". Due to that, no new certificates could be created, because the certificate sizes were limited by the CA.
- After optimizing GRE, routing performance of GRE tunnels has been improved by approx. 15% (LAN-LAN and LAN-WAN).
- When using multiple Internet connections and IKEv2-VPN connections, delete notifications were routed via the false Internet route when changing the Internet connection.

Wi-Fi

- When using iPhones in a Wi-Fi network broadcasted by a LANCOM LN-17xx access point, issues could occur while transmitting data which could only be fixed by a short disconnect of the Wi-Fi connection.
- Due to a faulty transmission of CAPWAP packets, a sudden restart of a LANCOM WLAN controller could occur.
- In big networks it could happen that ARP replies could not be transmitted when using P2P connections, a client bridge, or Auto WDS.
- With 802.11ac access points and enabled station monitoring high Wi-Fi data throughput could cause high CPU load and high channel load. This led to a dissociation of the Wi-Fi client from the Wi-Fi network.

VoIP

- In the menu „Voice Call Manager > Extended > Quality of Service > Prioritize outgoing packets“ the value „PMTU reduction & fragmentation“ was set as the default after a factory reset, although the default value „PMTU reduction“ should be set.
- When transferring a fax with T.38 (Deutsche Telekom), a ReINVITE of the LANCOM router was acknowledged with „200 OK“ by the Deutsche Telekom. Anyway, the fax transmission failed.
- While no call routing rule was executed, a conversion of the call number was done in the FROM field from „+“ to „00“. This did not comply with the E.164 format.
- When using call groups, it could happen that the „Busy-on-Busy“ flag was not transmitted accurately. This could cause unwanted multiple calls. The „Busy-on-Busy“ flag is now transmitted even if „Busy-on-Busy“ is disabled in the router’s configuration.
- After having updated to LCOS 10.12 RU5, it could happen that calls to particular end devices (e.g. SNOM-phones) were no longer put through.
- A sudden VoIP router restart could occur if an analog user cancelled a mistakenly dialed number while call establishment.

LCOS improvements 10.12.0242 RU4 > 10.12.0243 RU5

Bugfixes / improvements

General

- Issues concerning the config reset have been fixed.

LCOS improvements 10.12.0147 SU3 > 10.12.0242 RU4

New features

- Besides the realm types „Mail Domain“ and „MS Domain“, the RADIUS server now supports the realm type „MS-CompAuth“ by default.
- The devices LANCOM LN-1700, LN-1702, LN-860, and LN-862 indicate a non-sufficient PoE power supply by a permanently orange power LED.
- The VDSL line code for devices of the LANCOM 1781, 1783, 1784, R800, R88x series, and for the LANCOM 730VA has been updated.
- Connection establishments and clearings and connection errors of SIP lines are now saved to the syslog.
- Blocked IPv4 routes for RFC 1918 networks are no longer activated by default in new configurations.
- Devices managed by the LMC can now synchronize local configuration changes with the LMC on demand.

Bugfixes / improvements

General

- No WAN statistics were sent per SNMP which caused missing displays in e.g. LANmonitor.
- While checking for free addresses, the DHCP server blocked addresses tagged as already allocated with the maximum lease time. These addresses are now blocked for only five minutes.
- The default rule for the Content Filter in the IPv6 firewall captured all protocols and all stations to all stations.
- SNMP access to a LANCOM router was not possible via WAN interface, if the SNMP right “read only” was configured for the WAN interface’s access rights.
- In some cases routes with activated “sticky for RIP“ were not propagated accurately per RIP protocol.
- The LANCOM ARP implementation included a check to discard received ARP packets with a sender MAC address and set group bit (multi- / broadcast). This could cause a non-functioning layer-2 communication and e.g. a failed ping to a local server.
- Port forwarding of the UDP port 500 did not work as expected in some scenarios.
- If a configuration was read as script, it could not be written back accurately due to error messages within the Public Spot module.
- If a configuration snapshot for synchronizing was bigger than 1 Mbyte, a parameter alignment could not be done by config sync.
- Static routes can be distributed per route redistribution in OSPF. After a restart of the LANCOM router the route was deleted from the OSPF database, and thus could not be distributed via the LSAs.
- If a LANCOM router received a time request (NTP via UDP) which contained a “0” checksum, the request was rejected by the internal router service.
- DHCPoE based Internet connections which received an additional masquerading address used this address only for half of the DHCP lease time. On a DHCP renew the address got lost and from that time on the address which was received by DHCP was used.

Routers & VPN

- Statically configured routes on VPN tunnels are now propagated per route redistribution by OSPF.
- No data was transmitted through a VPN tunnel if an IKEv2 connection was established via IPSec-over-HTTPS mode. Affected were IKEv2 connections between two LANCOM routers, and IKEv2 connections between Advanced VPN Client and a LANCOM router, too.
- If an additional administrator account should be created using WEBconfig, some fields for configuration parameters and checkboxes for functional rights were missing on the GUI.
- With some browsers the WEBconfig configuration interface could freeze and the CPU load of the configured router could increase to 100% if the setup wizard „Provide remote access“ was used in combination with the option „VPN client with user-defined parameters“.

Wi-Fi

- Devices with 802.11ac Wave1 Wi-Fi modules could suddenly restart which was caused by a faulty reset of the Wi-Fi module.
- EAPoL packets for 802.1X authentication were not forwarded by the access point, if protocol filters were configured on the devices (under Wireless-LAN ↑ Security ↑ Protocols), which should discard packets from clients. An explicit “allow” filter for EAPoL packets (Ethertype 888e) solved the problem.
- After a firmware update to LCOS 10.12 SU3 LANmonitor displayed no value for „TX rate (to remote site)“ for point-to-point connections.
- The Spectral Scan function of WEBconfig led to a freezing browser tab after a short time, so that no Spectral Scan data could be displayed anymore.
- If no template cache was activated for a Public Spot template page, it could happen that the login page of the Public Spot could not be invoked after some time. For devices with more than 128 Mbytes of RAM the template cache is now enabled by default.
- When activating a Public Spot option on a LANCOM device the needed folders were not created in the LCOS menu tree. The folders were then created only after a manual device restart.
- After a firmware update to LCOS 10.12 SU3 it could happen in some cases, that a previously working point-to-point connection could no longer be established. This behavior was only seen when the spanning tree protocol (STP) was activated, too.
- After a firmware update it could happen that some Wi-Fi clients could not connect if the Wi-Fi protocol filter was enabled.

VoIP

- When using the LANCOM router as a VoIP gateway, bandwidth reservations for telephony could cause an Internet communication loss in certain cases.
- A CANCEL request which was received by the LANCOM router while establishing the call was not forwarded to the phone. The call was still indicated at the phone.
- "SIP" was written in capital letters within the URI of a SIP packet's route header, which was not conforming to RFC and could result in calls being ended after 30 seconds.
- If an UnREGISTER packet was unanswered, further UnREGISTER packets were sent instead of a normal REGISTER packet, which caused that a SIP line could not be registered at some providers.
- Calls with suppressed caller number could not be put through if they were sent via trunk lines which needed a SIP-ID within the „FROM" header.
- If a T.38 ReINVITE was answered directly with a „487 Request Terminated", the LANCOM router did not immediately terminate the call. As a result, no more faxes could be received.
- Calls failed which should be forwarded from a DECT user (connected via DECT base station 510) to a SIP or ISDN user. While forwarding, the DECT base station added a second (proxy) authorization field to the SIP header which could not be handled by the LANCOM Voice Call Manager.
- After a loss of the primary WAN connection registered SIP lines were not reconnected after switching to an available LTE backup.
- The table for analog users was reduced from four to two entries in LCOS version 10.12 REL, which resulted in a deletion of the third and fourth user on a firmware update.
- The Voice Call Manager did not evaluate the allow headers of received SIP packets, but added his own, fixed allow list when putting through a call.
- If a VoIP configuration was written to the device by the setup wizard, and a call was put through via the still existing VoIP configuration in that precise moment, a sudden device restart could occur.

LCOS improvements 10.12.0146 RU2 > 10.12.0147 SU3

Bugfixes / improvements

Security update for LANCOM routers, gateways, access points, and WLAN controllers

This update fixes a security-related vulnerability in the management functionalities.

Potentially affected are all devices running the following firmware versions:

- LCOS 10.12 REL, SU1, RU2
- LCOS 10.10 RU2, 10.10.0165 PR, 10.10 RU4
- LCOS 9.24 RU6, SU7, RU8

This update is recommended for these devices. All other versions are not affected.

LCOS improvements 10.12.0084 SU1 > 10.12.0146 RU2

New features

- The driver for the IEEE 802.11ac Wave1 Wi-Fi modules of the following products was updated:
  LN-630acn dual Wireless, LN-830acn dual Wireless, L-1310acn dual Wireless, L-1302acn dual Wireless, IAP-821, IAP-822, OAP-821, OAP-822, OAP-830
- vRouter licenses of type „vRouter 500" can now be activated.
- Zero touch provisioning with the LANCOM Management Cloud: By default, LANCOM routers with Ethernet WAN port connect to the LANCOM Management Cloud via DHCPoE using the WAN port.

Bugfixes / improvements

General

- Writing the configuration via LANconfig per TFTP or serial interface was not possible if the LANCOM device did not have an activated Public Spot Option.
- A configured WWAN connection (LTE or UMTS) on a LANCOM 1780EW-4G+ could sporadically not be used, because the mobile radio module did no longer get an IP address per DHCP.
- 2G (GPRS) could be configured as fallback for mobile radio connections on a LANCOM 1780EW-4G+, although the device does not support it.
- The LCOS-internal CA hierarchy which creates the device certificates for HTTPS connections to the device was faulty for the LANCOM 7100(+) VPN, 9100(+) VPN, WLC-4025+, and WLC-4100. Due to this, device certificates were not accepted by the web browser.
- A failed SCEP request prevented the execution of further SCEP requests, although the request was for a different certification site.
- A connection to a DHCPoE remote site could not be established if the allocated DSLoL interface of the remote station was allocated to a bridge group.
- If the iperf command was entered incomplete or abbreviated on the LANCOM device's command line (e.g. „iper" instead of „iperf"), the iperf server started displaying a warning message.
- Two servers could not be specified as target under /Setup/DNS/DNS Destinations, if one or both were extended by a ‚@' character. You can add a routing tag using the '@' character.
- Information about the configured BOOTP server under "Boot images" was missing in the DHCP offer for a BOOTP client.
- No objects containing the ‚@' character could be created in the firewall (LCOS menu tree: /Setup/IP-Router/Firewall/Objects; LANconfig: Firewall/QoS > IPv4 rules > Station objects), although the allowed character set included the '@' character.
- Packets which should be deferred by a firewall rule were transmitted if two QoS rules with activated linking were active in the firewall ("Observe further rules after this rule matches"), and the packets matched to one of these rules.

Routers & VPN

- A sudden device restart could occur when IPSec disconnection and delivery of a data packet, still belonging to the disconnected session, happened simultaneously.
- It was not possible to execute more than one Dynamic VPN negotiations simultaneously. Due to that, the corresponding VPN tunnels could not be established.

Wi-Fi

- A configured transmission power reduction for the IEEE 802.11ac module was not observed in subband 2. The reduction was calculated on the EIRP and not, as desired, on the maximum transmission power of the module.
- The function „Adaptive RF Optimization“ was enhanced by a channel usage rating by other Wi-Fi devices.
- The WPA rekeying mechanism did not work as expected due to a missing rekeying ID.

VoIP

- A SIP line could lose its registration if the DNS name of the registrar was resolved by a DNS server which supplied a TTL=0.
- Setting a call prefix to a SIP remote station under „Voice Call Manager > Lines > SIP Lines > ...“ resulted in forwarding the calling numer in an invalid format (e.g. 0+49), because the international dial prefix was not converted (e.g. from +49 to 0049).
- If an incoming Voice-over-IP call was signaled for longer than 120 seconds without being answered and was then cancelled by the provider, the call remained in the calling list with status “ringing”.

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-830E Wireless,
  LN-822acn dual 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 cannot 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.

Routers & 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

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.

General 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/

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.

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.