Release Notes

LCOS

10.20 SU12

Table of contents

03 **1. Preface**

03 **2. The release tag in the software name**

04 **3. Device-specific compatibility to LCOS 10.20**

04 **4. Advices regarding LCOS 10.20**
04 Information on default settings
04 Information on the LANCOM vRouter

05 **5. Feature overview LCOS 10.20**

05 **5.1 Feature highlights LCOS 10.20**
05 WPA3 - State-of-the-art Wi-Fi security
05 Auto Updater – always up-to-date
05 Client Management – for best-ever Wi-Fi
05 LEPS-U & LEPS-MAC
05 WAN Policy-Based NAT

06 **5.2 Further features LCOS 10.20**
06 Enhanced Open
06 DSL-Bridge-Mode
06 OCSP responder – more power for Smart Certificate
06 LISP (Locator / ID Separation Protocol) support
06 Public Spot CSV import

LANCOM SYSTEMS

September 10th, 2024, CBuersch

07 **6. History LCOS 10.20**
07 LCOS improvements 10.20.0642 SU12
08 LCOS improvements 10.20.0639 SU11
08 LCOS improvements 10.20.0637 SU10
09 LCOS improvements 10.20.0485 SU9
09 LCOS improvements 10.20.0484 RU8
10 LCOS improvements 10.20.0482 RU7
12 LCOS improvements 10.20.0455 RU6
13 LCOS improvements 10.20.0446 RU5
16 LCOS improvements 10.20.0369 RU4
17 LCOS improvements 10.20.0355 RU3
20 LCOS improvements 10.20.0298 RU2
22 LCOS improvements 10.20.0259 RU1
26 LCOS improvements 10.20.0175 Rel
27 LCOS improvements 10.20.0145 RC2
29 LCOS improvements 10.20.0097 RC1

32 **7. General advice**
32 Disclaimer
32 Backing up the current configuration
32 Using converter firmwares to free up memory

1. Preface

The LANCOM family of operating systems—LCOS, LCOS SX, LCOS LX, and LCOS FX—forms the trusted basis for the entire LANCOM range of products. Within the scope of the hardware specified by the products, the latest firmware version is available for all LANCOM products and is offered by LANCOM Systems for download free of charge.

This document describes the innovations within LCOS software release 10.20 SU12, as well as the improvements since the previous version.

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

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

2. The release tag in the software name

Release Candidate (RC)

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

Release Version (REL)

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

Release Update (RU)

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

Security Update (SU)

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

3. Device-specific compatibility to LCOS 10.20

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 10.20, support for the following devices is discontinued:

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

4. Advices regarding LCOS 10.20

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.

Information on the LANCOM vRouter

If you had initially installed a vRouter instance using LCOS 10.20 RC1 or LCOS 10.20 RC2, it is necessary to reinstall the vRouter with LCOS 10.20 Rel.
The LANCOM vRouter for Microsoft Hyper-V will be available with a future LCOS release update.

5. Feature overview LCOS 10.20

5.1 Feature highlights LCOS 10.20

WPA3 - State-of-the-art Wi-Fi security

The latest generation of Wi-Fi encryption - WPA3 (Wi-Fi Protected Access) - now offers you more security for your WLAN infrastructure. As the successor of WPA2, WPA3 offers important extensions and security features for small („WPA3-Personal“) and large networks („WPA3-Enterprise“). With LCOS 10.20, all LANCOM access points and WLAN routers support the new Wi-Fi security standard. Learn more in our Whitepaper

Auto Updater – always up-to-date

The Auto Updater keeps your installations up-to-date automatically: If desired, LANCOM devices can search for new software updates, and download and install them without any user interaction. You can choose whether to install only security updates, release updates, or all updates automatically. If automatic updates are not desired, the feature can still be used to check for new updates, which can then be installed with a single click.

Client Management – for best-ever Wi-Fi

Client Management steers Wi-Fi clients to the best available access point and frequency band. This feature improves the quality of wireless networks of all sizes—whether they operate stand-alone or orchestrated by the LANCOM Management Cloud. The popular Band Steering and Client Steering, which so far were separate features, have now been combined and even operate without a WLAN controller.

LEPS-U & LEPS-MAC

Keep control of who is in your Wi-Fi. With LEPS-U (LANCOM Enhanced Passphrase Security – User), individual clients or entire groups each receive a unique Wi-Fi password for an SSID. Using LEPS-MAC, you additionally authenticate the clients by their MAC address—ideal for secure corporate networks.

WAN Policy-Based NAT

WAN Policy-Based NAT allows an easy assignment of static WAN IPv4 addresses to desired services. Due to a NAT action in the firewall rules internal addresses are masked behind a WAN address from the Internet access provider. Ideal for scenarios e.g. for the operation of mail servers and web servers with different WAN addresses.

5.2 Further features LCOS 10.20

Enhanced Open

Thanks to the introduction of additional data encryption, Enhanced Open improves the security of clients in open Wi-Fis such as hotspots in cafés or hotels.

DSL-Bridge-Mode

VDSL routers now operate optionally in DSL bridge mode. This allows a device to work purely as a DSL modem. Ideal for scenarios where multiple DSL connections are operated on one router.

OCSP responder – more power for Smart Certificate

Maximum security with VPN access: Smart Certificate is the easy way to create digital certificates with your LANCOM device—without any need for an external certificate authority. This feature has now been extended to include the OCSP (Online Certificate Status Protocol) network protocol, which enables clients to automatically and efficiently query the integrated CA for the status of X.509 certificates.

LISP (Locator / ID Separation Protocol) support

The Locator / ID Separation Protocol (LISP) is a new routing architecture. LISP allows the implementation of highly scalable networks with an integrated routing protocol, tunneling, and overlays. Ideal for service providers or enterprise networks.

Public Spot CSV import

Public Spot management is now even easier: Hotspot users are easily imported and exported by text file (CSV).

You can find further features within the individual builds sections in chapter 6 “History LCOS 10.20”.

6. History LCOS 10.20

LCOS improvements 10.20.0642 SU12

Bugfixes / improvements

General

→ A security vulnerability in the web interface has been fixed, which allowed unauthenticated attackers to cause an unexpected device restart (DoS attack) by sending a manipulated packet. This affected administrative access via WEBconfig from the LAN and the WAN (if management access via HTTP/ HTTPS from the WAN was enabled), as well as the web services IPSec-over-HTTPS, SCEP, OCSP server/responder, and the Public Spot. In the default configuration, access to the router from the WAN is disabled, meaning the router was not affected by this vulnerability in such cases. The TR-069 protocol was also not affected by the vulnerability.

LCOS improvements 10.20.0639 SU11

Bugfixes / improvements

General

→ Fix for ‘Aggregation & Fragmentation Attacks Against Wi-Fi’ (CVE-2020-24588, CVE-2020-26144,
CVE-2020-26146, and CVE-2020-26147)

→ If H.323 is enabled in the configuration (default setting), this will be disabled after an upgrade to LCOS 10.20 SU11. If the protocol is reactivated in the configuration, a message is generated in the syslog protocol.

LCOS improvements 10.20.0637 SU10

Bugfixes / improvements

General

→ A potentially security relevant cross-site scripting issue has been fixed that allowed JavaScript code to be executed from the LANCOM Public Spot login page. If such code was used, information could be infiltrated which could be used to attack a Public Spot user’s system via a manipulated link.

LCOS improvements 10.20.0485 SU9

Bugfixes / improvements

General

→ A potentially security-relevant issue has been fixed on LANCOM routers in conjunction with IPv6.
This issue can occur when IPv6 networks are connected via IPSec (IKEv1 or IKEv2), and an IPv6 Internet connection is used simultaneously.
In this case, an update to the current LCOS version is strictly recommended.
This issue has been fixed in the following LCOS versions:

- LCOS 10.32 SU3
- LCOS 10.20 SU9
- LCOS 10.12 SU14
- LCOS 9.24 SU12
- LCOS 9.00 SU8
- LCOS 8.84 SU11

LCOS improvements 10.20.0484 RU8

Bugfixes / improvements

VoIP

→ Concerning particular setups with analog phones, a VoIP issue has been solved which resulted in unidirectional voice communication or no connection establishment. The update is available for the following devices:
LANCOM 1783VA, 1783VAW, 1783VA-4G
LANCOM 1793VA, 1793VAW, 1793VA-4G
LANCOM 1906VA, 1906VA-4G
LANCOM 883 VoIP

LCOS improvements 10.20.0482 RU7

Bugfixes / improvements

General

→ The checksum calculation of Ethernet packets did not work accurately in the vRouter. This could lead to communication issues.

→ In a PMS server scenario the LANCOM devices ISG-1000, ISG-4000, and WLC-1000 tried to reach the IP address 0.0.0.0 instead of the PMS server address, because the network loopback address was not recognized correctly. As a result, no communication to the PMS server was possible.

→ If a LANCOM router obtained the IP parameters for the remote station INTERNET 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 considered itself responsible for the IP address xx.xx.xx.254, too. This resulted in no communication being possible to the Internet and to the LMC.

→ Invoking website URLs which were listed in the Content Filter whitelist took an unusually long time.

→ If configuration changes were performed directly on the device, and a communication loss occured while saving the modified configuration to the LMC, all changes were discarded.
Configuration changes are now cached and re-transmitted when the communication is possible again.

→ Due to a false SOAP header format in the LANCOM router the TR-069 negotiation was refused by the Auto Configuration Server (ACS). As a result, automatic configuration and firmware update by the ACS were impossible.

VPN

→ 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 client was connected to the LANCOM router via IKEv1 protocol, and the client received an IP address by the router via config mode, the address was not saved to the router’s RIB/FIB table.
If, additionally, under ‚IP-Router / General‘ the option „send packets from internal services via router“ was activated, this resulted in no communication being possible from the LANCOM router to the client. The communication from the VPN client to the local network, however, was not affected.

→ After a re-keying no communication via an IKEv1 VPN connection was possible, if the allocated values of the phase-1 and phase-2 lifetimes were identical.

→ A configured loopback interface for the LISP ETR was not rolled out.

Wi-Fi

→ After obtaining the Wi-Fi profile including the password the initial setup wizard is invoked when opening the access point's configuration in WEBconfig for the first time. If this wizard was cancelled by the user, any configuration changes on the accesspoint could be performed in WEBconfig without ever being asked for a configuration password.

→ Wi-Fi clients could not authenticate to an SSID if the encryption method "Enhanced Open" was selected, but Wi-Fi encryption was disabled.

VoIP

→ When using a Telekom DeutschlandLAN IP Voice/Data line with activated VoSIP, no incoming faxes could be received by an analog fax device. The reason for this was, that the LANCOM Router switched to T.38, and for this, sent a Re-INVITE. Due to faulty encryption settings in the router's re-INVITE, the VoIP provider refused the Re-INVITE with the message "403 Forbidden".

→ If an external call was answered by an ISDN phone box which forwarded this call to an external number, the call forwarding failed. The Voice Call Manager did not process the so-called REDIRECT correctly, so after processing, the line allocation was faulty.

→ 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 ermination.

→ A Voice over LTE (VoLTE) subscriber offers multiple codecs in its INVITE, as well as 8 and 16 kHz sampling rates for DTMF. On an incoming call of a VoLTE subscriber the LANCOM router answered with a faulty DTMF payload type in its ‚200 OK'. Also, the Voice Call Manager supported only a DTMF sampling rate of 8 kHz.
Due to this, no DTMF information could be transmitted. Partly, this resulted in no voice communication being possible.

- If, on an outgoing call, a LANCOM router received the parameter Require: 100rel in the ‘183 Session Progress’ from the provider, the router sent the parameter Supported: 100rel in the ‘183 Session Progress‘ to the internal SIP subscriber.
  Due to this, the caller did not hear any call sign, and after the call was answered, no voice data could be transferred. Furthermore, the call was disconnected after 10 seconds.
- If, during an active phone call, a LANCOM router sent the parameter Require: timer in the RE-INVITE, it could happen, that the remote station refused this with the message ‚420 Bad Extension‘ with the parameter Unsupported: timer, although the parameter Supported: timer was included in the initial INVITE of the remote station. As a result, phone calls were cancelled after 10 minutes.
  The parameter Require: timer is no longer transmitted in a RE-INVITE, because it is not necessary.
- In scenarios with an Octopus NetPhone phone system, faulty T.38 fax transmissions could occur, because the LANCOM Voice Call Manager answered an INVITE with an unauthorized NOTIFY in the CSeq header.
- If a SIP subscriberreceives an INVITE with a too small session timer, it confirms the INVITE with the message ‚422 Session Intervall Too Small‘. In a call goup scenario with multiple SIP subscribers the message ‚422 Session Intervall Too Small‘ was not sent to the caller. Due to that, the call could not be established.

LCOS improvements 10.20.0455 RU6

Bugfixes / improvements

General

- When a service (e.g. e-mail) was invoked by a local client via port forwarding (Hairpin-NAT), packet loss could occur on the Internet connection. As a result, the Internet connection was faulty for all further established sessions.

LCOS improvements 10.20.0446 RU5

Bugfixes / improvements

General

→ 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.

→ 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.

→ The SCEP client erroneously used the command "GetNextCACert" for the initial obtainment of a certificate instead of the command "GetCACert". This resulted in answering the request with an HTTP error "400 Bad Request" by the certification site.

→ After disconnecting the power supply of a LANCOM 1780EW-4G+ the transmission of NMEA- and GPS data via COM port server did not work.

→ 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".

→ At the first obtainment of a device certificate, the SCEP client saved the initially received CA certificate directly to the configured VPN container. This resulted in an incomplete VPN container which could not be used by VPN. The CA certificate is now saved to a temporary container. Only when all elements of the container are complete, the SCEP client writes the data to the configured container.

→ For TR-069 the SOAP header has been extended by the parameter "cwmp:IDsoapenv" to support further ACS systems.

→ After changing the bridge configuration or after link up/down events (network interface available / inavailable) the LAN interfaces lookup table (conversion table which contains statically defined connection information) was not updated. As a result, obtaining IP addresses via DHCP failed.

→ While changing router configurations with LANconfig and via LMC all sessions were disconnected for a short time. This was particularly noticeable during active remote maintenance sessions (e.g. Teamviewer or RDP).

→ The LANCOM vRouter was missing the function for determining and defining data- and time budgets.

- → With LANCOM routers of the 179x series and the LANCOM R883+ downstream data rates could drop or variate if the integrated modem was operated at a supervectoring connection and synced with ADSL2+.
- → 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.
- → When configuring an Internet connection using the WEBconfig setup wizard, a false value was written to the IPv6 column of the remote station table.

Wi-Fi

- → If on a dual radio access point with two 802.11ac modules a client switched from one module to the other one, it could sporadically happen, that the client did not receive a unique association ID from the access point and the client could not transmit any data.
- → The WLAN client mode on the 802.11ac module (WLAN-2) did not work on access points of the LN-1700 series.
- → 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.

VPN

- → 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 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.
- → 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 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.

VoIP

- 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.
- 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).
- 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 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 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.

LCOS improvements 10.20.0369 RU4

Bugfixes / improvements

General

- In rare cases, SSL/TLS handshake packets can become so big that they have to be split over multiple records. An SSL/TLS reassembler has now been implemented which reassembles these packets.
- On LANCOM devices with newer types of mobile radio modules (e.g. LANCOM 1783VA-4G) no cell connection speed was displayed in the LANCOM Management Cloud (LMC) due to a recently unsupported command sent from LCOS to the module.

Wi-Fi

- In a Public Spot scenario with activated re-login for Public Spot users a user was deleted from the Public Spot auto re-login table after expiration of the „WLAN-Idle timeout", which caused a failure of the automatic re-authentication at the Public Spot.
- In the console path "Status/WLAN/Client-Steering/Operating" the value "2" was displayed on an access point with activated client steering. Now the more descriptive term "Controller" is displayed.

VoIP

→ If a SIP client does not support both functions „Session Timer“ and „UPDATE“, the SIP provider uses Re-INVITEs to check if a call is still active (Session Refresh). These Re-INVITEs were not forwarded to the SIP client by the VoIP router. Due to that, the phone call was cancelled after some time.

→ In scenarios with a configured Telekom SIP trunk and a link line to a local Session Border Controller (SBC) on a LANCOM VoIP router the DTMF recognition for an established call only worked if the SBC and the SIP provider were using a common payload type.

→ If a SIP telephone system connected to a LANCOM VoIP router initiated an outgoing call using a too small SIP session timer within the INVITE, the SIP provider discarded the call with the message „422 Session Interval Too Small“. The following INVITE of the SIP telephone system using the correct value for the SIP session timer was not sent to the SIP provider by the router. As a result, the outgoing call was not possible.

LCOS improvements 10.20.0355 RU3

New features

→ The LCOS Auto Updater informs the user by e-mail about newly found, successfully completed, and failed updates. To use this feature, an e-mail address can be configured in the appropriate menu. If a device name is specified in the device configuration, the device name is included in the e-mail, too.

Bugfixes / improvements

General

→ If one or more weekdays were selected in the WEBconfig menu „Configuration / Date/Time / General / Timeframe“, the selected days were not saved when writing the configuration.

→ No LANCOM devices could be found using the LL2M broadcast command “ll2mdetect - b” from the CLI.

→ When using a LANCOM router as a certificate authority (CA), the „Subject Alternative Name“ (SAN) value was not saved while creating a certificate containing a particular field for the SAN in the certificate profile (menu: “Certificates / Certificate handling / Profiles“).

- → If one or more IP parameter profiles for managed access points were stored in a LANCOM WLC configuration, and these profiles contained a DNS entry, the specified DNS entry was not saved to the access point when rolling out the configuration. As a result, the access point could not connect to the WLC in all instances after a restart or the DNS resolution failed.
- → If the CLI command "set" was used with multiple arguments, which were separated from each other using at least one blank character, the blank character had to be completed with an Escape character "\". This led to a misrepresentation followed by the command not being able to be executed correctly.
- → LANCOM devices which were managed by the LANCOM Management Cloud (LMC) occasionally were in offline status for time periods of some minutes up to some hours. Because no communication to the LMC was possible in this time, these devices could not be configured within the LMC. Furthermore, no monitoring information was shown in the LMC for these devices.
- → A configured load balancer could cause a sudden device restart when simultaneously using the LANCOM Content Filter.
- → A sudden restart could happen on a LANCOM ISG-1000 if the Rapid Spanning Tree protocol (RSTP) for an interface (e.g. ETH-1) was active in the device configuration, and a link on this interface was established.
- → With activated IPv4 and IPv6, and when using a minimum of two loadbalancing remote stations, a disconnect from one of the remote stations could lead to a non-functional DNS forwarding.
- → Using QoS (Quality of Service) in a LISP tunnel did not work correctly in all cases. In failure cases the QoS settings were ignored by the LANCOM router.
- → Automated requests for the Layer-7 application detection statistics per SSH could lead to a sudden device restart.
- → SNMP requests in combination with VRRP could lead to a sudden device restart.
- → The DMZ in a router or access point is existing and active as a network in the default configuration under "IPv4 / General / IP networks". If a further network was created using the same interface as the DMZ the communication to a downstream router (next hop) was not possible anymore when the ARP cache has been cleared (e.g. by changing the configuration in LANconfig). The reason for that was that the DMZ was recognized as the receiver address.

VPN

- An IKEv1 connection to another gateway with activated SSL encapsulation was not established via port 443, but via port 500 (ISAKMP).
- A VPN connection establishment between a LANCOM router and a third-party router could fail, if the third-party router sent an IKEv2 notification packet which was not supported by the LANCOM router.

Wi-Fi

- In the WEBconfig menu “Manage Public Spot users“ user data of existing Public Spot users could not be printed again, because the application only showed a blank page in print preview.
- If, when executing the Public Spot setup wizard in WEBconfig, the access method “Individual tickets per guest“ was selected, the fields “Common user name“ and “Generic password“ had to be configured, although these are obsolete for the selected access method.
- In Wi-Fi scenarios with many access points and accordingly many connected Wi-Fi clients the IAPP table was refreshed very frequently which could cause sudden restarts on LANCOM access points.

VoIP

- Cancelling an outgoing call attempt via the provider swisscom did not result in cancelling the call at the called party (telephone still ringing), because the “CANCEL” command sent by the LANCOM router was not accepted by the provider. The “CANCEL” command has to contain the request URI of the “INVITE” command.
- Outgoing phone calls via a Vodafone Trunk Plus have always been discarded by the provider with the message “480 Temporarily Unavailable”. Vodafone expects the P-Preferred-Identity within the “INVITE” command, including the root number of the port. The value “PPI-woDDI” was added as an additional user-ID, so the P-Preferred-Identity is now sent without specifying the direct dialing number.

LCOS improvements 10.20.0298 RU2

Bugfixes / improvements

General

→ After expiration of a vRouter license the configuration of the vRouter could not be read out as configuration- (*.lcf) or script file (*.lcs).

→ If a backup case was invoked in a VRRP scenario by a restart of the VDSL modem in the master device, the connection was switched back to the master device after re-established WAN connection, but the master device's default route remained pointing to the VRRP IP address, so the master router was not able to forward IP packets to the WAN.

→ Sudden restarts could occur on the LANCOM ISG-1000, if there was an entry in the „Volume Budgets" table.

→ It could happen occasionally that the LCOS LMC client reported wrong values to the LMC if "apply local device configuration changes" was selected in the default settings of an LMC project. This led to a "configuration not accepted" message in the LMC, and the device log displayed the message "When setting the device configuration 1 error occured:…".

→ The maximum length of the RADIUS authentication login name was limited to 16 characters. This value has been extended to 48 characters.

→ In certificate-based scenarios (VPN and WLC) which used the internal SCEP client of the LANCOM router for certificate distribution, the SCEP client did not renew expiring RA certificates automatically. As a result, e.g., certificate-based VPN connections could no longer be established, and WLC-managed access points could no longer establish a connection to the WLC. Further information on this behavior is available in the LANCOM Support Knowledge Base.

  Due to a validity check error the device certificate could not be renewed when using the RA Auto Approve function.
  As a result, certificates could not be received in WLC- and VPN scenarios.
  Further information on this behavior is available in the LANCOM Support Knowledge Base.

  On certificate requests via SCEP client to external certificate authorities (e.g. Windows CA), it could happen, that certificates could not be accepted due to a wrong "mime type". The certificate is now checked directly without considering the "mime type".

VPN

- → Configured IKEv1 client connections which used NAT Traversal (UDP Encapsulation, Port 4.500) could not be established because the LANCOM router did not replay correctly to the connection request of the VPN client.
- → When using the WEBconfig setup wizard for configuring a dial-in access (RAS, VPN), the wizard denied to configure connections without selecting a PFS group.
- → When using certificate-based connections with flexible identity comparison the VPN connection could not be established. The error message “IKE-R-ID-type-mismatch” was displayed on the responder.
- → When executing a “show” command, a sudden restart could sporadically happen if the access to the requested table was not released in time. The output of all “show” commands is now initially written to a buffer memory.
- → Sudden restarts could occur when using VPN connections via IKEv1.

Wi-Fi

- → On dual radio access points a spectral scan could not be performed on the second radio module.

VoIP

- → An incoming call for an internal ISDN subscriber with activated call forwarding led to an error in case of activated call forwarding with SIP302. The call could not be established.
- → If SIP over TLS (SIPS), and SIPS as URI type was used by a provider or SIP client on an incoming call, the call could not be established via the LANCOM router.
- → When receiving a fax via T.38 it could happen that the confirmation (ACK) which was sent by the LANCOM router contained multiple route headers which were listed in the wrong sequence. This led to a termination of the fax call.
- → If an instant call forwarding to Voice over LTE (VoLTE) was configured in the Telekom customer center, a call could not be established because the LANCOM router answered the VoIP provider in the wrong network context. The device received a new “to” tag due to the configured call forwarding at the provider which, however, was not saved to the device. As a result, the call could not be established.
- → If a SIP trunk subscriber called an analog user at another SIP trunk (LANCOM router), and the called subscriber had configured an active call forwarding to a mobile phone subscriber (VoLTE), the caller received an indication about call signalling. The mobile phone subscriber, however, only received a message about a missed call.

LCOS improvements 10.20.0259 RU1

New Features

→ The new command “ssldefaults” can be executed from the CLI. After answering a confirmation promt, the
SSL/TLS settings in all submenus of the current configuration are reset to default values.
→ The timeout for UDP connections in the firewall was increased to 120 seconds.
→ The rollout wizard can now be used for linking devices to the LANCOM Management Cloud.
→ Support for “Call Deflection” by the SIP feature SIP302.

Bugfixes / improvements

General

→ If a DNS update with configured routing tag had to be performed in the action table, the routing tag was not considered. This resulted in sending the HTTP command for the DNS update over the wrong default route.
→ If Internet access was configured in WEBconfig using the IPP (Internet Protect Pro) wizard on LANCOM R88x devices, the wizard did not create the required DNS forwarding entries for “TELEKOM”.
→ Error counters of the VDSL modems 1 and 2 were written to the same log table on 1906-series devices. As a result, it was not recognizable how many errors were counted on which modem.
→ If the SCEP was working on a task and, in the meanwhile, was switched off, this did not lead to stopping the service.
→ The Layer-7 application detection could not be configured on LANCOM ISG devices.
→ If an LMC-managed device obtained a new certificate from the LMC, the used TCP session was not stopped.
Furtheron the device used an invalid certificate and lost the connection to the LMC.
→ When operating a router or access point as a LAN DHCP client, the device lost its connectivity after switching the network (for example, when connecting to another router with a different IP network). This was caused by the fact that the device’s DHCP client was not restarted and thus the old IP address was still in use. The IP address was only reassigned after expiration of the DHCP lease.

→ The integrated LCOS SSH client sent packets with set “Don’t Fragment” flag, which were bigger than the smallest known MSS.

→ If a LAN computer was operated with a different MTU (MTU 1500) than the WAN router (MTU 1492 due to PPPoE) and an attempt was made to access the computer with map port via port forwarding, the computer did not acknowledge this maximum size packet with the message “Destination unreachable (Fragmentation needed but DF bit set)” if the “Don’t Fragment-Flag” was set at the same time.

→ After losing the xDSL sync it could happen that the Internet connection could not be re-established after re-syncing, because no PADI packets were sent to the provider.

→ When using IKE Config Mode the allocated IP parameters were not forwarded to the VPN service. Due to that, the router could no longer send DNS requests through the VPN tunnel.

→ The function “generate TCP/HTTP tunnel” did not work if a device should be addressed through a VPN tunnel via it’s own IP address, but no LAN link was valid for this IP address.

→ In a BGP scenario, it could happen that after a router restart no BGP connections could be established.

→ TFTP commands could only be transferred to a LANCOM device when being authenticated with root administrator authentication data.

→ If a LANCOM device received an LMC configuration while an Internet backup connection was used actively, the LMC could not be accessed after the configuration was received completely.

→ When using an ISDN LAN-LAN connection the first packet which should be transmitted via this connection was discarded if the connection was not yet established.

→ A “public_html” folder on a USB stick with LCOS firmware files which should be used for a firmware update was not recognized on the LANCOM devices ISG-1000, ISG-4000, and WLC-1000. As a result, a firmware update via USB was not possible.

VPN

→ An SSH/HTTP/Telnet access to LANCOM routers was not possible when using a VPN tunnel in combination with N:N NAT.

Wi-Fi

→ The five memory slots for uploading voucher pictures were absent.

→ When creating a Public Spot user via WEBconfig wizard, the value "Never" was used for user account expiration, regardless of the configured expiration mode.

→ If a logical network profile (SSID) with encryption method "Enhanced Open Transitional" was configured on a WLC, no configured network profiles were shown in LANmonitor.

→ If the indoor mode was activated on a LANCOM access point, and no fixed channel was configured on the device, solely 20 MHz channel widths were used.

→ If a firmware update to version 10.20 Rel was executed on WLC-managed access points with an 802.11ac Wi-Fi module (e.g. L-822acn), and the WLAN controller was operating an older LCOS version, no radio could be emitted by the 802.11ac Wi-Fi module.

→ If the MAC address of a Wi-Fi client was known to an access point / Wi-Fi router in the table "Wireless-LAN / Stations/LEPS / Station rules (access point or WLC)", this client could not connect to the wireless LAN. The message "Possibly wrong passphrase in key handshake with peer aa:bb:cc:dd:ee:ff" was displayed.

→ If a LEPS-U profile was created but no corresponding LEPS-U users, multiple sudden restarts did occur. The device the fell back to the firmware in the second slot.

→ It could happen that certificate backups which were created by the function "One Click Backup" could not be restored to a different device. A "file too big" message was displayed. Now files with sizes up to 1 MBytes can be uploaded.

→ Some Wi-Fi clients could not establish a connection, if the LANCOM router or access point additionally worked as a DHCP server. The DHCP server transmitted a VLAN priority tag within the DHCP-ACK which could not be handled by the Wi-Fi client. As a result, the Wi-Fi client could not obtain an IP address.

VoIP

→ A sudden router restart could occur on in- or outgoing calls if the Voice Call Manager could not create a UDP transport.

→ It could happen with some subordinate telephpone systems that outgoing calls could no longer be performed, because the "User Binding" within the Voice Call Manager could not be created by the LANCOM router.

- If the router receives a duplicate “BYE” from the provider, a timer is started on the ISDN bus which sends a DISCONNECT to the plugged ISDN phone (no user responding). Since the Voice Call Manager did not receive this information, no speech data could be transferred from the ISDN phone via SIP line.
- If a LANCOM VoIP router with a connected off-hooked phone at the analog port was restarted, the phone was not recognized as “busy”.
- If a local ISDN user used the ISDN Clearmode, after a faulty connection establishment (e.g. wrong phone number or destination not reachable) the message “normal call clearing” was displayed in the call manager trace in addition to the correct error message. The wrong message was also transferred to the Status/Voice-Call-Manager/ Calls/ table.
- When using T.38 in a scenario with a subordinate SIP telephone system it could happen that packets from incoming faxes were discarded. This resulted in cancelling the fax call at the sender side.
- With set call prefix on the SIP line, the prefix in the FROM field was set on incoming calls, but not in the P-Asserted-Identity. This resulted in callbacks partly not being possible. The prefix is now set in the P-Asserted-Identity, too.
- Using the SIP provider 1&1 unidirectional communication could occur, so that only the called party was hearable. The second audio stream was discarded because it was sent from a different source RTP address. The reason for this was the default activation of the Symmetric RTP function in the configuration of the LANCOM router which expected both RTP addresses (source and target address) to be identical. In the RFC it is not mandatory that both addresses have to be identical, so the Symmetric RTP function has been removed.
- In certain scenarios recognition of DTMF signaling on calls from the own IP-based connection to another one or to a cellular network was not possible.

LCOS improvements 10.20.0175 Rel

New features

→ as from LCOS 10.20 the Voice Call Manager (VCM) is activated by default for the following devices:

- LANCOM 1900EF
- LANCOM ISG-1000
- LANCOM ISG-4000

→ For the following devices the VCM can be activated using the All-IP Option:

- LANCOM 1640E
- LANCOM 1780EW-4G+
- LANCOM 1790-4G
- LANCOM 7100+ VPN
- LANCOM 9100+ VPN

Bugfixes / improvements

General

→ The routing method “Obey DiffServ field” did not work correctly due to packets marked with AFxx were not only allocated to the send queue “SAFE”, but also to the send queue “URGENT”. This resulted in QoS rules having no effect, because not only packets which had to be handled as preferred, but also subordinate packets were forwarded via URGENT queue.

→ With activated SNMP SNMPv1/2 as well as SNMPv3 was shown with active status in the service table under Status/Config/Services/, even if one of both protocols was not activated. The status is now shown separately for each protocol.

→ Due to a polling failure mobile connections with activated ICMP polling were disconnected right after connection establishment.

→ The mobile radio module MC7710 of the LANCOM 1781VA-4G stated faulty network name values for some providers, so that these values were shown in LCOS and LANmonitor. In such cases, now the numeric identifier of the provider network is shown.

VPN

→ When using IKEv2 with activated PFS it could happen that after a re-keying or immediately after connection establishment ESP tunnels could no longer be used for data communication, if the LANCOM router established a connection to a third-party provider.

Wi-Fi

→ If a LANCOM device which is compatible to the LANCOM Public Spot XL Option was paired to the LANCOM Management Cloud, the Public Spot XL Option did not activate itself automatically on the device.

VoIP

→ If a SIP domain which referenced to another alias name instead of the IP address (CNAME) was specified as SIP registrar, the SIP registration was not possible.

LCOS improvements 10.20.0145 RC2

New features

→ LANCOM Auto Updater for automatic firmware updates
→ Support for WPA3
→ Enhanced Open for improved client security in open Wi-Fis
→ Redistribution of RIP routes in BGPBugfixes / improvements

Bugfixes / improvements

General

→ Obtaining DHCP addresses via WLC- or EoGRE tunnel could fail due to IP packet related processing problems. Rarely, this could lead to a sudden router restart, too.
→ Due to a faulty channel allocation on Wi-Fi routers an IPoE connection which was configured on a DSL interface (e.g. DSL-1) was allocated to an ISDN interface.
→ When using a backup connection via backup table, switching from the main to the backup connection caused TCP sessions to not being taken over to the backup connection or not being terminated accurately. Additionally, DNS requests were not using the established backup connection.
→ If the access to the management protocol “TFTP” was forbidden from WAN side, the router answered a port scan with a “TFTP error (Access violation)”. The following “TFTP ack” of the port scanner was answered with the message “Destination unreachable (Port unreachable)”. Now a port scan is immediately answered by the router with a “Port unreachable”message.

→ When executing a file system operation in the Layer 7 application detection (enabling an internal resource), a sudden LANCOM router restart could occur.
→ Due to a missing initialization during a LANCOM router start, all interfaces which were set disabled on startup were shown as active on an SNMP request.
→ If only one DSL remote station was configured and active, MLPPP packets did not contain a multilink header, which led to these packets always being sent on the first channel (master channel).
→ When using a LANCOM router as a VDSL modem the bridge stopped working after a short time. This caused a non-working Internet connection.
→ After disconnecting the ADSL connection (e.g. forced provider disconnect) the Internet connection was not re-established in some cases. This behavior occurred, if a VDSL remote site (with VDSL as layer 1) was used on an ADSL line.
→ When using a Plain Ethernet connection (IPoE or DHCPoE), ICMP polling failed if the sender address specified a network with an allocated, but unplugged Ethernet port. Due to this, the Plain Ethernet connection could not be established.

Routers & VPN

→ The speed of establishing VPN tunnels on central site VPN gateways has been improved in big scenarios.
→ The VPN status trace output used an IKEv2 technology term while negotiating a phase 2 SA of an IKEv1 connection.
→ Simultaneously disconnecting and connecting an IKEv2 connection with simplified dial-in could cause a sudden LANCOM router restart.

Wi-Fi

→ If the amount of “Max-Login-Tries” was set to “0” in the path “Setup / Public-Spot-Module / Brute-Force-Protection”, and thus the brute force detection function was disabled, the function was still active and a Public Spot user could not log on to the system.
→ When using an access point with two 802.11ac Wi-Fi modules (IAP-822, OAP-822 and OAP-830), switching between the two modules by a Wi-Fi client caused a sudden router restart because a wrong interface pointer was allocated, if the Wi-Fi client did not log off or had not been logged off.

VoIP

→ After a router restart it could occasionally happen that incoming calls were not signaled on an IPv6 SIP provider line. The telephony worked only after disabling and re-enabling the Voice Call Manager.

→ In scenarios with routing tags for all IP networks and routing entries it could occur in certain constellations that telephony via Voice Call Manager led to a unidirectional communication. An option was implemented now to configure one loopback address (sender address) per SIP line. Using these lines, the outgoing path can now be explicitly defined.

→ The Voice Call Manager did not check the server name stored in the SIP domain/realm when using TLS authentication. This led to SIP registrations executed even if the server name in the SIP domain/realm did not match the certificate’s server name.

LCOS improvements 10.20.0097 RC1

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.

7. General advice

Disclaimer

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

Backing up the current configuration

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

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

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

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

Using converter firmwares to free up memory

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

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

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

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

LANCOM
SYSTEMS

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de | lancom-systems.com