LANCOM Release Notes
LCOS 10.20 RU1

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

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

21.11.2018, 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 RU1, as well as the improvements since the previous version.

Before upgrading the firmware, please pay close attention to chapter 6 „General advice“ of this document.

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

2. Device-specific compatibility to LCOS 10.20

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/lcos/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

3. Advices regarding LCOS 10.20

3.1 Information on default settings

Devices delivered with LCOS 10.00 or higher automatically connect to the LANCOM Management Cloud (LMC). This functionality provides zero-touch installation for new devices. In case you do not want to use the LMC, this feature can be disabled while running the default setup wizard for the initial configuration, or at any time from within LANconfig under Management > LMC. You can manually re-enable the usage of the LMC whenever you want.

3.2 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.

4. Feature overview LCOS 10.20

4.1 Feature highlights

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.

4.2 Further features

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.

Even more flexibility for the LANCOM vRouter

The LANCOM vRouter now supports the Micorosoft Hyper-V virtualization platform. Furthermore: Managing the vRouters is now even easier, because firmware updates are easy to import as a UPX file.

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 5 “History LCOS 10.20”.

5. History LCOS 10.20

LCOS improvements 10.20.0175 Rel > 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 10.20.0145 RC2 > 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 10.20.0097 RC1 > 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.

6. General advice

Disclaimer

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

Backing up the current configuration

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

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

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

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

Using converter firmwares

To 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.