LANCOM Release Notes

LCOS

10.42

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

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

April 21st, 2021, CBuersch

Table of Contents

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 10.42.0284, as well as the improvements since the previous version.

Before upgrading the firmware, please pay close attention to chapter 3 “Advices regarding LCOS 10.42” 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 10.42

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/

With LCOS 10.40, support for the following devices is no longer available

- LANCOM 1780EW-4G
- LANCOM 1781A-4G
- LANCOM L-322E
- LANCOM L-1302acn
- LANCOM L-1310acn

3. Advices regarding LCOS 10.42

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.

4. Feature overview LCOS 10.42

4.1 Feature highlight 10.42

Dynamic Path Selection

With the new highlight feature Dynamic Path Selection, you can route mission-critical business applications in your SD-WAN always over the best quality line. The feature continuously monitors your WAN connections in terms of load, packet loss, latency, or jitter and dynamically decides the best route for specific applications depending on the current connection quality. You can flexibly define the performance policies for the WAN connection according to your application. Thus, you benefit from maximum performance and reliability in large-scale SD-WAN infrastructures with several WAN connections in active/active mode.

Next-generation SD-WAN: LANCOM High Scalability VPN (HSVPN)

High scalability VPN significantly improves the extensibility and efficiency of your SD-WAN architecture. Previously each individual application needed its own individual VPN tunnel, but HSVPN now transports any number of networks on a single VPN tunnel to the remote site. Networks remains secure and strictly separated from one another. The advantage for your business: Significantly fewer VPN tunnels are required and faster recovery times in case of failover.

Modern look & feel: New WEBconfig

You can look forward to the completely new look and feel of LANCOM WEBconfig. Based on the modern and bright design of the LANCOM Management Cloud, WEBconfig has been completely redesigned to offer you an attractive and fresh appearance.

Multicast routing

Multicast data such as IPTV is now transmitted efficiently to multiple devices. Previously, separate data packets had to be sent to each recipient, whereas multicast routing now allows an IP stream to be transmitted to multiple recipients. This reduces the load on the router and makes better use of available routing capacity.

4.2 Further features 10.42

Dynamic DNS Service for the Public Cloud

The LANCOM Management Cloud (Public) becomes a DynDNS provider! Simply assign a fixed, self-selected subdomain (mycompany.dyndns-lmc.de) to the gateways implemented there in the sites settings. This subdomain can then be stored in VPN remote stations such as the LANCOM Advanced VPN Client. Even gateways with dynamic WAN IP addresses remain accessible at all times via this domain name.

Cloud-managed Hotspot

Create a simple Wi-Fi hotspot with a few clicks – directly from the LMC. No additional gateway or WLAN controller with LANCOM Public Spot Option is required. Intuitive menus provide you with the opportunity to customize your hotspot welcome screen with your logo and corporate colors and integrate important information such as imprint and usage guidelines for your hotspot users. Afterwards you can assign the new hotspot to the respective location and it will be available to your visitors.

BLE API for the realization of innovative location-based services

Whether for the indoor localization of patients in hospitals, the evaluation of customer traffic in retail, or asset tracking in the logistics sector: A new API interface (REST) for the integration of location-based services is now available for all LANCOM access points with Bluetooth Low Energy module (BLE). In cooperation with third-party providers, this enables the implementation of a wide range of location-based services (LBS) and innovative IoT applications.

SD-WAN zero-touch deployment for DSL routers

Automatic installation of DSL routers at BNG Telekom connections with the LANCOM Management Cloud—without the laborious configuration of DSL access data on the router.

Netflow

With Netflow, network analysis information about the router's incoming and outgoing IP traffic (source, destination, ports, etc.) can be sent to a central server for processing.

IKEv2 VPN with Windows login

Mobile VPN clients using IKEv2 EAP can now authenticate against a central database such as Microsoft Active Directory or RADIUS without having to store VPN credentials on the LANCOM router.

More flexibility with backup scenarios

Route prioritization offers new levels of flexibility for backup scenarios.

New SD-WAN functions for the load balancer

On central-site gateways, VPN load balancers can be generated automatically with the help of RADIUS. Furthermore, multiple VPN channels are aggregated into tunnel groups, so that even in the case of failover, the VPN connects to a common gateway.

WLAN scheduling

Enables time-based activation and deactivation of SSIDs in the wireless LAN. Ideal for WLAN networks that should only be available at specific times, such as hotspots or Wi-Fi in educational institutions.

More security in the VPN

Support for new and modern encryption algorithms such as Chacha20-Poly 1305, digital signature with ECDSA, and new Diffie-Hellmann groups.

TLS 1.3 client mode

Support for the new TLS 1.3 protocol improves security for router accessing web services.

New filters for individual notifications

Configurable filter lists for SNMP traps and SYSLOG enable individualized monitoring notifications to be received.

You can find further features within the individual builds sections in chapter 5 “History LCOS 10.42”.

5. History LCOS 10.42

LCOS improvements 10.34.0283 -> 10.42.0284

Bug fixes / improvements

General

- If H.323 is enabled in the configuration (default setting), this is disabled after an upgrade to LCOS 10.42 RU3. If the protocol is enabled again in the configuration, a syslog message is generated.

LCOS improvements 10.34.0168 -> 10.42.0283

New features

General

- The 802.1X authenticator for Ethernet ports is now included in all devices.
- The 802.1X authenticator can now optionally perform an immediate check of the MAC address of the connected Ethernet device with a RADIUS server instead of 802.1X negotiation.
- In new configurations, the MAC address of bundle interfaces is now '0' and is converted to the system-wide, device-specific MAC address during operation. This facilitates the porting of configurations.
- The HTTP(S) hit list of the Layer 7 application detection has been updated.
- The ThinAP2.0/TLS protocol can now be used to connect to a Wireless ePaper server.
- In new configurations, the Telnet and Telnet-over-SSL management protocols are now disabled by default.
- MLD snooping support
- In the SLA Monitor, DSCP tags can now be set, too.
- The cache time for using DNS objects in the firewall is now configurable.
- The main device password and the passwords of other administrators can be stored using the SHA-256 and SHA-512 hash methods.
- CRL checking is now switchable per IKEv2 peer.
- New design for WEBconfig
- Syslog messages during firmware change as well as firmware info at boot time
- For IPv6 WAN access, the DHCPv6 client is now also started if no router advertisements were previously received.
- For zero-touch commissioning on Deutsche Telekom BNG connections, a corresponding Internet remote station has been included in the standard configuration of DSL routers.
- In the default configuration, a main device password must now be assigned at the first console login.
- Support for WAN connections that are assigned only one DHCPv4 address with /32 mask on the provider side
- When 80% of a configured volume budget is reached, information is now sent by e-mail and/or syslog.
- WAN bandwidths > 1 Gbps can now be configured for QoS.
- Support for TLS 1.3 client mode
- SNMP traps to be sent can now be filtered.
- Syslog messages to be sent can now be filtered.
- A send address is now configurable for the alive test.
- The RADIUS dictionary can now be extended by user-defined attributes.

Routing & VPN

- IPv6 source address filter for IKEv2 VPN connections
- The line code of the xDSL modem of the LANCOM 179x series has been updated.
- Support for SD-WAN Dynamic Path Selection
- Support for multicast routing
- Support for IGMP and MLD proxy
- Support for PIM (Protocol Independent Multicast)
- Remote stations can now be established without an existing route in the routing table, if required.
- The DHCP client now supports option 121 (Classless Static Route) according to RFC 3442.
- The BGP connection retry timer is now configurable.
- The behavior when propagating the default route in BGP can now be configured.
- BGP now stores a history of sent prefixes.
- The IPv4 firewall now does not support MAC addresses as targets. Existing configurations continue to work.
- The time-controlled default route has been omitted.
- Administrative distance can now be configured for static IPv4 and IPv6 routes.
- Support for NetFlow/IPFIX
- The administrative distance at OSPF is now configurable.
- A prefix filter list can be configured for route redistribution via LISP and OSPF.
- The ‘DMZ’ line has been removed from some tables as a default.
- The TFTP operating switch now also handles the ‘Sysinfo only’ mode.
- The scalability of the IPv4 router has been significantly improved for many routes.
- If the provider transmits the actual Layer 3 bandwidth as additional information in the PPP, this is used in QoS.
- Support for LANCOM High Scalability VPN (HSVPN)
- Support for IKEv2 EAP
- ChaCha20 poly1305 support for IKEv2
- Support for EdDSA for IKEv2
- Support for Digital Signature with ECDSA according to RFC 7427
- Support for Curve25519 and Curve448 for IKEv2
- A VPN load balancer can be dynamically generated by RADIUS.
- Requesting an address in IKEv2 config mode is now switchable.
- Alternative gateways can now be grouped and prioritized.
- Omission of IPCOMP for IKEv1
- Omission of AH for IPsec

Wi-Fi

- Support for Stanley-AeroScout RTLS tags
- If the result of the channel assessment of the automatic Wi-Fi channel selection consists of several equally good channels, one channel is selected from them based on the system-wide MAC address. This improves scenarios in which several neighboring access points perform automatic channel selection at the same time.
- Support of a JSON API for BLE and Wi-Fi location data offloading
- The default Wi-Fi passphrase is now empty. To enable an encrypted Wi-Fi SSID, it is necessary to set a custom passphrase.
- Support for PassPoint R2 configuration via WLC
- Omission of the default Wi-Fi passphrase
- A LANCOM WLC now configures the first Wi-Fi module (2.4 GHz) of a managed access point for 20 MHz channel width by default. This only affects access points newly added to the management.
- Support for OCSP in the RADIUS server in connection with EAP(-TLS)
- Wi-Fi SSIDs can be turned on and off based on schedules.
- For Public Spot, a custom branding logo (“powered by LANCOM”) can now be used on the login page.
- HTTPS is now always used for the Public Spot login page when HTTPS is selected as the login page protocol. Previously, only the actual login data and the status page were transferred via HTTPS.
- For Wi-Fi clients, a threshold value can be defined, below which a client is disassociated.
- VLAN group keys are now assigned automatically.

VoIP

- For SIP lines, the transfer of a fixed PPI or PAI can be configured.
- A loopback address can now be configured for SIP PBX lines.
- The Voice Call Manager table ‘User Settings’ can now contain any number of entries.
- Passwords for SIP lines may now be up to 64 characters long.
- Support for ‘Telekom Company Flex’ access.
- The format of the ‘Connected Number’ is configurable.
- Support for Early Media
- Calls can be dynamically distributed to different SIP lines.
- The maximum number of parallel calls for a SIP line is configurable.

WLC

- ‘Unknown seen clients’ are no longer reported to the WLC in the default configuration.
- The client bandwidth limit is now configurable via the WLC.

Bug fixes / improvements

General

- The cellular modem did not send regular router advertisements (RA) during IPv6 operation. This meant that after the router lifetime of 65,535 seconds (approx. 18 hours) had elapsed, the router no longer had a gateway and IPv6 communication was therefore no longer possible.
  Shortly before the RA Lifetime expires, a Router Solicitation (RS) is now sent for the purpose of updating the Router Lifetime.
- On Internet connections of 'Deutsche Glasfaser', the router advertisement is sent to the multicast IPv6 group and the unicast MAC address of the router. This caused the router to discard the router advertisement and thus Internet communication was not possible.
  The router accepts the Router Advertisements now.
- The configuration reference via TR-069 when using an IPv6 address failed because the router's own IPv6 address was enclosed in square brackets by the TR-069 process and therefore not recognized correctly.
  In this case, a fallback via IPv4 was performed.
- Communication with an external syslog server via a user-defined port (not equal to 514) was not possible regardless of the protocol used (TCP or UDP). The router ignored the setting and continued to use port 514.

VoIP

- If a SIP PBX sent the characteristic for SDP in lower case (rtp/avp) to the router in the message "200 OK", the router did not recognize the SDP and sent the "200 OK" without SDP to the provider. The provider responded with a BYE and the error message "488 Not Acceptable Here".
  This led to the fact that in such a case the telephone call did not take place.
- Fixed problems with transferring phone calls with methods RE-INVITE, REFER and related voice codec handling in scenarios with Swyx PBXs.
- In an incoming SIP call, the calling party (in this case the provider) represents the UAC (User Agent Client) and the accepting party (in this case the LANCOM router) represents the UAS (User Agent Server). If there is a change in the negotiation (such as an UPDATE or a RE-INVITE), the direction changes. The provider thus becomes the UAS and the LANCOM router the UAC.
  In the 'Session-Expires' header, the calling party tells how long the negotiated session may initially last and whether the UAC or the UAS will update the session (the 'Refresher'). The 'Refresher' usually remains the same (e.g. the provider), so the role changes from UAC to UAS and must be adjusted accordingly in an UPDATE or RE-INVITE.
  If there was a change in the codecs during an incoming call with a 'Session-Expires' header containing the 'Refresher' UAC, the LANCOM router sent a RE-INVITE with the 'Refresher' UAC contained in the initial 'Session-Expires' header instead of UAS to the provider. The LANCOM router should therefore have sent the 'Refresh Request' to the provider, but this is not intended. Thus, there was no session refresh anymore. This resulted in the call being terminated after the 'Session Expires' timer had expired (e.g. after 30 minutes).
- An outgoing call with suppressed phone number initiated by a SIP user could not be established because the call could not be assigned to a user.

- It could happen that an ISDN telephone displayed the destination number (Connected Number) in an unwanted format. It is now possible to suppress the connected number so that it is not sent in the ISDN 'Connect Message'.
- If the Voice Call Manager received a REFER for call forwarding from a SIP PBX to a SIP client and received a 'Session Progress' with SDP data from the SIP PBX after sending an INVITE to the SIP client, the Voice Call Manager first sent a Re-INVITE to the SIP client and then, after receiving the message "200 OK" from the SIP client, erroneously sent an ACK to the SIP PBX, although the call negotiation was still open (such behavior will mainly occur in a scenario with a Swyx PBX in combination with a CTI+ client). This led to a call termination.

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 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.