

Information regarding

LCOS Software Release 9.24 RU4

Copyright (c) 2002-2017 LANCOM Systems GmbH, Wuerselen (Germany)

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

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

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

07.03.2017, CBuersch

Table of Contents

1. Preface	2
Warning hint – Backing up the current configuration	2
Advice	2
Upgrading central site components	2
Using converter firmwares	2
Dynamic VPN registration	3
Device specific support of the current LCOS version	3
2. Known Issues	4
3. New Features, Improvements and History	5
LCOS improvements 9.24.0153 RU3 ► 9.24.0212 RU4	5
LCOS improvements 9.24.0076 RU2 ► 9.24.0153 RU3	7
LCOS improvements 9.24.0075 RU1 ► 9.24.0076 RU2	8
LCOS improvements 9.24.0070 Rel ► 9.24.0075 RU1	8
LCOS improvements 9.20.0683 RU2 ► 9.24.0070 Rel	8
LCOS improvements 9.20.0647 RU1 ► 9.20.0683 RU2	9
LCOS improvements 9.20.0566 Rel ► 9.20.0647 RU1	10
LCOS improvements 9.20.0517 RC2 ► 9.20.0566 Rel	11
LCOS improvements 9.20.0385 RC1 ► 9.20.0517 RC2	11
LCOS improvements 9.10.0530 RU5 ► 9.20.0385 RC1	12
Comments	14

1. Preface

LCOS („LANCOM Operating System“) is the operating system for all LANCOM routers, wireless LAN access points and wireless 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 9.24 RU4, as well as the improvements since release 9.10.

Warning hint – Backing up the current configuration

Before upgrading your device to a new LCOS version it is essential to backup the configuration of your router. Due to extensive features it is not possible to downgrade to a previous firmware without using the backup configuration.

Please see the reference manual for instructions on how to backup the router 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.

Advice

LANCOM 178x 4G: To avoid delayed connection establishments within mobile radio (eg in case of backup) it is recommended to use the latest firmware version 3.5.24 for the LTE mobile modem (Sierra MC-7710). Please refer also to the following Knowledgebase article: [Link](#)

Upgrading central site components

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

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 firmsave function of the LANCOM device is available only on a limited scale. The update to a newer firmware is furthermore possible. However, in case of an update failure the LANCOM will only work with a minimal-firmware which allows just local access to the device. Any extended functionality, in particular remote administration, is not possible when running the minimal-firmware.

Dynamic VPN registration

By reason of patent you have to register the functionality „Dynamic VPN“ with IP address transmission over ISDN. This operating mode is usually required when you configure a VPN tunnel with dynamic IP addresses on both sides without dynamic DNS services.

Any other Dynamic VPN operation mode (e.g. transmitting the IP address via ICMP, provoking a callback etc.) does not require registration.

The registration process is fully anonymous - no personal or company data will be transmitted.

The registration of the Dynamic VPN option requires administrator rights on the LANCOM device.

Device specific support of the current LCOS version

As from LCOS 8.84 support for the following devices is discontinued:

- > Telekom R800+
- > LANCOM 821+
- > LANCOM 1611+
- > LANCOM 1711
- > LANCOM 1821n

As from LCOS 9.00 support for the following devices is discontinued:

- > Telekom R1011
- > LANCOM 1823 VoIP
- > LANCOM L-54 Wireless
- > LANCOM 1751 UMTS
- > LANCOM 8011
- > LANCOM 7111
- > LANCOM C-54ag

As from LCOS 9.04 support for the following devices is discontinued:

- > LANCOM 1711+ VPN
- > LANCOM 1721+ VPN
- > LANCOM 1722 VoIP
- > LANCOM 1723 VoIP
- > LANCOM 1724 VoIP
- > LANCOM 1811n Wireless
- > LANCOM 1821+ Wireless ADSL
- > LANCOM 3850 UMTS
- > LANCOM 800+
- > LANCOM DSL/I-10+
- > LANCOM L-315agn dual Wireless
- > LANCOM OAC-54-1 Wireless
- > LANCOM OAP-310agn Wireless
- > LANCOM OAP-54 Wireless
- > LANCOM WLC-4006
- > LANCOM WLC-4025
- > LANCOM XAC-40-1
- > Swyx 1722 VoIP
- > Swyx 1723 VoIP
- > Swyx 1724 VoIP

Note: Even if devices do not support the latest LCOS version, they will still be maintained with LCOS Release Updates including bugfixes and general improvements on a regular basis.

The latest LCOS version overview can be found on our website under
<https://www.lancom-systems.com/products/lcos/version-overview/> .

2. Known Issues

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/>

3. New Features, Improvements and History

LCOS improvements 9.24.0153 RU3 ► 9.24.0212 RU4

Bugfixes / Improvements:

General

- > Local IPv6 networks can communicate with each other again, if one of these networks is allocated to a bridge group (e.g. BRG-1), and the other network to a logical network (e.g. LAN-2).
- > An unconfigured device in factory state can be reached within the local network by specifying an arbitrary DNS name
- > If the device time is set (manually or by NTP server), milliseconds are reset, too
- > An IPv6 address is generated on the WAN interface when connecting to internet providers SWN or Wilhelm-tel, too
- > A standby device within a VRRP cluster which is addressed by a client as NTP server does not establish an internet connection if the NTP server service is enabled
- > On a router with WAN-RIP-configured remote sites (e.g. L2TP or PPTP), an arbitrary configuration change leads no longer to a disconnect of remote sites without active RIP routes
- > Data traffic limitation by firewall rules with trigger "per station" works again, if a logical LAN interface (e.g. LAN-1) is allocated to a bridge group (e.g. BRG-1), and a logical LAN interface is explicitly allocated within the IP network configuration
- > The second logical EXT interface was added to the MIB-2
- > Devices without dual SIM do not show a second logical EXT interface in the status tree
- > Routes which were learned dynamically via eBGP, iBGP or RIP are only added to their related routing context (routing tag) in the Forwarding Information Base (see [LANCOM knowledgebase](#))
- > The IKEv2 dead peer detection (/Setup/VPN/IKEv2/General/DPD-Inact-Timeout) does not only work with intervals of 60 seconds
- > IPv4 fragment forwarding (/setup/ip-router/1-N-NAT/Fragments/) with simultaneous QoS limitation is no longer classified as an attack. Communication is possible again
- > Fixed an unexpected router restart while accessing SCEP-CA certificate information
- > Fixed the usage of a wrong certificate for WEBconfig
- > Password length can now exceed a length of 15 characters when changing the router password of a user with administrative rights
- > The SNMP port 161 is no longer shown as closed, although SNMPv3 is allowed on the WLAN interface
- > The services SNMPv2 and SNMPv3 can be displayed separately
- > A CA fingerprint can now be applied to the internal LANCOM SCEP client, even if it consists of more than 59 characters

VPN

- > An IKEv2 VPN connection is not disconnected after a while, if the dead peer detection (DPD) cannot detect a connection to the VPN remote site due to a no longer existing child SA
- > An L2TP tunnel which was configured on one site only does not lead to a disconnect of an active second L2TP tunnel between the two routers
- > A configuration change by use of the sleep command caused by a script does not lead to a disconnect of an IKEv1 IPsec tunnel which cannot be established again
- > A „default -r“ within a script does no longer cause a VPN tunnel to not being established
- > If a LANCOM Router has accepted an IKEv2 connection via LAN, the connection is also established if the routing tag of the source address is 0

Wi-Fi

- > RADIUS authentication (IEEE 802.1x) of Wi-Fi clients in a WLC scenario is no longer aborted with the error message „missing private key“
- > Public spot authentication of a disabled user account by the „Manage Public Spot Users“ wizard is no longer possible, even if the user is listed in the auto ReLogin table
- > Access points can again connect via auto WDS, even if the applying frequency band within the WDS profile is set to “only 5GHz”
- > In a public spot scenario with PMS connection the link for authentication via voucher is available again, even if the language settings of the Wi-Fi client are set to French or Italian
- > Fixed an unexpected router restart which was caused by usage of the public spot user table (/setup/public-spot-module/user-table)
- > When printing a voucher again from within the public spot user management wizard the volume budget is displayed accurately on the integrated device templates
- > The IPv6 data communication over a WLC tunnel between a Wi-Fi client and a LANCOM Wi-Fi controller works again

VoIP

- > Fixed an unexpected router restart when transferring a DNS resolution to the Voice Call Manager (VCM)
- > A configuration update of the DECT base station LANCOM DECT 510 IP works after an address change of the provisioning update server (/Setup/Provisioning-Server). The base station is now provided with the information of an update URL change
- > Identical SIP users can be handled by multiple handsets registered to the same base station
- > DECT base stations are no longer listed with wrong IP address within the status table. The related LANmonitor display error is fixed
- > After software reboot (warm start) a connection to the SIP server can be established again, even when using an external SIP trunk line. A power disconnect (cold boot) is no longer necessary
- > When using a SIP trunk line, the "to" field within the SIP header is now converted properly to the E.164 format
- > With two configured SIP trunks it is now possible again to pass a call from one of the SIP trunks to a single SIP line account
- > The „Registered Mode“ for a Telekom SIP trunk is now active by default within the ALL-IP wizard

LCOS improvements 9.24.0076 RU2 ► 9.24.0153 RU3**Important notice to the update**

By default, SNMP access is disabled via WAN interface. If WAN access for SNMP was activated manually by configuration, access to SNMPv1 / SNMPv2 must be activated manually after the firmware update. The previous configuration setting for SNMP is retained for SNMPv3.

Bugfixes / Improvements:**Network Connectivity**

- > Fixed an issue which led to noise interference on clearmode connections
- > Fixed an issue with noise interference on outgoing SIP calls
- > WLC script rollout works again
- > Improved IKEv2 re-keying
- > IKEv2 VPN connections are established reliably
- > SIP phones can register to a superordinate VoIP phone system via SIP-ALG again
- > Outgoing calls can be established via the designated line if more than one SIP trunks or single accounts are configured
- > Unnecessary Wi-Fi modem load information have been removed from the bootlog

Wi-Fi

- > The confirmation page after a successful login is hidden earlier
- > Fixed a problem where no client could connect to a wireless network
- > Stability improvements for 802.11ac P2P Wi-Fi connections

LCOS improvements 9.24.0075 RU1 ► 9.24.0076 RU2**Important notice to the update**

By default, SNMP access is disabled via WAN interface. If WAN access for SNMP was activated manually by configuration, access to SNMPv1 / SNMPv2 must be activated manually after the firmware update. The previous configuration setting for SNMP is retained for SNMPv3.

Bugfixes / Improvements:**Network Connectivity**

- Reliable initialization of the integrated VDSL modem in particular situations

LCOS improvements 9.24.0070 Rel ► 9.24.0075 RU1**Important notice to the update:**

By default, SNMP access is disabled via WAN interface. If WAN access for SNMP was activated manually by configuration, access to SNMPv1 / SNMPv2 must be activated manually after the firmware update. The previous configuration setting for SNMP is retained for SNMPv3.

Bugfixes / Improvements:**Network Connectivity**

- The access rights for SNMPv2 can be switched separately now
- Fixed a problem that led to a non-working HTTPS communication from an Apple device with iOS 10 or macOS 10.12 to a LANCOM.
- A problem with the LANCOM DECT 510 IP has been fixed.

LCOS improvements 9.20.0683 RU2 ► 9.24.0070 Rel**New Features:****Network Connectivity**

- Auto provisioning support for LANCOM DECT 510 IP
- Support for Call-Forking within the Voice Call Manager
- Support for SIP methods PRACK and UPDATE
- Support for Message Waiting Indication within the Voice Call Manager
- The available Rx/Tx bandwidth can be configured manually for routers with integrated ADSL/VDSL modem

Wi-Fi

- Predefined bandwidth profiles for Public Spot
- Support for RADIUS CoA (Change of Authorization) within the Public Spot

LCOS improvements 9.20.0647 RU1 ► 9.20.0683 RU2**Important notice to the update**

The Loader 4.18 has to be flashed before updating the firmware of the LANCOM 1631E, LANCOM 831A and Business LAN R800A to LCOS 9.20.

Bugfixes / Improvements:**Network Connectivity**

- > Fixed a problem within the jitter buffer which led to a fax transmission abort
- > Access attempts to certain WEBconfig configurations no longer trigger a device restart
- > To avoid server problems, the HTTP client reads the complete server reply when authentication is needed before another request is started
- > IKEv2 VPN with NAT traversal works as designed
- > Fixed a problem with codec selection if a phone is directly connected to the LANCOM
- > Clip no Screening works again as desired, if a telephone system is connected to the LANCOM via S0 interface

LCOS improvements 9.20.0566 Rel ► 9.20.0647 RU1**Important notice to the update**

The Loader 4.18 has to be flashed before updating the firmware of the LANCOM 1631E, LANCOM 831A and Business LAN R800A to LCOS 9.20.

Bugfixes / Improvements:**Network Connectivity**

- > As of now, BGP packets are marked with DSCP CS6
- > Dial-up routes with simplified certificates for IKEv1 are set correctly
- > The table for automatic VLAN provider selection can be edited
- > DiffServ tags from inner tunnels as PPTP, L2TP, GRE or EoGRE are now applied to the outer VPN tunnel
- > Improvements in IKEv2 re-keying
- > Interoperability improvements for TLS 1.2 connections
- > RIP propagates a conditional route if the remote station is connected
- > ICMP polling works again with loopback addresses
- > Fixed the active calls counter within the voice call manager
- > LANmonitor displays the firewall rule of the first matching action
- > No syslog message is sent if a broadcast is received and rejected on the LAN interface
- > SMS can be sent and deleted via LANmonitor
- > Improvements in SIP-ALG in conjunction with Mitel telephone systems. OPTIONS packets are sent from the correct port
- > Fixed a problem with SIP ALG
- > Fixed an issue where routing between local networks in conjunction with policy based routing did not work
- > A forwarded call from an analog phone does not lead to unilateral voice transmission
- > The rollout agent starts a rollout even if a config server URL is not transmitted via DHCP-Option 43, but instead is provided within the device configuration
- > Fixed issues in conjunction with Swyx (CTI+, call forwarding, etc.)
- > Support for 1TR114 SIP methods PRACK und UPDATE by Deutsche Telekom vSDP
- > VLAN assignments per ISP are now possible

Wi-Fi

- > OAP-830: The internal assembly of the Wi-Fi modules has been swapped to improve Wi-Fi performance. When running point-to-point connections with the OAP-830, please consider the following knowledge base article:
<https://www2.lancom.de/kb.nsf/0/2FD8349316D983AAC1257FF0002F850D?opendocument>
- > Fixed a problem where remotely managed access points did not receive the configuration from a WLC if the WAN link MTU was too large.
- > An access point in client mode within an 802.11ac connection can re-connect to a base station

LCOS improvements 9.20.0517 RC2 ► 9.20.0566 Rel**Important notice to the update**

The Loader 4.18 has to be flashed before updating the firmware of the LANCOM 1631E, LANCOM 831A and Business LAN R800A to LCOS 9.20.

Bugfixes / Improvements:**Network Connectivity**

- > Fixed a problem with T.38 fax transmission
- > If the WEBconfig All-IP wizard is started a second time, all previous settings are replaced as expected
- > PPTP tunnels are re-established after an item is added to the backup table
- > Fixed a problem with enforced bandwidth reservation

Wi-Fi

- > Clients with an Intel AC-7260 chipset can connect to an Access Point running in „ac only“ mode
- > Authentication via 802.1x under occurrent high packet load works again with 11ac Access Points
- > CAPWAP does not set any host routes to targets within the local network, if a static IP address was allocated by a WLC

LCOS improvements 9.20.0385 RC1 ► 9.20.0517 RC2**Important notice to the update**

The Loader 4.18 has to be flashed before updating the firmware of the LANCOM 1631E, LANCOM 831A and Business LAN R800A to LCOS 9.20.

Bugfixes / Improvements:**Network Connectivity**

- > Fixed an All-IP wizard bug where not all entries were deleted as desired
- > If an L2TP remote station is disconnected, the according RIP routes are no longer provided
- > After a fallback to 2G the router does not remain in Edge mode permanently
- > The iPerf server daemon is accessible via VPN, if WAN access is limited to VPN
- > Fixed a problem where a SIP line could not register due to missing DNS resolution
- > SIP packets bigger than 1024 bytes are no longer cut
- > The iPerf server report can be received by the iPerf client if client packets contain a VLAN tag
- > If a call is put on hold, music on hold playback is correct

Wi-Fi

- > Location Based Services (LBS) is no longer configurable on devices without Wi-Fi or WLC option
- > Public Spot template preview is visible only if a Public Spot option exists on the LANCOM device
- > A configured Public Spot login text is displayed correctly
- > Reduced memory usage with enabled aggregation and 802.11n modules

LCOS improvements 9.10.0530 RU5 ► 9.20.0385 RC1**Important notice to the update**

The Loader 4.18 has to be flashed before updating the firmware of the LANCOM 1631E, LANCOM 831A and Business LAN R800A to LCOS 9.20.

New Features:**Network Connectivity**

- > Support for automated rollout via DHCP option 43
- > The SCEP client obeys certificate dependencies
- > Support for DTMF conversion for All-IP
- > Support for SNMPv3
- > The Voice Call Manager supports now TCP for SIP connections
- > The Voice Call Manager supports now Voice over Secure IP (SIPS/SRTP)
- > The amount of detected devices is shown with ll2mdetect
- > The ADSL/VDSL state displays modem sync duration and connection count
- > NTP client and server support IPv6
- > Option for changing EAP-TLS settings, if the LANCOM device works as 802.1x supplicant
- > Support for IKEv2
- > Support for BGP v4
- > The device status display shows an active backup connection and the number of established backup connections
- > A backup can be triggered if a memorized route is no longer available (Route Monitor)
- > The IPv6 firewall rule „Allow-IPSec“ is enabled by default
- > Using syslog, DNS requests can be forwarded to an external syslog server
- > LCOScap supports IPv6
- > Support for IPv6 VPN with IKEv1
- > A Syslog server can be enregistered as DNS name or IPv6 address
- > SIP messages can be set to be only accepted from the SIP registrar
- > Overlap dialing support for SIP trunks
- > WAN connection prio tags are taken over to the VLAN header according to 1TR-112 or DSCP
- > Extended support for TR.069 and TR.181
- > The syslog shows the reason for a denied RADIUS server authentication request
- > Support for ChaCha20-Poly1305 for SSH
- > CA support for SCEP message GetCaCaps
- > Adapted IKE and PFS default groups to DH group 14 within VPN
- > Registered SIP users are not deleted on configuration changes
- > Support for ISDN parallel calls
- > Support for IPPerf as server and client
- > Switchable configuration protocols
- > Added an open ports display in WEBconfig under the „Services“ tab
- > Powersaving for ethernet interfaces is enabled by default
- > Removed the VLAN tagging mode „Incoming mixed“
- > DHCP lease time is configurable per network
- > Password complexity for the main device password and further administrators can be forced

Wi-Fi

- > IAPP is disabled if a CAPWAP tunnel is active
- > Support for Airtime Fairness
- > Radio-field optimization can be done on autonomous Access Points
- > Multiple AutoWDS profiles can be configured on a WLC
- > Support for Adaptive RF Optimization
- > Support for Wireless Intrusion Detection System (WIDS)
- > Average Wi-Fi error rates of particular Access Points can be read out on a WLC
- > Using the URL variable „%r“, the MAC address of the Access Point to which a client is authenticated can be transmitted in a Public Spot redirect.
- > The absolute elapse time of a Public Spot voucher can be configured in minutes and seconds
- > Added a counter for displaying failed WPA authentication attempts
- > Specified data rates can be configured per SSID
- > The Public Spot function „Accept Terms and Conditions“ is utilizable when using PMS
- > The displayed columns can be configured within the Public Spot/Manage User wizard
- > Surplus blank characters while typing usernames and passwords are removed automatically
- > The assigned bandwidth profile for a Public Spot user can be shown on the voucher
- > Brute Force protection can be realized by configuring a login blocker
- > Added a switch to forward HTTPS connections from unauthenticated clients to the Public Spot gateway
- > Added an option to preview the uploaded Public Spot templates via WEBconfig
- > Support for Spectral Scan for 802.11ac Wi-Fi modules
- > Improved Wi-Fi rate adaption
- > The current channel width and used MCS are now displayed in the Wi-Fi interpoints table and in the station table

Bugfixes / Improvements:**Network Connectivity**

- > Fixed a bug which led to a router restart when viewing the SMS inbox via WEBconfig
- > Fixed a DNS resolution problem where an explicit DNS forwarding configuration was needed
- > Port forwarding of VPN ports 500 and 4500 works again
- > Fixed the firewall packet action „Only when default route“
- > Variable „DEVICE_URL“ works again when used with the „loadscript“ command
- > If a VPN tunnel is established via DynDNS names, the name is re-resolved immediately after a disconnect, so that the tunnel is not established to the previous address
- > A SIP phone call via SIP-ALG, which uses PRACK, is no longer disconnected
- > The Internet configuration wizard sets the correct netmask within WEBconfig
- > Fixed a problem which led to a router restart due to lack of memory
- > A dynamic VPN connection can be established via Load Balancer
- > The time display within the IPPerf status table is shown more noticeable
- > Outgoing SIP Trunk lines of a phone system via SIP-ALG are no longer disconnected
- > Corrected the negotiated WAN interface MTU for IPv6
- > Fixed a bug which prevented a 4G backup connection establishment

Wi-Fi

- > Fixed a problem that only particular clients could authenticate to an 802.11ac accesspoint
- > Fixed a bug which led to a several minute lasting inaccessibility of an accesspoint in client mode while roaming between base stations
- > Configuration can be written again to devices with less memory
- > Check of the DNS server response is now case insensitive
- > Fixed a certificate error when an accesspoint tries to connect to a WLC

Comments

If you want to upgrade the firmware of your device to a new version, please install the latest LCMS version first. **Before running the firmware-upload you should save the router configuration to a file.** After that you can use LANconfig to load the latest LCOS-version into the device.

In principle, we suggest upgrading the firmware of your device only if you are in need of the latest features.

Please note that different firmware files might be available for your device. Further information can be found in the file README.PDF in the download area of our homepage.