LANCOM Systems

Information regarding

LCOS Software Release 8.80 SU2

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

Internet: http://www.lancom.eu

25.10.2017, CBuersch

Table of Contents

1. Preface

LCOS („LANCOM Operating System“) is the operating system for all LANCOM routers, wireless LAN access points and WLAN 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 dowload from LANCOM Systems.

This document describes the innovations within LCOS software release 8.80 SU2, as well as the improvements since release 8.62.

Warning hints – 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 WLAN bridges, please keep in mind to upgrade the remote device first and the local device afterwards.

Warning hint – LCOS upgrade for devices LANCOM OAP/IAP-321-(3G) and LANCOM 1780EW-3G

Some of the current LANCOM WLAN routers and access points with LCOS 8.5 or earlier, which are to receive new firmware or extensive new configurations over the wireless LAN interface, may under certain circumstances suffer from WLAN connection loss. The result of this error is that the wireless link is interrupted and, in the worst case —such as with an outdoor point-to-point link— the device may lose contact completely. In this case, re-establishing the radio link would require a manual restart of the remote device by pressing the reset button. To prevent this we recommend to configure an -> alive test before uploading a new firmware.

Note – 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.

Note – Using converter firmwares

You will need enough free memory to use a firmware 6.0 and newer in your LANCOM 15x1, 1611+, 821+ and DSL/I-10+ and LCOS 8.0 in a LANCOM XAC or LANCOM 1823 VoIP. These changes apply for devices LANCOM 1722, 1723 and 1724 with LCOS 8.8 ff., too.
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.

Note – 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.

Note – Using VoIP options

VoIP options for LANCOM 1821 Wireless ADSL are discontinued with LCOS 7.20. The final version containing the VoIP Call Manager is LCOS 6.32.
As from LCOS 7.5x support for VoIP options for the devices LANCOM 1511 Wireless DSL and 1521 Wireless ADSL is discontinued. The final version containing the VoIP Call Manager is LCOS 7.30.
For the „VoIP ready“ routers LANCOM 1711 VPN, 1721 VPN and 1811 Wireless DSL support for the subsequently installed VoIP option will be discontinued with LCOS version 7.56. If you want to continue using your VoIP option, please do only use LCOS versions up to and including 7.54.
For T-Systems Business LAN R800+ VoIP functionality is discontinued in LCOS 7.60
LCOS 7.70 is the final version supporting VoIP options for the remaining „VoIP ready“ devices.

Note – Device specific support of the current LCOS version

As from LCOS 8.50 support for the following devices is discontinued:

- LANCOM 1811 Wireless
- LANCOM 1721 VPN

For the following devices the additional, LANconfig-like WEBconfig view is removed as from LCOS 8.60:

- LANCOM L-310
- LANCOM L-305
- LANCOM L-54 dual Wireless
- T-Systems Business LAN R800+

Please use instead either LANconfig or use the configuration view “LCOS Menu Tree” in WEBconfig

As from LCOS 8.80 support for the following devices is discontinued:
- LANCOM L-54 Wireless (Hardware release <E)
- LANCOM L-54 dual Wireless (Hardware release <G)
- LANCOM OAP-54-1 Wireless

2. Known Issues

Latest support notes and known issues regarding the current LCOS version can be found in the download area of our website http://www.lancom-systems.eu/Common-Support-Hints.64.0.html

3. New Features, Improvements and History

LCOS improvements 8.80.0159 RU1 ► 8.80.0219 SU2

Bugfixes / Improvements:

- A security issue within WPA2 authentication (KRACK attack) using P2P connections with 802.11a/b/g/n Wi-Fi modules has been fixed:

  CVE-2017-13077: reinstallation of the pair-wise key in the Four-way handshake
  CVE-2017-13080: reinstallation of the group key in the Group Key handshake

  The WLAN client mode / WLAN station mode with 802.11a/b/g/n Wi-Fi modules is not affected.

Note:

- LCOS is not affected by the following WPA2 security issues (KRACK attack):

  CVE-2017-13084: reinstallation of the STK key in the PeerKey handshake
  CVE-2017-13086: reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake
  CVE-2017-13087: reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame
  CVE-2017-13088: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame
  CVE-2017-13078: reinstallation of the group key in the Four-way handshake
  CVE-2017-13079: reinstallation of the integrity group key in the Four-way handshake
  CVE-2017-13081: reinstallation of the integrity group key in the Group Key handshake

- LCOS would only be affected by the following WPA2 security issues (KRACK attack) when using 802.11r (fast roaming), but this is not supported by this LCOS version:

  CVE-2017-13082: accepting a retransmitted Fast BSS Transition Reassociation Request and reinstalling the pair-wise key while processing it

LCOS improvements 8.80.0157 RU1 ► 8.80.0159 RU1

Bugfixes / Improvements:

Network Connectivity:

- The initial recognition of the mobile access card on the device start up has been improved

LCOS improvements 8.80.0135 Rel ► 8.80.0157 RU1

Bugfixes / Improvements:

WLAN:

- The configuration of a LANCOM 3850 without external WLAN card can be stored to the device without errors
- The automatic MAC address authentication within the Public Spot module can be used again
- URL forwarding works again after login when using Public Spot SmartTicket
- Radio-field optimization does no longer affect RADIUS configuration

VoIP:

- SIP-ALG can be used with LAN-LAN routing, too
- SIP-ALG can handle multiple accounts of a Telekom Call&Surf IP connection
- SIP-ALG allows for SIP update requests.

Network Connectivity:

- A RADIUS server can assign IPv4 addresses to the LANCOM again
- If a dynamic IPv6 prefix is used in conjunction with fixed address assignment, the assigned address is released when the current prefix is discontinued
- The masking address of the WAN IP table is no longer used for answering ARP requests
- Dynamic VPN over D channel can be used again
- An entry in the DNS forwarding table is operative without restart
- If a server sends a TCP ACK to an expired session, the LANCOM answers with an RST
- If no DNS server was assigned to an internet remote station, the DNS server under TCP/IP->Addresses is used

LCOS improvements 8.80.0128 RC3 ► 8.80.0135 Rel

Bugfixes / Improvements:

WLAN:

- Syslog reporting if a WLAN client is disassociated due to an invalid MAC address
- On a L-452dual point-to-point connections are displayed by WLAN LED in addition to the WLAN station count
- The LANCOM 1781VA supports the Public Spot administration portal SmartTicket, too, and the XML interface between LANCOM Public Spot module and an external authentication gateway

Network Connectivity:

- Configured session- and user limits are considered again
- If a LANCOM 1781VA is used with an analog line, incoming calls do no longer lead to a loss of the ADSL sync of the internal modem
- Neighbour Solicitations on a PPP connnection do not lead to proclamation of the default router in the LAN

LANCOM Systems

LCOS improvements 8.80.0095 RC2 ► 8.80.0128 RC3

New Features:

Network Connectivity:

- LANCOM devices without integrated WLAN module can provide LEPS information for access points via the internal RADIUS server

Bugfixes / Improvements:

WLAN:

- After activating a WLC option the access table is extended by the WLAN interface automatically

VoIP:

- If media information is missing in INVITE packets, there is no router restart if SIP-ALG is activated
- Optimized memory usage with activated SIP-ALG

Network Connectivity:

- Internal DNS requests are no longer blocked by the firewall if the DNS rule refers explicitly to the internet remote station
- The SSL port can be changed by WEBconfig again
- Invalid routes do no longer cause a router restart
- The LANCOM device can be configured via an interface which uses IPv6 auto configuration
- The default settings wizard allows device access from local and by VPN connected networks by default
- The internet wizard offers already existing remote stations in a selection list for activating IPv6
- A new IPv6 route is created in WEBconfig with correct default values
- The 4G LED of the LANCOM 1781-4G exclusively shows the state of the mobile connection
- If the WAN connection is terminated or the LANCOM device is manually restarted, VPN- and PPTP connections are terminated before
- Loadbalancer connections with a routing tag are considered in IDS recognition
- Improved VPN error display

LCOS improvements 8.80.0078 RC1 ► 8.80.0095 RC2

New Features:

WLAN:

- If all WLAN channels are blocked due to DFS detection this is reported to WLAN log table and syslog

Network Connectivity:

- Implementation of the new contentfilter category „Command & Control Server“
- Date and time can be set via GPS on devices with integrated mobile radio module
- IPv6 support for LANCOM 1722, LANCOM 1723 and LANCOM 1724

Bugfixes / Improvements:

WLAN:

- Configurable country code in Public Spot / Smart Ticket

VoIP:

- No more faulty IP information in the contact field if SIP-ALG is used in conjunction with the loadbalancer

Network Connectivity:

- No error when trying to set an overlength password via WEBconfig
- The remote station is displayed in the accounting syslog
- Mobile connections can be established with the LANCOM 1781-4G again

LCOS improvements 8.62.0050 RU2 ► 8.80.0078 RC1

New Features:

WLAN:

- Implementation of WLAN Band Steering
- Implementation of Spectral Scan
- Support for STBC (Space/Time Block Coding) and LDPC (Low Density Parity Check)
- Support for DFS 4
- Support for Public Spot Administration portal SmartTicket
- Release for DNS domains in the Public Spot table „Free Networks“
- Implementation of an XML interface between the LANCOM Public Spot module and an external authentcation gateway
- Public Spot users who become authenticated via the internal LANCOM RADIUS server do no longer have to pay attention for upper-/lowercase when entering their usernames
- The link state of a WLAN Point-to-Point connection is shown
- WLAN performance improvements between 11n- and abg clients (Airtime Fairness)
- abg clients are rejected in Greenfield mode
- Wildcards may be used In the Public Spot table „Free Networks“
- A possible multi-login can be configured using the WEBconfig’s PublicSpot Wizard
- Using a WLC different RADIUS servers can be assigned to the accesspoints for each SSID
- Public Spot user management can be allowed via seperate access rights
- If a LANCOM dual radio client roams, one WLAN module is connected to the “old” access point until the second WLAN module is connected successfully to the “new” access point
- UUID transmission within the WLAN beacons, so that WLAN planning software is able to recognize dual access points

Network Connectivity:

- Migration of IPv4 and IPv6 (Dual-Stack)
- IPv6 Gold certification (Core protocols and DHCPv6 servers)
- Implementation of the IPv6 firewall
- Support for stronger key lenghts for encrypted connections
- Syslog-, eventlog- and bootlog output can now be saved to flash bootpersistent
- Configuration files and certificates can be uploaded to the LANCOM via SSH
- Configuration changes are written to the syslog protocol
- By default, syslog output is changed to show new entries on top of the table
- Pre-calculation of Diffie-Hellman keys for faster connection establishment
- SNMP read access via community „Public“ is possible on VPN connections, too.
- Support for IPsec Replay Detection
- By default, accounting data is no longer written to the syslog protocol
- Configurable SSH protocols and key lengths
- The DSLoL interface is used in exclusive mode by default
- Network traffic can be recorded via WEBconfig (Wireshark compatibility)
- Configurable Brute Force protection for profile requests for the myVPN application
- Profile request for the myVPN application can be suppressed on the WAN
- Support for the Link Layer Discovery Protocol (LLDP)
- Multiple VPN errors can be reset using only one command
- Invalid column names or SNMP-IDs are ignored by a script’s tab command
- By default, NTP server requests are done with reduplicate timeouts, until time is successfully synced. Syslog messages are generated for success or fail

Bugfixes / Improvements:

WLAN:

- If a PublicSpot voucher is printed via „Manage Public Spot users “ at a later time, the SSID is printed, too
- Activating an alternative boot configuration includes the WLAN parameters, too
- If an access point gets an IP address from a WLAN controller over a routed connection, the WLC remains accessible for the AP
- No more WLAN performance problems due to aggregation errors on a LANCOM L-45x

VoIP:

- Incoming calls on a PBX connection can be answered via SIP-ALG
- Via SIP-ALG incoming calls can be answered even if there are multiple lines to the same registrar

Network Connectivity:

- If the clock is set with disabled DST, the time is set correctly
- Improvements in fax receiving via LANCAPI
- DNS forwardings are sent with the correct source address with multiple tagged ARF networks
- Connection via ll2m works even if data packets arrive duplicate (e.g. redundant network paths)
- Uncategorized sites are no longer treated as whitelist addresses by the Content Filter
- The email notification of the content filter sends daily messages only if an appropriate event has occured (e.g. license expiration)

4. 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.

