

LANCOM Release Notes for GS-13xx

LCOS SX

3.32 RU7

Copyright (c) 2002-2020 LANCOM Systems GmbH, Wuerselen (Germany)

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

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

October 23rd, 2020, MKoser

Table of Contents

1. Preface	2
2. New features, improvements, and history	3
LANCOM GS-13xx improvements 3.32.0222 RU7	3
LANCOM GS-13xx improvements 3.32.0221 SU6	4
LANCOM GS-13xx improvements 3.32.0210 RU5	4
LANCOM GS-13xx improvements 3.32.0208 RU4	4
LANCOM GS-13xx improvements 3.32.0114 RU2	5
LANCOM GS-13xx improvements 3.32.0110 RU1	5
LANCOM GS-13xx improvements 3.32.0012 Rel	6
LANCOM GS-13xx improvements 3.30.0450 RU4	6
LANCOM GS-13xx improvements 3.30.0417 RU3	7
LANCOM GS-13xx improvements 3.30.0321 RU1	7
LANCOM GS-13xx improvements 3.23.0006 Rel	7
LANCOM GS-13xx Switch OS 3.23.0001 Rel	8
3. Common advice	9
Disclaimer	9
Support notes & known issues	9

1. Preface

LCOS SX is the operating system for all LANCOM switches. In the context of the hardware given by the products the at a time latest LCOS SX version is available for all LANCOM switches and is available free of charge for download from LANCOM Systems.

This document describes the innovations within LCOS SX software release 3.32 RU7, as well as the improvements since the previous version.

Before upgrading your device to a new firmware it is essential to **backup your device's configuration**.

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

Please note that different firmware files might be available for your device.

2. New features, improvements, and history

LANCOM GS-13xx improvements 3.32.0222 RU7

Bugfixes / improvements

- With MAC-based 802.1X authentication against a RADIUS server, a client was authenticated although the RADIUS authentication was answered with a 'RADIUS Reject' and 'EAP Success'. However, the 'Success' type EAP packet only refers to successful EAP communication.
The switch only interpreted the EAP part, but not the contents of the RADIUS packet (the 'RADIUS Reject'). Therefore a client that was not known on the RADIUS server was also successfully authenticated.
- The switch is now able to transmit the RADIUS attributes 'NAS Identifier' and 'Service Type=Call Check'.
- The maximum length of an SSH hostkey has been extended from 1024 bits to 2048 bits.
- A MAC-based 802.1X authentication against a RADIUS server was passed as a RADIUS request without EAP components and with the MAC address as user name.
- When using 802.1X authentication with the 'Single 802.1X,' 'Multi 802.1X' and 'MAC-based Auth.' modes, the MAC addresses were not transferred to the MAC address table after the terminal devices successfully logged in.

LANCOM GS-13xx improvements 3.32.0221 SU6

Bugfixes / improvements

- › Special user input via the web interface was not validated correctly. This could provoke a sudden restart of the device.

LANCOM GS-13xx improvements 3.32.0210 RU5

Bugfixes / improvements

- › When operating LANCOM switches of the GS-13xx series, it could happen that devices lost their serial number and MAC address after a restart and were also unable to obtain an IP address. The devices continued to operate, but the affected switches could no longer be reached via their IP address.

LANCOM GS-13xx improvements 3.32.0208 RU4

New features

- › In the 'Authentication Method Configuration' it is now possible to configure the protocols HTTP and HTTPS separately.
- › Simplification of the VLAN port marking
- › A warning is now displayed in the 'System Log Configuration' for insecure 'SNMPv2 Get community' configuration.

Bugfixes / improvements

- › The passwords stored in the configuration files are now stored encrypted.
- › When using 802.1X with the 'Mac-based Auth.' authentication mode, the 'RADIUS-Assigned VLAN Enabled' feature could not be enabled.
A new 'MAC-based single Auth.' authentication mode has been implemented to allow the use of the 'RADIUS-Assigned VLAN Enabled' feature.
- › Although access to the web interface was blocked in the configuration, the login page of the web interface was displayed when an access attempt was made. However, a login was not possible.
- › After disabling 'Web' in the 'Authentication Method Configuration', port 80 was displayed as open, but access to the web interface was not possible.
- › When using the feature 'Port Based 802.1X' and the VLAN mode 'Trunk' a connected device could be authenticated, but a data transmission was not possible.
- › If a Voice VLAN was configured on the switch, the MAC address of individual connected network devices was sporadically no longer included in the MAC address table after the 'Voice VLAN Aging Time' had expired. This caused these devices to no longer being able to communicate in the network. Only devices in VLANs that did not correspond to the Voice VLAN were affected.

- When setting a static MAC table entry in the menu 'Filtering Data Base / Configuration', the switch restarted abruptly.
- If a port-based VLAN was configured and an additional configuration for MAC-based VLAN was added, only the MAC-based settings worked; the advanced settings were ignored.
- The 'Limit Control' function in the 'Security / Port Security' menu could only be activated via the web interface. If an attempt was made to activate the function via the console, the error message "Port Security Limit Control Configuration of easyport must be preserved" was displayed.

LANCOM GS-13xx improvements 3.32.0114 RU2

Bugfixes / improvements

- If the LANCOM switch detected a network loop, until now only the timestamp and blocked port have been logged to a syslog message. The network loop detection now additionally logs the number of the second involved port, and also shows an information about which port was the sender and which one was the receiver of the loop protection frame.

LANCOM GS-13xx improvements 3.32.0110 RU1

New features

- Extension of the device logs
- Extension of PoE Detection (Legacy Mode)
- New switch for sFlow (Always On)

Bugfixes / improvements

- The LANCOM switches transmitted MAC addresses (e.g. from supplicants with 802.1X on a RADIUS server) exclusively using small letters (e.g. 00-10-a4-23-19-c0). However, according to RFC-3580, upper case letters must be used (e.g. 00-10-A4-23-19-C0), which is now the case.
- The automatic conversion of the time to Central European Summer Time (CEST) was one week too early.
- Due to a too small internal data buffer, too large TLV (Type-Length-Value) packets were discarded. As a result, the authentication of a client via 802.1X to a RADIUS server failed.
- If the web interface of the switch was prompted via an IPv6 address, the online help display did not work.

LANCOM GS-13xx improvements 3.32.0012 Rel

New features

- Added a hint for a not yet saved configuration to the configuration interface
- For SSL and TLS configurations, the minimum SSL and TLS versions to be applied are now selectable from a drop down list.

Bugfixes / improvements

- If STP was activated on the switch ports, and this configuration was saved as "Start configuration", it could happen that after a cold boot the displayed uptime value in the menu "configuration > port status" was stated with 2627 days.
- When saving a configuration to an *.xml file, PoE configuration parameters for "Power delay", "Auto checking" and "Scheduling" were missing.
- Switch ports with configured 802.1X Single-/ multi mode port authentication were blocked after 4-6 minutes and re-released after a further 4-6 minutes. The port status was always (even with blocked status) shown as "Authorized".
- The automatic completion of "show" commands using the tab key failed on the command line due to the spelling of the command "show-3rd-party-licenses" for all managed switches.
- In the web configuration the error string of an error message was not scaled to the size of the message area.
- Descriptions for configuration options for individual switch types were missing in the online help for the function "Configured link speed" (in the menu "Port configuration").
- When using the function MAC-based authentication for connected access points, a change of the switch ports due to Wi-Fi roaming caused a sudden switch restart, if the MAC address of the Wi-Fi clients was deposited on the RADIUS server.
- When using multiple switches with activated RSTP in a ring structure, and simultaneously activated DHCP snooping 100% CPU load was generated on a big amount of clients (more than 500).
- General stability improvements.

LANCOM GS-13xx improvements 3.30.0450 RU4

New features

- The current memory consumption can now be shown on the GUI.
- Device configuration files can now be exported and imported encrypted.

Bugfixes / improvements

- Only 94 different clients (MAC addresses) could access the switch management at the same time. If one more client tried to access the switch, its web interface was not accessible.

- With LANCOM SFP-CO1 copper modules, the status of the numerically smaller port was displayed with “up” instead of “down” in case of a loop.
- A malfunction within the DHCP snooping function created a false linkage in the switch’s internal IP address list, which caused a list-internal LOOP. This caused internal services to be executed endlessly when working the list. This led to a 100 % CPU load and blocked any further services from executing (e.g. packet flow).

LANCOM GS-13xx improvements 3.30.0417 RU3

New features

- Support for the new SFP copper module LANCOM SFP-CO1
- New function “Password Policy” (minimum requirements for a secure password)

Bugfixes / improvements

- General stability improvements

LANCOM GS-13xx improvements 3.30.0321 RU1

Bugfixes / improvements

- Though more than one IPv6 management addresses were announced in LLDP, the dialogue „LLDP > LLDP Neighbours” showed only the first IPv6 management address.
- The link to a second management address of another device, which was learned via LLDP, could not be invoked.
- A request of the port status via HTTP/S under Security > Port Security > Port Status -> Port lead to a non-availability of the switch management (via management IP), if this function was activated, and many MAC addresses were listed for the requested port.
- Adding a hostname under ‘TACACS+ Authentication Server Configuration’ lead to a sudden restart of the switch after confirmation of the changes.

LANCOM GS-13xx improvements 3.23.0006 Rel

Bugfixes / improvements

- The OIDs for displaying the device’s complete system information in LANmonitor were added. At least LANmonitor version 10.10.0012-RU3 is necessary for displaying this information.

LANCOM GS-13xx Switch OS 3.23.0001 Rel

New features

- > Initial Switch OS with support for the LANCOM GS-1326

3. Common 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.

Support notes & known issues

Latest support notes and known issues regarding the current LCOS SX version can be found in the download area of our website: [Common support hints](#)