Release Notes

LCOS SX
4.00 SU13

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.

LCOS SX 4.x is the operating system for all LANCOM switches of the GS-3000 series.

The LCOS SX 5.x operating system is available for all LANCOM switches of the GS-4500 and XS series.
The LCOS 3.32 operating system is available for all LANCOM switches of the GS-1300 / GS-2300 series.
The release notes for these device series can be found as usual on the LANCOM website in the download area of the respective switch.

This document describes the new features of the LCOS SX software release 4.00 SU13 as well as the changes and improvements to 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. The release tag in the software name

Release Candidate (RC)

A Release Candidate has been extensively tested by LANCOM and includes new LCOS featurses. It is suitable for testing and is not recommended for use in productive environments.

Release Version (REL)

The release version has been extensively and successfully tested in practice. It contains new features and improvements over previous LANCOM operating system versions and is therefore recommended for use in productive environments.

Release Update (RU)

A release update is a further development of an initial release version in productive environments and contains minor improvements, security fixes, bug fixes and smaller features.

Security Update (SU)

Contains important security fixes for the respective LANCOM operating system version and ensures that your security level remains very high on an ongoing basis in your productive environment.

3. New features, improvements, and history

LANCOM GS-3100 / 3500 series - LCOS SX 4.00.0716 SU13

Bug fixes

→ A security vulnerability in the RADIUS protocol has been fixed (VU #456537).

LANCOM GS-3100 / 3500 series - LCOS SX 4.00.0715 RU12

Bug fixes

→ After updating a LANCOM GS-3510XP to version 4.00 RU11, it could happen that the switch remained in the status ‘Checking availability’. As a result, it was no longer possible to roll out a configuration.

LANCOM GS-3100 / 3500 series - LCOS SX 4.00.0713 RU11

New features

→ The password length of the user account has been increased to 128 characters.

→ The length of SNMP-USM passwords has been increased to 128 characters and the length of RADIUS secrets has been adjusted to 64 characters.

→ A password for MAB authentication can now be assigned globally per switch.

→ The 802.1X MAC-based MAC format is now configurable as follows:

- **Group-Size:** 1 / 2 / 4 / 12 (Nibble / Byte / 2-Byte / No separator)
- **Separator:** Dash - / Colon : / Dot .
- **Case:** Uppercase / Lowercase

Bug fixes

→ The ACL (Access Control List) is always active for DHCP. DHCP packets are allowed. BootP packets without ‘DHCP Message Type’ set were not supported by the ACL and therefore discarded. This caused that additional parameters could not be transferred via BootP.
BootP packets are now internally treated as DHCP request or DHCP ACK so that the packets are allowed by the ACL.

→ If a configuration was uploaded to the switch via SCP with a password that did not meet the password policy, the password subsequently remained blank.

→ When using Voice VLAN, a Wi-Fi client could only roam successfully after 5 minutes if MAC traps were used on the switches.

→ If an entry was added in the detailed configuration of the LMC in the menu ‘Security / ARP Inspection’, the configuration could no longer be rolled out to the switch.

→ The data field for the 802.1X Identity could not hold enough characters. The length of the field has now been extended.

→ If a server name was specified in the LMC’s detail configuration that contained a 4-digit IP address (e.g. 9.9.9.9), it was appended with a ‘0’ in the switch’s configuration after the LMC rolled it out (e.g., 9.9.9.90).

→ The CLI command ‘show running-configuration all-defaults’ did not check the default values of the entry ‘event group link-status trap’ against the values of the running configuration, resulting in inconsistent values.

→ When configuring multiple VLANs in an MST instance via the detailed configuration of the LMC, only the last VLAN was always taken over by the switch. This resulted in Spanning Tree not working on the other VLANs.

→ If the ‘Config-Change Notification’ from the LMC client in the switch to the LMC after a configuration change was not successful at the first attempt, the notification was not deleted after a successful notification to the LMC. This resulted in the LMC client sending the ‘Config-Change Notification’ to the LMC again and again.

→ The ARP table of the LANCOM GS-3510XP holds a maximum of 256 entries. Obsolete entries were only deleted after reaching 128 entries. This could result in limited ARP communication.
Obsolete entries in the ARP table of the GS-3510XP are now deleted in increments of 16/64/128 entries.

→ When importing a configuration backup, if a new configuration was created in the switch and a name with a space at the end was selected, the view in WEBconfig showed the string “%2520” instead of the space. This resulted in the file not being able to be deleted from the switch and an error being displayed instead.

→ In individual cases, a deadlock could occur between two threads in the RADIUS module after a rollout of the configuration in the LMC when using 802.1X. This led to an immediate restart of the switch.

→ When changing all ports via WEBconfig in the menu ‘Port Management / Port Configuration’ to another mode at the same time, not all ports were set to the same mode, so that some ports remained in the previously set mode.

LANCOM GS-3100 / 3500 series - LCOS SX 4.00.0614 RU10

New features

→ The switch can now be authenticated as a ‘supplicant’ on the RADIUS server.

→ A software switch has been added to the RADIUS Supplicant feature that changes the MAC address used by the 802.1X supplicant to the system MAC address for easier use of single and multi-auth modes.

→ SYSLOG support according to RFC 5424

→ Switches return the host name instead of the IP address as SYSLOG message.

→ A config check for an SSH / SCP based rollout tool has been added.

Bug fixes

→ When accessing a switch via SSH, the switch always performed a reverse lookup of the requesting client. If the IP address of the client was not contained in the station table of the DNS server, the SSH connection was only established after a DNS timeout and thus with a corresponding delay.
Now a reverse lookup is no longer performed when accessing via SSH.

→ When the switch receives a configuration via SSH/SCP, it acknowledges the successful import of the configuration with a message on the command line.

→ If a network device connected to the switch sent an ‘EAP Logoff’ when ‘MAC-based Fallback’ was enabled, the switch switched back to ‘Single 802.1X’ or ‘Multi 802.1X’ authentication mode on this port. This meant that authentication by MAC address was not possible.
After an ‘EAP Logoff’ the ‘MAC-based Fallback’ is now activated immediately.

LANCOM GS-3100 / 3500 series - LCOS SX 4.00.0501 RU9

New features

→ RADIUS MAC address bypass / fallback has been implemented - e.g. if 802.1X authentication is rejected, the MAC-based request is sent after an optionally definable waiting time.

→ RADIUS assigned VLANs are now also supported for multi-client modes ‘Multi 802.1X’.

→ To monitor the temperature of the switches, an OID was added as an integer. Previously, this information was only available as a DisplayString.

Bug fixes

→ Vulnerabilities in the Net-SNMP software suite have been fixed. (CVE-2022-24805 to CVE-2022-24810).

→ If the ‘NAS IP Address’ field was left blank or a specific IP address was stored in the RADIUS server configuration, the switch always used the default IP address 172.23.56.250 for RADIUS authentication instead of the configured ‘NAS IP Address’ or the management IP address.

→ If an addin script was used in an LMC scenario that subsequently adjusted values set via detail configuration, an invalid configuration could occur during a rollout attempt (e.g., if the guest VLAN was first deactivated and then the guest VLAN ID was adjusted). This resulted in an error during the rollout, so that the configuration could not be updated.

LANCOM GS-3100 / 3500 series - LCOS SX 4.00.0414 RU8

New features

→ **Switch Config Notifier** - as from LCOS SX 4.00 RU8 local configuration changes of the GS-3000 series switches are reported to the LMC and changed parameters are taken into account by it in the detailed configuration.

→ MAC addresses of connected clients are reported via SNMPv3 trap.

→ An update of the PoE chip firmware is now conveniently possible via CLI and WebGUI.

→ The non-stop PoE feature has been added and prevents access points or other powered devices from also rebooting during a switch reboot. The feature is disabled by default, but can be conveniently enabled via CLI (config-mode) using <non-stop-poe> followed by <enable> and WebGUI (restart device menu).

→ The boot and event log can now be conveniently deleted via <clear eventlog> or <clear bootlog>. This prevents long loading times if the log has grown accordingly.

→ The default setting of the Spanning Tree protocol has been changed to “switched on”.

→ The command extension ‘delayed-reboot <seconds>’ executes a reboot of the device only after the specified number of seconds.
This function is used for cooperation with some management systems.

→ TLS 1.1 is deprecated and will be disabled so that only TLS 1.2 is usable.

Bug fixes

→ A vulnerability in the zlib library has been fixed (CVE-2018-25032).

→ When a hostname was assigned to a switch and the configuration of the device was subsequently downloaded, the configured hostname appeared twice in the configuration file (in the first and the last entry).

→ If there were very many entries in the syslog of the switch (>20,000), the display of the log in the WEBconfig interface was aborted with the error “Error=500”.

→ A reset of the switch to the delivery state via reset button was already executed if the button was pressed for longer than 5 seconds, although this should only happen after more than 10 seconds.

→ In an LMC terminal session, the context-sensitive online help with the notation “<command>?” could not be performed.

→ In the OID path ‘PoEFirmwareVersion’ the value for the total PoE power of a switch was output.

→ An SNMP query of the switch ports via MIB browser returned 100 Mbps ports with a speed indication of 1000 Mbps.

→ After restarting the switch, the message “Password of user ‘admin’ was changed” was displayed in the log file, although the administrator password was not changed.

→ No error message was issued after uploading an incorrect configuration file via SCP. In this case, the message “scp: config file validation failed” is now issued.

Furthermore, no error message was issued when updating the firmware via SCP and using a non-firmware file. In this case, the message “scp: Invalid image” is now output. If the firmware file is for a different switch model, the message “Firmware product code mismatch” is output.

→ If STP/RSTP was active on a port with the tagging mode ‘Access’, Voice-VLAN could not be activated on this port.

→ No RADIUS servers could be entered if the IP address contained the number 255 in the second or third octet. In this case, the error message “Invalid host name or IP address” was issued. Furthermore, already existing valid entries were deleted.

→ When using Spanning Tree and Loop Protection at the same time, a loop between different switches was not detected. There is now an additional parameter ‘Action Port’ which can be used to specify which port should be deactivated during a loop (over multiple switches this is the ‘Sender Port’).

→ If the switch had obtained its IP address via DHCP, no IP address could be stored under ‘IP interfaces’ that was located in the same network as the IP address obtained via DHCP. In this case, the error message “Subnet of VLAN 1 overlaps VLAN 1” was issued.

→ Syslog messages sent to an external syslog server contained the ‘Model Name’ inside a STRUCTURED-DATA object. Since the ‘Model Name’ contained a space, the syslog messages could not be processed by the external syslog server. The STRUCTURED-DATA object including the ‘Model Name’ has now been removed as it is not required here.

LANCOM GS-3100 / 3500 series - LCOS SX 4.00.0349 RU7

New features

→ LMC preconfiguration of the LANCOM GS-3152P has been enabled and is now available.

Bug fixes

→ If a switch was assigned a fixed local IP address and a gateway IP address via the LMC add-in, a malfunction of the routing daemon used in the switch could mean that WAN communication was no longer possible via the switch's default route after the configuration was rolled out, and the switch could therefore no longer be reached by the LMC.

→ The switch normally obtains an IP address via DHCP. For a switch managed by the LMC, the IP address obtained via DHCP is statically stored in the LMC as a fallback address with a corresponding static route in case the DHCP server fails.

The priority of the route was changed from 1 (static route) to 254 (DHCP-related route) in case of an error, which caused a conflict. As a result, the routing daemon lost the tracking information for the route, so that this route was no longer taken into account for events that came from the kernel, for example.

→ An LAG group (LACP) created via LMC was not transferred to the running config or startup config of the switch. As a result, the LAG configuration was no longer available after a reboot and link aggregation no longer worked.

→ A vulnerability in the OpenSSL library was fixed (CVE-2022-0778) which allowed an attacker to perform a DoS attack on the target system using compromised TLS certificates.

LANCOM GS-3100 / 3500 series - LCOS SX 4.00.0333 RU6

New features

→ Support for the LANCOM GS-3152P

Bug fixes

→ Due to a failure during the rollout of a configuration from the LMC to the switch, it could happen that individual switch ports were not configurable in the LMC. Since the rollback of the original configuration did not work, the error state (ports not configurable) remained.

→ If in the configuration of a switch of the GS-3000 series the SNMP read community was disabled, no configuration tables could be transmitted to the LMC when claiming the device.

→ When using the „startlmc“ CLI command on a switch that was in preclaimed state with the LMC (device was known to the LMC), a pairing token was requested to connect to the LMC even though it was not necessary.

→ Removing an entry for an LMC rollout project via CLI command „no lmc rollout-project“ was aborted with an error message because the parameter ‚no‘ could not be interpreted.

→ Devices connected to a LANCOM GS-3510XP managed via the LMC could lose their connection to the LMC due to runtime problems.

→ In individual cases, interference could occur on the data bus of a LANCOM GS-3152XSP, which is responsible for controlling the PoE chip and the temperature sensor.

→ Switches of the LANCOM GS-3510 series could experience increased downshift problems with port speeds in firmware version LCOS SX 4.00 RU5. The negotiated port speeds of connected network components (e.g. access points) were suddenly downshifted (e.g. to 100 Mbps or 1 Gbps), although the devices support faster speeds (e.g. 2.5 Gbps).

LANCOM GS-3100 / 3500 series - LCOS SX 4.00.0305 RU5

New features

→ Support for AES-192/256 and SHA-2 algorithms enables even more secure SNMPv3 connections with LANmonitor.

→ The Radius service type in IEEE 802.1X authentication is now configurable and distinguishes between ‚Framed' and 'Call-Check' packets.

→ The LAG detail configuration is now available in the LMC.

→ The 'dir' and 'more' commands now allow viewing and managing configuration scripts and backups on the CLI.

→ In the menu 'VLAN Management / VLAN Membership' several consecutive and identically configured VLANs are now combined in the membership table for a better overview. If there are differences in the configured VLANs, their membership information is displayed in a new row.

→ The boot log of the switches has been extended with a backtrace (memory trace).

Bug fixes

→ When a switch was paired with another LMC instance, the device used the new instance's LMC domain temporarily, but it was not included in the switch's active configuration.

→ The default HTTPS certificate is now replaced by an individually generated certificate.

→ The OID value 'Serial' was output with the incorrect value 'System MAC: <MAC address>' in monitoring tools.

→ In the routing table of a LANCOM GS-3152X an additional row for a default route could not be rolled out from the LMC to the switch. In addition, the value for the distance was not taken over in the switch. The valid distance '1' became the invalid value '0' in the switch.

→ A start of the LMC module trace on the console led to an immediate reboot of the device.

→ When using the 'Force Authorized as Admin State' option in the 802.1X port configuration (default setting), the status 'Unauthorized' was displayed instead of 'Authorized'.

→ If a topology change was detected by the switch in a Spanning Tree network (e.g. due to a cable change), the switch sent a large number of 'topology change notifications' (BPDU storm). This led to a failure of the Spanning Tree function.

→ MAC addresses were not automatically deleted from the ARP cache. When the MAC address was changed (e.g. in environments with virtual machines), this resulted in the affected network subscriber no longer being reachable from the switch.
Furthermore, when trying to clear the ARP cache manually using the console command ‘clear ip arp’, it could happen that this failed and the error message ‘Failed to clear IP ARP: MESA_RC_ERROR’ was issued.

→ If errors occurred when rolling out a configuration via the LMC, it could happen that these were transmitted to the LMC incompletely or not at all.

→ If the switch was configured as a DHCP client and could not establish a connection to the LMC, no DHCP renew was performed. In this case, the error message ‘No DHCP server detected’ was issued in the LMC control state trace.

→ SNMP is disabled by default, but the SNMPv1 / SNMPv2 communities are enabled by default. This means that when SNMP is enabled, the SNMPv1 / SNMPv2 communities are also active without any further adjustments. However, the use of SNMPv1 / SNMPv2 is not recommended for security reasons.
The SNMPv1 / SNMPv2 communities are now disabled by default (reinstallations only).

→ If the switch was accessed via WEBconfig tunnel in the LMC and an HTTP redirect to HTTPS was set up, local authentication was always performed, even if a different method was stored for HTTPS.
If HTTP was disabled for access, access via the WEBconfig tunnel in the LMC was not possible, although access via HTTPS was allowed.

→ A username in the Layer 7 application detection table was displayed illegibly. As a result, this username was also output illegibly in management tools, such as the LMC (Dashboard tile ‘LMC Top-User Table’).

→ In the configuration dialog of a RADIUS server, only an IP address could be entered in the ‘Hostname’ field. It was not possible to specify a DNS name.

LANCOM GS-3100 / 3500 series - LCOS SX 4.00.0261 RU4

New features

→ If the VLAN membership is changed via the Q-Bridge MIB, the port mode is no longer necessarily set to Hybrid.

→ As with the aggregation switches, it is now also possible with these switches to establish a direct WebGUI tunnel from the LMC.

Bug fixes

→ When using the DHCP option 61 (DHCP client identifier), the hardware type ‘0‘ including host name was sent in the ‘DHCP discover‘ instead of the MAC address.

→ If the ‘LLDP Neighbors’ were called in the configuration, the switch could sporadically restart.

→ It could happen that the switch went offline for a short time during the rollout of a configuration via the LANCOM Management Cloud (LMC) and thus the configuration could not be rolled out.

→ After a cold start, the default route was deleted, so that routing to other networks via the switch was no longer possible.

→ With the LANCOM switches of the GS-3000 series it could happen that a configuration rollout via the LMC ended in an endless loop and was not completed.

LANCOM GS-3100 / 3500 series - LCOS SX 4.00.0219 SU3

Bug fixes

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

LANCOM GS-3100 / 3500 series - LCOS SX 4.00.0212 RU2

New features

→ The clock role for the 2.5 Gbps ports of the GS-3528X and GS-3528XP is now switchable via CLI:
- slave preferred
- master preferred
- force slave
- force master.

The default setting is ‚slave preferred'.

→ RADIUS-assigned VLAN with Mac-based authentication can now be used.

→ MAC-based authentication now also works without EAP components The MAC address is now transferred as the user name.

→ The status information of the built-in fans can now be read out via SNMP. They can also be read out as syslog message and sent as e-mail event in case of alarm.

Bug fixes

→ With MAC-based IEEE 802.1x authentication against a RADIUS server, a client was authenticated although a 'RADIUS Reject' returned with an 'EAP Success' in RADIUS authentication. However, the EAP packet of type 'Success' only refers to successful EAP communication.
The switch interpreted only the EAP part and 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.

→ By default, the GS-31x and GS-35x series switches had the HTTPS protocol disabled for communication with the switch and the unencrypted TFTP and SNMPv1 protocols enabled. In the current factory settings, the insecure protocols are disabled and HTTP, HTTPS, and SSH are enabled.

→ If a GS-3528 series switch was connected to a network device with a 1 Gbps port speed on a 2.5 Gbps port, it was possible that the connection was negotiated at 100 Mbps only. In this case, if the port speed on both the switch and the network device was fixed to 1 Gbps, the connection failed.

→ The VLAN configuration could not be set correctly via SNMP (Q-Bridge). When setting the PVID for a port in Access or Trunk mode, all VLANs were stored in the 'Allowed VLAN' field instead of just the 'Port VLAN ID'. The 'Allowed VLAN' field could not be set and remained at its original value.

LANCOM GS-3100 / 3500 series - LCOS SX 4.00.0139 RU1

New features

→ Support for the PowerEthernet MIB
→ SNMPv1/2: The read community can now be disabled
→ LMC client: DHCP option 43 is now configurable
→ LMC client: DHCP renew after ‘Connection error’

Bug fixes

→ The creation of IP routes on a LANCOM GS-3152XP via CLI resulted in deleting an existing default route.
→ If more than one default route was configured on the LANCOM GS-3152XP, the switch always initialized the latest created default route after a restart. All other default routes were not loaded and thus were missing in the configuration.
→ After a restart, the switch sent some STP packets into the network using all ports, although the STP function (Spanning Tree Protocol) was disabled in the configuration.
→ When someone tried to access a LANCOM switch via a LANCOM router using the function ‘create TCP/HTTP tunnel‘, or via a routed connection per HTTP(s), the switch cancelled the request with an ‘Internal Server Error‘.
→ If a backup configuration was loaded into a LANCOM switch, the switch did not store this as a start configuration (boot persistent). As a result, the switch always used its default configuration after a restart.
→ The LANCOM switches of the GS-31xx series and the GS-3528XSP could not be restarted via the LANCOM Management Cloud (LMC).
→ After having successfully uploaded a firmware via web interface the message ‘service unavailable’ was displayed right before the mandatory device restart. This message has been replaced by an informative dialog concerning the firmware update process.
→ The error message which was displayed when trying to upload a non-suitable device firmware was not precise. Now an error message with a precise text is displayed.
→ The LMC diagnose trace output was only shown on the console using the command ‘trace on’ when using a serial connection to the LANCOM switch.
→ An LACP link consisting of more than four interfaces could not be operated stable. Furthermore, network malfunctions on the devices connected to the switch could occur when operating an LACP link.
→ Configuration elements could not be written per SNMP if the default value ‘private’ did not exist in ‘Write community’.
→ An SNMP request for the available switch ports on a GS-3152X returned the

value 54 instead of 52.

→ With disabled SNMPv1/2 protocol (default setting) access per SNMPv3 protocol was not possible, too.

→ In the table ‘Static ARP Inspection‘ no additional line could be added, neither per web interface, nor per SNMP.

→ If the PoE budget was exceeded, no appropriate message was displayed in the switch’s webinterface or syslog.

→ No name designations for VLANs could be added on the web interface.

→ In a console session which was established via the switch’s serial interface no backspace function could be used (backspace key).

→ When using a RADIUS authenticated login for the web interface or console the switch did not send RADIUS authentication packets. The switch login was successful, but accounting did not work.

LANCOM GS-3100 / 3500 series - LCOS SX 4.00.0070 Rel

Features

→ Initial release version for all new switches of the series GS-3000

→ New function: DHCP server

→ New function: static routing

→ Unified MIB: Starting from version LCOS SX 4.00 Rel there is a unified SNMP MIB file.

→ New operating status for the sFlow function: Always ON

4. 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 tips

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de | lancom-systems.com