LANCOM
Systems

Release Notes regarding

Switch OS 3.32 Rel for LANCOM GS-23xx

Copyright (c) 2002-2018 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

23.05.2018, CBuersch

Table of Contents

1. Preface

Warning hint

Before upgrading your device to a new firmware it is essential to backup your device's configuration.
Due to extensive features it is <u>not possible to downgrade</u> to a previous firmware without using the backup configuration.
Please see the reference manual for instructions on how to backup the router configuration.

Procedures

Hint for firmware update to 3.30

Updating from firmware 2.83 or older will reprogram the device's flash memory once.
Thus, the update may take up to 15 minutes, depending on the device

Never disconnect the device from power supply while updating the firmware.
In this case the device won't start again.

For LANCOM Switch types GS-2326(+)/GS-2326P, GS-2352 and GS-2310P:

Switches running Switch OS 2.83 or older have to be updated to Switch OS 3.17 first before being updated to version 3.30.

For LANCOM GS-2352P:

Switches running Switch OS 2.83 or older have to be updated to Switch OS 3.04 first before being updated to version 3.30.

2. Known Issues

Latest support notes and known issues regarding the current Switch OS version can be found in the download area of our website <u>Common support hints</u>

3. New features, improvements, and history

Devices delivered with Switch OS 3.30 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 at any time on the device's WEBconfig under Configuration > LMC. You can manually re-enable the usage of the LMC whenever you want.

LANCOM GS-23xx improvements 3.30.0450 RU4 ► 3.32.0012 Rel

New features

> Scripting ability via the LANCOM Management Cloud
> 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.
> A main device password which was configured via the LANCOM Management Cloud was not included in an *.xml configuration file export.
> No online help was available for the switch's system information "LMC pairing state", "LMC control state", "Largest free mem block", and "Free memory", as well as for the functions "Configuration save" and "Configuration upload".
> 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.
> It was possible that no IPv6 packets were transmitted on particular ports of the GS-2352x switches.
> 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 deposed 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).
> Communication problems with IPv6 packets could occur with activated MLD snooping, if the network connection to the client was cut and reconnected afterwards. A high amount of packet losses could occur when using IPv6, too.
> General stability improvements

LANCOM GS-23xx improvements 3.30.0417 RU3 ► 3.30.0450 RU4

New features

> Display of the current memory consumption on the GUI and CLI
> Device configuration files can now be exported and imported encrypted.
> Persistent boot- and event log

Bugfixes / improvements

> Although the cable LANCOM SFP-DAC10 was displayed accurately in the SFP information, LANCOM GS-2310(P)+ series devices could not establish a link.
> When writing back a configuration from the LMC to a switch, an SNMPv3 user password was overwritten with 8 asterisks (********).
> 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.
> If authentication data of a switch user account were created or modified, the LMC overwrote the existing password using the appropriate user name. The administrator account of the switch was not affected by this.
> 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 being executed endlessly when working the list. This led to a 100 % CPU load and blocked any further services from executing (e.g. packet flow).
> If a configuration was written to the switch by LMC or SNMP, not all possible action values for ARP spoofing could be set. This prevented the configuration from being written to the switch.

LANCOM GS-23xx improvements 3.30.0324 RU2 ► 3.30.0417 RU3

New features

> Support for the new SFP copper module LANCOM SFP-CO1
> Support for the new Direct attach cable LANCOM SFP-DAC10 for all switch models with 10G-ports
> New function "Password Policy" (minimum requirements to a secure password)

Bugfixes / improvements

> Fixed a misbehavior related to the management accessibility
> Improvements in usage of the LANCOM Management Cloud
> General stability improvements

LANCOM GS-23xx improvements 3.30.0321 RU1 ► 3.30.0324 RU2

Bugfixes / improvements

> New monitoring entries could not be created in the LANCOM Management Cloud if the appropriate table did not contain any entries yet.
> If no DHCP server was found within the network for a DHCP-configured LANCOM switch, the fallback to the default IP address failed (172.23.56.250).
> If the trace "lmc-control-data" was executed on a serially connected LANCOM switch, the trace output displayed faulty infomation.

LANCOM GS-23xx improvements 3.30.0204 Rel ▶ 3.30.0321 RU1

Bugfixes / improvements

> A firmware upgrade which was triggered by the LANCOM Management Cloud (LMC) works reliable again.
> The entries under 'TACACS+ Authentication Server Configuration' could not be deleted via LANCOM Management Cloud (LMC).
> If a pairing between a LANCOM switch type GS-23xx and the LMC was performed, and the device did a restart while pairing, the pairing process was not completed after the device restart.
> If the management VLAN ID of a LANCOM GS-2352(P) was not '0', the device could not be found by LANconfig, if IGMP snooping was enabled.
> 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.
> The SNMP output of "dot1qVlanStaticEgressPorts" of the Q-Bridge MIB was done decimal. This was now changed to an SNMP output as octet string.
> 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-23xx improvements 3.30.0115 RC1 ▶ 3.30.0204 Rel

Bugfixes / improvements

> Possible memory losses when using SNMP and SSH have been fixed.
> Random disconnects when using SSH were fixed.
> The activation of Voice VLAN no longer leads to the static entry of dynamic MAC addresses in the MAC address table.

LANCOM GS-23xx improvements 3.22.0003 Rel ► 3.30.0115 RC1

New features

> Support for the LANCOM Management Cloud (LMC)
> It is now possible to invoke a cold boot of the device from the configuration interface as well as via command line.
> Syslog is now able to store up to 1.000 syslog messages.The entries oft he syslog table can now be sorted by time of day.
> Thanks to enhancements within the SNMP MIB structure (private MIB) it is now possible to configure AAA, IGMP snooping, SNMPv2/v3, NAS, private based VLAN, and MAC based VLAN.
> Innovaphone was added as a manufacturer to the OUI table in the Voice VLAN menu.

Bugfixes / improvements

> The configuration interface is displayed accurate again in 2560 x 1440 pixels resolution.
> An SSH connection which was configured with keepalive does no longer lead to a device restart.

LANCOM GS-23xx improvements 3.17 Rel ► 3.22.0003 Rel

New features

> Support for AES 128 with SNMPv3
> SNMP Get Community can be enabled/disabled now
> The NTP synchronization interval can now be configured
> A time for a switch restart can be added on the CLI

Bugfixes / improvements

> The LLDP neighborhood is shown with the correct IPv6 addresses
> Fixed a bug which sometimes led to inaccessability of the switch after a restart
> Fixed a problem with DHCP option 43
> If IPv6 autoconfiguration is enabled, the IPv6 address will be updated automatically if the prefix changes
> If the authentication via Telnet is forbidden, the appropriate port will be disabled completely

LANCOM GS-2326(P) / GS-2352(P) / GS-2310P improvements 3.10 Rel ► 3.17 Rel

New features

> Five additional SNMP GET communities can be configured
> SSL certificates are now signed with SHA2 (SHA512)
> Dropbear SSH Version update

Bugfixes / improvements

> Four-wire network cables are supported in auto-negotiation mode
> For HTTPS access via Firefox there is no need to execute "cert-renew" after a firmware upgrade
> Port speed can be changed from "10 Mbps half duplex" or "100Mbps half duplex" to "Auto" via CLI
> Improvements for EasyPort and SCP functionality

LANCOM GS-2326(P) / GS-2352(P) / GS-2310P improvements 2.83 Rel ► 3.10 Rel

New features

> An automatic protocol based access lock can be configured based on incorrect logins.
> XML configuration files are saved containing an additional header which holds information about device type, export date, firmware version and serial number.
> Enhanced IPv6 information within the system information
> NTP configuration now supports domain names
> Configurable QoS settings for prioritizing source and target IP address
> The IPv6 prefix now has a default length of 64 bit
> Extended the RADIUS Shared Secret password length to 64 characters
> Easy Port supports now Multi-VLAN, and user-defined templates can be created.
> Support for DHCP option 43
> Improvements for the DHCP relay function
> LSR support
> Support for RSA 2048 with SSH and HTTPS access
> Removed DES based encryption
> Support for ARP Spoofing
> The DHCP relay agent now supports multiple VLAN, port and access groups.
> Configurable GIADDR for DHCP relay function
> Added 5 more SNMP communities
> Improved generation of the HTTPs certificate
> Support for DH 2048 Bit

Bugfixes / improvements

> The switch sends a Stop-Accounting-Status-Type when the accounting is finished.
> The switch sends TFTP accounting information if TACACS+ authentication is enabled.
> MAC based authentication via 802.1X works again.
> Static Trunk configuration is included again when exporting/importing a configuration.
> The port description can be edited and/or deleted using the CLI.
> Fixed a bug which caused a switch reboot if IGMP packets were forwarded and a link was deleted.
> The PVID can be changed again via CLI.
> The switch does no longer reboot when receiving a DHCP offer/ack packet bigger than 576 bytes.
> HTTPS access with Firefox v39.0 and higher works again

LANCOM GS-2326(P) / GS-2352(P) / GS-2310P improvements 2.52 Rel ▶ 2.83 Rel

New features

> The online help was improved.
> The hardware version is displayed in the system information.
> Configuration and firmware can now be installed via SCP.
> Support for further radius attributes at login/logout
> The default values of configuration time were adjusted
> HTTPS certificates have been improved
> With the new CLI command „cert-renew" a new HTTPS certificate with a unique serial number can be generated
> Access via TFTP can be configured
> LANCOM GS-2352 and GS-2352P support the following 10GB SFP Direct-Attach-Cable:
>> HP SFP+ Direct Attach 1m J9281B
>> D-link DEM-cb300S P3400XA03000-A
>> Intel Ethernet SFP+ Twinaxial Cable XDACBL3M - Twinaxial-Kabel - SFP+ (M)
> The device name is displayed within the browser tab

Bugfixes / improvements

> If DHCP snooping is activated in a PXE environment, a client still get an address assigned
> Without authentication you won't get an address on a port with 802.1x authentication
> Enabling DHCP Snooping no longer causes a crash
> If several commands be performed, the connection to a TACAS+ server won't get disconnected when the accounting is activated
> Access to other switches using single IP over HTTPS has been corrected
> If the IPv4 and IPv6 client is activated and the device name contains more then 254 signs, this will don't lead to a countless sending of Router Solicitations per second
> When several clients sign in to a port with 802.1x authentication, this will not lead to a crash
> The configuration can be imported/exported via LANconfig as XML again
> If the password contains invalid characters, this leads to an error message
> The download and upload of the configuration via TFTP can only be performed by a user who has the permission configured
> The TFTP download and upload works even if the first character of the password is a "@"
> When sending emails the setting for summer / winter time is taken into account

LANCOM GS-2326(P) / GS-2352(P) improvements 2.26 Rel ► 2.52 Rel

New features

> Protected device access by TACACS+ or RADIUS authentication is displayed on the web interface
> Extended the private MIB by PoE and VLAN port configuration
> Support for 1024bit SSL encryption
> The default value for the VLAN port was changed to „C-port"
> Adjusted background color for the web interface
> A status code is returned for a correct LANconfig display while updating the firmware

Bugfixes / improvements

> Access via LACP Link with IPv6 is possible after reboot
> Revised legend for the serial number field
> If no user data is transferred during TFTP access, an appropriate error code is returned for LANconfig
> Added help items for TACACS+ Authorization, Accounting Configuration and Traffic Class
> The navigation bar is displayed in Internet Explorer 10
> Customized help for ACL configuration
> LLDP-MED settings can be retrieved via MIB
> A PXE Boot client gets an IP address if DHCP snooping is enabled
> Fixed serial number help
> Configuration export and import allows for all parameters
> If DHCP Snooping is enabled on a trusted ethernet port, DHCP packets on ports 66-89 and 4011 are allowed, too
> The switch waits up to 15 minutes for an IP address allocation by a DHCP server before it falls back to its default IP address
> Adjusted DHCP host name
> Fixed help for Circuit- and Remote ID
> The MIB contains the correct value for „pethPsePortDetectionStatus"
> Corrected the default values for the IPv6 configuration
> Increased the default value for access level modification to Privilege Level 15
> If a loop is plugged between 802.1x configured ports, the switch does not boot
> When configuring SMTP, the recipient is listed only once
> Configuration import works with long VLAN names, too

LANCOM GS-2326(P) / GS-2352 improvements 1.65.Rel ► 2.26 Rel

Bugfixes / improvements

> SNMPv3 trap host configuration display is correct after an SNMP command was executed from CLI
> ACL works again, even if ARP packets were received
> The password is no longer deletd if the system name was changed
> The model name is displayed correctly if retrieved by SNMPc
> Improved Reboot/Restore button
> Path cost is determined correctly when using STP and aggregation at the same time
> On a Windows 2008 Server the switche's MAC address is displayed
> All devices with identical first 4 byte MAC address are displayed
> No trap events are sent if the respective port is disabled
> Easy Port: The traffic class value can be changed for IP-CAM and WiFi-AP
> Easy Port: Feedback when pressing the Apply button
> Easy Port: If Port Security is enabled for one port, it is activated globally
> Easy Port: A VLAN group is built with the selcted ports using the VLAN ID with IP-CAM and WIFI AP
> The model name is shown on the command line
> No reboot when accessing the switch via LANconfig/SSH
> Improved answer times when scanning ethernet- and PoE-ports with LANmonitor
> Modification within the NTP protocol: NTP request is working reliably
> % and + characters can be used for passwords

LANCOM GS-2326 / GS-2352 improvements 1.48 RC1 ► 1.65 Rel

Bugfixes / improvements

> Improved ping answer times
> Changing the system description parameters can no longer cause a device password reset
> Optimization of the 10 GBit ports improves handling for packets with high run time
> Multicast packets in a ring topology do no longer cause loss of management access while plugging and unplugging the cable
> Fixed a problem which could cause an incompletely read MIB file
> An SNMP walk can now be done without errors
> Fixed a problem with configuration file import
> Improved 802.1x authentication when using a Windows 2008 Server as a Radius server

LANCOM GS-2326 / GS-2352 improvements 1.32 Rel ▶ 1.48 RC1

Bugfixes / improvements

> Switching a port On/Off repeatedly could lead to connection loss
> Fixed a problem with speed recognition in automode for the 10G SFP ports
> Improved LACP stability
> Improved display of the IPv6 link-local address
> Corrected answer behaviour for the link-local address
> Fixed faulty syslog configuration display
> Improved system stability when simultaneously configuring STP and LACP
> Improved Web interface display after saving the user configuration
> It is now possible to configure an SNMP trap server IP address
> Corrected display after firmware upload or restart via webinterface

4.   Comments

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.